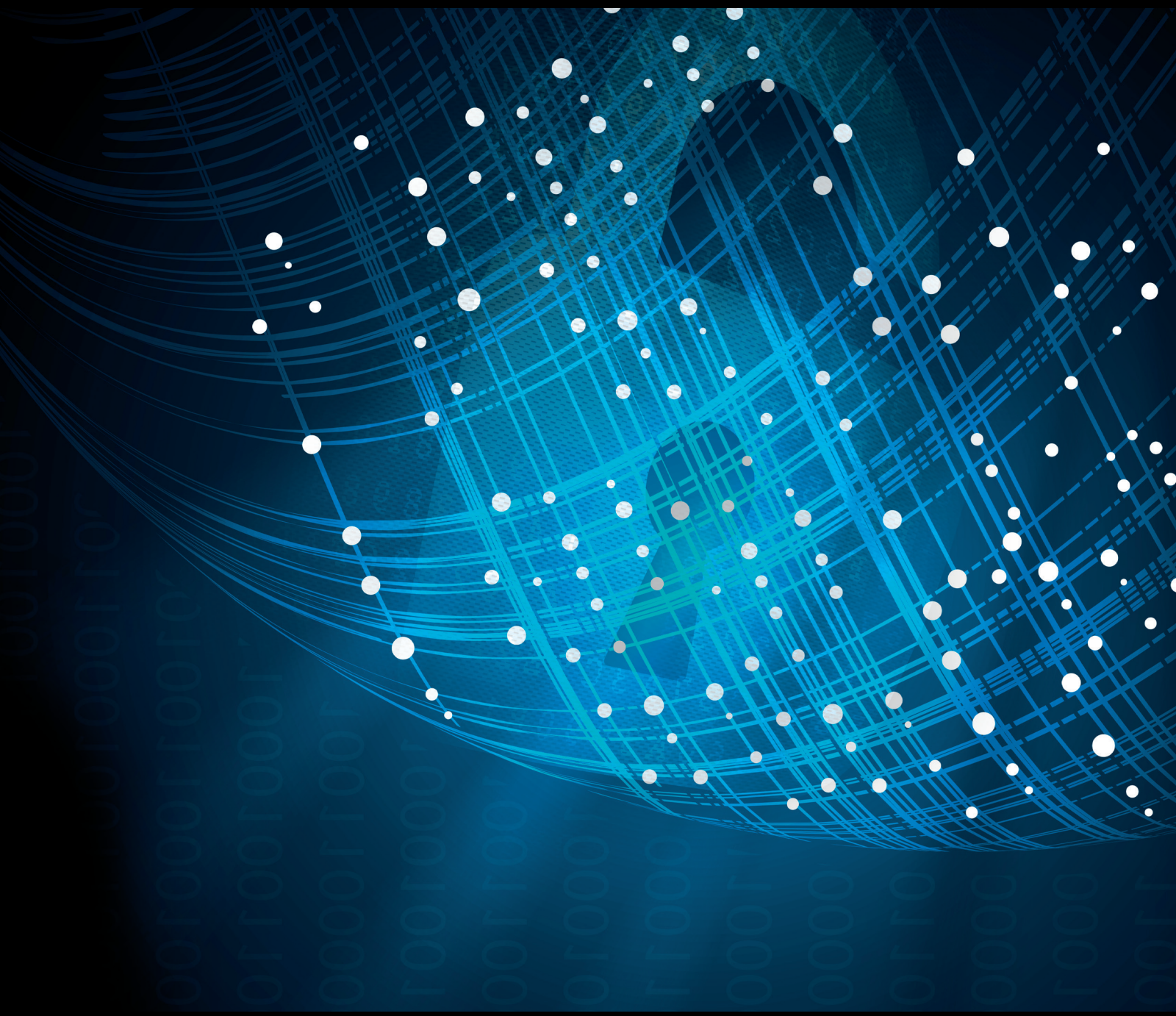
Security and Communication Networks

Privacy Enhancing Technologies for Emerging Computing Systems

Lead Guest Editor: Zhiping Cai
Guest Editors: Li Chen, Xiaojun Wang, and Fang Liu



Privacy Enhancing Technologies for Emerging Computing Systems

Security and Communication Networks

Privacy Enhancing Technologies for Emerging Computing Systems

Lead Guest Editor: Zhiping Cai
Guest Editors: Li Chen, Xiaojun Wang, and Fang Liu

Contents

Retracted: Network Interconnection Security Buffer Technology for Power Monitoring System
Security and Communication Networks
Retraction (1 page), Article ID 9850571, Volume 2024 (2024)

Retracted: Performance Evaluation Method of Online Supply Chain Finance Logistics Enterprises Based on GARCH-VAR
Security and Communication Networks
Retraction (1 page), Article ID 9847896, Volume 2024 (2024)

Retracted: Prediction and Analysis of the Physical Test Scores Based on BP Neural Network and Principal Component Analysis Algorithm
Security and Communication Networks
Retraction (1 page), Article ID 9829563, Volume 2024 (2024)

Retracted: Model Construction of Hierarchical Polarization Characteristics Combined with Social E-Commerce Consumer Behavior
Security and Communication Networks
Retraction (1 page), Article ID 9829542, Volume 2024 (2024)

Retracted: Software Security Testing through Coverage in Deep Neural Networks
Security and Communication Networks
Retraction (1 page), Article ID 9827176, Volume 2024 (2024)

Retracted: Application of User Experience Gene Extraction Model Based on Industrial Design
Security and Communication Networks
Retraction (1 page), Article ID 9826419, Volume 2024 (2024)

Retracted: Intelligent Planning of Tourist Routes Based on Cloud Computing and Marching Algorithm
Security and Communication Networks
Retraction (1 page), Article ID 9823136, Volume 2024 (2024)

Retracted: Enterprise Financial Risk Analysis Based on Improved Model *C*-Means Clustering Algorithm
Security and Communication Networks
Retraction (1 page), Article ID 9818032, Volume 2024 (2024)

Retracted: Application of Long-Term and Short-Term Memory Neural Network in Technical Evaluation of Hurdle Track and Field
Security and Communication Networks
Retraction (1 page), Article ID 9816525, Volume 2024 (2024)

Retracted: Engineering Management Model Analysis Using Partial Differential Equation Hilbert Space
Security and Communication Networks
Retraction (1 page), Article ID 9816081, Volume 2024 (2024)

Contents

Retracted: Economic Globalization and Corporate Accounting Risks: An Analysis of Enterprise Risk Management Based on Big Data
Security and Communication Networks
Retraction (1 page), Article ID 9819712, Volume 2023 (2023)

Retracted: Measurement of Economic Fluctuations Based on High-Frequency Financial Time Series
Security and Communication Networks
Retraction (1 page), Article ID 9865347, Volume 2023 (2023)

[Retracted] A Secure and Efficient Multi-Object Grasping Detection Approach for Robotic Arms
Hui Wang, Jieren Cheng, Yichen Xu, Sirui Ni, Zaijia Yang, and Jiangpeng Li
Research Article (16 pages), Article ID 7723164, Volume 2023 (2023)

[Retracted] Economic Globalization and Corporate Accounting Risks: An Analysis of Enterprise Risk Management Based on Big Data
Yantai Zhang
Review Article (11 pages), Article ID 8673357, Volume 2022 (2022)

Multiparty Threshold Private Set Intersection Protocol with Low Communication Complexity
Xiaopeng Yu, Fagen Li, Wei Zhao, Zhengyi Dai, and Dianhua Tang
Research Article (12 pages), Article ID 9245516, Volume 2022 (2022)

[Retracted] Jamming Meets Antijamming: A Survey of GPS Communication Networks
Yifan Yang
Review Article (7 pages), Article ID 9438027, Volume 2022 (2022)

[Retracted] A Table Tennis Motion Correction System Based on Human Motion Feature Recognition
Liangzi Han
Research Article (8 pages), Article ID 7049429, Volume 2022 (2022)

[Retracted] Software Security Testing through Coverage in Deep Neural Networks
Weiyu Fu and Lixia Wang
Research Article (7 pages), Article ID 2834982, Volume 2022 (2022)

[Retracted] Research on Securities Portfolio Model Based on Genetic Optimization Neural Network
Puming Zhang
Research Article (10 pages), Article ID 6476168, Volume 2022 (2022)

[Retracted] Analysis of Risk Assessment of Overseas Infrastructure Projects Integrating BP-ANN Algorithm
Chengni Li and Jian Zhou
Research Article (13 pages), Article ID 7864665, Volume 2022 (2022)

Contents

Contents

Hindawi
Security and Communication Networks
Volume 2024, Article ID 9897623, 1 page
https://doi.org/10.1155/2024/9897623

Retraction

Retracted: A New Method for Inverter Diagnosis of Electric Locomotive Using Adversarial Neural Networks

Security and Communication Networks

Received 8 January 2024; Accepted 8 January 2024; Published 9 January 2024

This article has been retracted by Hindawi following an investigation undertaken by the publisher [1]. This investigation has uncovered evidence of one or more of the following indicators of systematic manipulation of the publication process:

(1) Discrepancies in scope

(2) Discrepancies in the description of the research reported

(3) Discrepancies between the availability of data and the research described

(4) Inappropriate citations

(5) Incoherent, meaningless and/or irrelevant content included in the article

(6) Manipulated or compromised peer review

The presence of these indicators undermines our confidence in the integrity of the article's content and we cannot, therefore, vouch for its reliability. Please note that this notice is intended solely to alert readers that the content of this article is unreliable. We have not investigated whether authors were aware of or involved in the systematic manipulation of the publication process.

Wiley and Hindawi regrets that the usual quality checks did not identify these issues before publication and have since put additional measures in place to safeguard research integrity.

We wish to credit our own Research Integrity and Research Publishing teams and anonymous and named external researchers and research integrity experts for contributing to this investigation.

The corresponding author, as the representative of all authors, has been given the opportunity to register their agreement or disagreement to this retraction. We have kept a record of any response received.

References

[1] Y. Shi, C. Chen, and Y. Luo, "A New Method for Inverter Diagnosis of Electric Locomotive Using Adversarial Neural Networks," *Security and Communication Networks*, vol. 2022, Article ID 5606328, 10 pages, 2022.

Hindawi
Security and Communication Networks
Volume 2024, Article ID 9897316, 1 page
https://doi.org/10.1155/2024/9897316

Retraction

Retracted: Research on Tourism Route Recommendation Strategy Based on Convolutional Neural Network and Collaborative Filtering Algorithm

Security and Communication Networks

Received 8 January 2024; Accepted 8 January 2024; Published 9 January 2024

This article has been retracted by Hindawi following an investigation undertaken by the publisher [1]. This investigation has uncovered evidence of one or more of the following indicators of systematic manipulation of the publication process:

(1) Discrepancies in scope
(2) Discrepancies in the description of the research reported
(3) Discrepancies between the availability of data and the research described
(4) Inappropriate citations
(5) Incoherent, meaningless and/or irrelevant content included in the article
(6) Manipulated or compromised peer review

The presence of these indicators undermines our confidence in the integrity of the article's content and we cannot, therefore, vouch for its reliability. Please note that this notice is intended solely to alert readers that the content of this article is unreliable. We have not investigated whether authors were aware of or involved in the systematic manipulation of the publication process.

In addition, our investigation has also shown that one or more of the following human-subject reporting requirements has not been met in this article: ethical approval by an Institutional Review Board (IRB) committee or equivalent, patient/participant consent to participate, and/or agreement to publish patient/participant details (where relevant).

Wiley and Hindawi regrets that the usual quality checks did not identify these issues before publication and have since put additional measures in place to safeguard research integrity.

We wish to credit our own Research Integrity and Research Publishing teams and anonymous and named external researchers and research integrity experts for contributing to this investigation.

The corresponding author, as the representative of all authors, has been given the opportunity to register their agreement or disagreement to this retraction. We have kept a record of any response received.

References

[1] S. He, "Research on Tourism Route Recommendation Strategy Based on Convolutional Neural Network and Collaborative Filtering Algorithm," *Security and Communication Networks*, vol. 2022, Article ID 4659567, 9 pages, 2022.

Hindawi
Security and Communication Networks
Volume 2024, Article ID 9893281, 1 page
https://doi.org/10.1155/2024/9893281

Retraction

Retracted: Analysis of Dynamic Influence Mechanism of Network Public Opinion Based on Simulation Feature Extraction

Security and Communication Networks

Received 8 January 2024; Accepted 8 January 2024; Published 9 January 2024

This article has been retracted by Hindawi following an investigation undertaken by the publisher [1]. This investigation has uncovered evidence of one or more of the following indicators of systematic manipulation of the publication process:

(1) Discrepancies in scope

(2) Discrepancies in the description of the research reported

(3) Discrepancies between the availability of data and the research described

(4) Inappropriate citations

(5) Incoherent, meaningless and/or irrelevant content included in the article

(6) Manipulated or compromised peer review

The presence of these indicators undermines our confidence in the integrity of the article's content and we cannot, therefore, vouch for its reliability. Please note that this notice is intended solely to alert readers that the content of this article is unreliable. We have not investigated whether authors were aware of or involved in the systematic manipulation of the publication process.

In addition, our investigation has also shown that one or more of the following human-subject reporting requirements has not been met in this article: ethical approval by an Institutional Review Board (IRB) committee or equivalent, patient/participant consent to participate, and/or agreement to publish patient/participant details (where relevant).

Wiley and Hindawi regrets that the usual quality checks did not identify these issues before publication and have since put additional measures in place to safeguard research integrity.

We wish to credit our own Research Integrity and Research Publishing teams and anonymous and named external researchers and research integrity experts for contributing to this investigation.

The corresponding author, as the representative of all authors, has been given the opportunity to register their agreement or disagreement to this retraction. We have kept a record of any response received.

References

[1] Y. Zhang, "Analysis of Dynamic Influence Mechanism of Network Public Opinion Based on Simulation Feature Extraction," *Security and Communication Networks*, vol. 2022, Article ID 8423643, 12 pages, 2022.

Hindawi
Security and Communication Networks
Volume 2024, Article ID 9891407, 1 page
https://doi.org/10.1155/2024/9891407

Retraction

Retracted: Secure Two-Party Computation Based on Fast Cut-and-Choose Bilateral Oblivious Transfer

Security and Communication Networks

Received 8 January 2024; Accepted 8 January 2024; Published 9 January 2024

This article has been retracted by Hindawi, as publisher, following an investigation undertaken by the publisher [1]. This investigation has uncovered evidence of systematic manipulation of the publication and peer-review process. We cannot, therefore, vouch for the reliability or integrity of this article.

Please note that this notice is intended solely to alert readers that the peer-review process of this article has been compromised.

Wiley and Hindawi regret that the usual quality checks did not identify these issues before publication and have since put additional measures in place to safeguard research integrity.

We wish to credit our Research Integrity and Research Publishing teams and anonymous and named external researchers and research integrity experts for contributing to this investigation.

The corresponding author, as the representative of all authors, has been given the opportunity to register their agreement or disagreement to this retraction. We have kept a record of any response received.

References

[1] Y. Wang, K. Xiong, H. Tian, J. Zhang, and X. Yan, "Secure Two-Party Computation Based on Fast Cut-and-Choose Bilateral Oblivious Transfer," *Security and Communication Networks*, vol. 2022, Article ID 3880413, 10 pages, 2022.

Hindawi
Security and Communication Networks
Volume 2024, Article ID 9890863, 1 page
https://doi.org/10.1155/2024/9890863

Retraction

Retracted: A Secure and Efficient Multi-Object Grasping Detection Approach for Robotic Arms

Security and Communication Networks

Received 8 January 2024; Accepted 8 January 2024; Published 9 January 2024

This article has been retracted by Hindawi following an investigation undertaken by the publisher [1]. This investigation has uncovered evidence of one or more of the following indicators of systematic manipulation of the publication process:

(1) Discrepancies in scope

(2) Discrepancies in the description of the research reported

(3) Discrepancies between the availability of data and the research described

(4) Inappropriate citations

(5) Incoherent, meaningless and/or irrelevant content included in the article

(6) Manipulated or compromised peer review

The presence of these indicators undermines our confidence in the integrity of the article's content and we cannot, therefore, vouch for its reliability. Please note that this notice is intended solely to alert readers that the content of this article is unreliable. We have not investigated whether authors were aware of or involved in the systematic manipulation of the publication process.

In addition, our investigation has also shown that one or more of the following human-subject reporting requirements has not been met in this article: ethical approval by an Institutional Review Board (IRB) committee or equivalent, patient/participant consent to participate, and/or agreement to publish patient/participant details (where relevant).

Wiley and Hindawi regrets that the usual quality checks did not identify these issues before publication and have since put additional measures in place to safeguard research integrity.

We wish to credit our own Research Integrity and Research Publishing teams and anonymous and named external researchers and research integrity experts for contributing to this investigation.

The corresponding author, as the representative of all authors, has been given the opportunity to register their agreement or disagreement to this retraction. We have kept a record of any response received.

References

[1] H. Wang, J. Cheng, Y. Xu, S. Ni, Z. Yang, and J. Li, "A Secure and Efficient Multi-Object Grasping Detection Approach for Robotic Arms," *Security and Communication Networks*, vol. 2023, Article ID 7723164, 16 pages, 2023.

Hindawi
Security and Communication Networks
Volume 2024, Article ID 9864701, 1 page
https://doi.org/10.1155/2024/9864701

Retraction

Retracted: Jamming Meets Antijamming: A Survey of GPS Communication Networks

Security and Communication Networks

Received 8 January 2024; Accepted 8 January 2024; Published 9 January 2024

This article has been retracted by Hindawi following an investigation undertaken by the publisher [1]. This investigation has uncovered evidence of one or more of the following indicators of systematic manipulation of the publication process:

(1) Discrepancies in scope

(2) Discrepancies in the description of the research reported

(3) Discrepancies between the availability of data and the research described

(4) Inappropriate citations

(5) Incoherent, meaningless and/or irrelevant content included in the article

(6) Manipulated or compromised peer review

The presence of these indicators undermines our confidence in the integrity of the article's content and we cannot, therefore, vouch for its reliability. Please note that this notice is intended solely to alert readers that the content of this article is unreliable. We have not investigated whether authors were aware of or involved in the systematic manipulation of the publication process.

Wiley and Hindawi regrets that the usual quality checks did not identify these issues before publication and have since put additional measures in place to safeguard research integrity.

We wish to credit our own Research Integrity and Research Publishing teams and anonymous and named external researchers and research integrity experts for contributing to this investigation.

The corresponding author, as the representative of all authors, has been given the opportunity to register their agreement or disagreement to this retraction. We have kept a record of any response received.

References

[1] Y. Yang, "Jamming Meets Antijamming: A Survey of GPS Communication Networks," *Security and Communication Networks*, vol. 2022, Article ID 9438027, 7 pages, 2022.

Hindawi
Security and Communication Networks
Volume 2024, Article ID 9860176, 1 page
https://doi.org/10.1155/2024/9860176

Retraction

Retracted: An Intrusion Detection Model Based on Improved ACGAN in Big Data Environment

Security and Communication Networks

Received 8 January 2024; Accepted 8 January 2024; Published 9 January 2024

This article has been retracted by Hindawi following an investigation undertaken by the publisher [1]. This investigation has uncovered evidence of one or more of the following indicators of systematic manipulation of the publication process:

(1) Discrepancies in scope

(2) Discrepancies in the description of the research reported

(3) Discrepancies between the availability of data and the research described

(4) Inappropriate citations

(5) Incoherent, meaningless and/or irrelevant content included in the article

(6) Manipulated or compromised peer review

The presence of these indicators undermines our confidence in the integrity of the article's content and we cannot, therefore, vouch for its reliability. Please note that this notice is intended solely to alert readers that the content of this article is unreliable. We have not investigated whether authors were aware of or involved in the systematic manipulation of the publication process.

Wiley and Hindawi regrets that the usual quality checks did not identify these issues before publication and have since put additional measures in place to safeguard research integrity.

We wish to credit our own Research Integrity and Research Publishing teams and anonymous and named external researchers and research integrity experts for contributing to this investigation.

The corresponding author, as the representative of all authors, has been given the opportunity to register their agreement or disagreement to this retraction. We have kept a record of any response received.

References

[1] J. Liao, "An Intrusion Detection Model Based on Improved ACGAN in Big Data Environment," *Security and Communication Networks*, vol. 2022, Article ID 6821174, 9 pages, 2022.

Hindawi
Security and Communication Networks
Volume 2024, Article ID 9858901, 1 page
https://doi.org/10.1155/2024/9858901

Retraction

Retracted: Digital Reconstruction Method of Power Metering Production Data Based on Digital Twin Technology

Security and Communication Networks

Received 8 January 2024; Accepted 8 January 2024; Published 9 January 2024

This article has been retracted by Hindawi following an investigation undertaken by the publisher [1]. This investigation has uncovered evidence of one or more of the following indicators of systematic manipulation of the publication process:

(1) Discrepancies in scope

(2) Discrepancies in the description of the research reported

(3) Discrepancies between the availability of data and the research described

(4) Inappropriate citations

(5) Incoherent, meaningless and/or irrelevant content included in the article

(6) Manipulated or compromised peer review

The presence of these indicators undermines our confidence in the integrity of the article's content and we cannot, therefore, vouch for its reliability. Please note that this notice is intended solely to alert readers that the content of this article is unreliable. We have not investigated whether authors were aware of or involved in the systematic manipulation of the publication process.

Wiley and Hindawi regrets that the usual quality checks did not identify these issues before publication and have since put additional measures in place to safeguard research integrity.

We wish to credit our own Research Integrity and Research Publishing teams and anonymous and named external researchers and research integrity experts for contributing to this investigation.

The corresponding author, as the representative of all authors, has been given the opportunity to register their agreement or disagreement to this retraction. We have kept a record of any response received.

References

[1] H. Wang, H. Shen, C. Li et al., "Digital Reconstruction Method of Power Metering Production Data Based on Digital Twin Technology," *Security and Communication Networks*, vol. 2022, Article ID 6835371, 10 pages, 2022.

Hindawi
Security and Communication Networks
Volume 2024, Article ID 9852914, 1 page
https://doi.org/10.1155/2024/9852914

Retraction

Retracted: Prediction of High-Frequency Economic Data Based on Stochastic Fluctuation Model

Security and Communication Networks

Received 8 January 2024; Accepted 8 January 2024; Published 9 January 2024

This article has been retracted by Hindawi following an investigation undertaken by the publisher [1]. This investigation has uncovered evidence of one or more of the following indicators of systematic manipulation of the publication process:

(1) Discrepancies in scope

(2) Discrepancies in the description of the research reported

(3) Discrepancies between the availability of data and the research described

(4) Inappropriate citations

(5) Incoherent, meaningless and/or irrelevant content included in the article

(6) Manipulated or compromised peer review

The presence of these indicators undermines our confidence in the integrity of the article's content and we cannot, therefore, vouch for its reliability. Please note that this notice is intended solely to alert readers that the content of this article is unreliable. We have not investigated whether authors were aware of or involved in the systematic manipulation of the publication process.

Wiley and Hindawi regrets that the usual quality checks did not identify these issues before publication and have since put additional measures in place to safeguard research integrity.

We wish to credit our own Research Integrity and Research Publishing teams and anonymous and named external researchers and research integrity experts for contributing to this investigation.

The corresponding author, as the representative of all authors, has been given the opportunity to register their agreement or disagreement to this retraction. We have kept a record of any response received.

References

[1] X. Zhang, T. Qi, and D.-J. Kim, "Prediction of High-Frequency Economic Data Based on Stochastic Fluctuation Model," *Security and Communication Networks*, vol. 2022, Article ID 4109563, 13 pages, 2022.

Hindawi
Security and Communication Networks
Volume 2024, Article ID 9852152, 1 page
https://doi.org/10.1155/2024/9852152

Retraction

Retracted: Research on Securities Portfolio Model Based on Genetic Optimization Neural Network

Security and Communication Networks

Received 8 January 2024; Accepted 8 January 2024; Published 9 January 2024

This article has been retracted by Hindawi following an investigation undertaken by the publisher [1]. This investigation has uncovered evidence of one or more of the following indicators of systematic manipulation of the publication process:

(1) Discrepancies in scope

(2) Discrepancies in the description of the research reported

(3) Discrepancies between the availability of data and the research described

(4) Inappropriate citations

(5) Incoherent, meaningless and/or irrelevant content included in the article

(6) Manipulated or compromised peer review

The presence of these indicators undermines our confidence in the integrity of the article's content and we cannot, therefore, vouch for its reliability. Please note that this notice is intended solely to alert readers that the content of this article is unreliable. We have not investigated whether authors were aware of or involved in the systematic manipulation of the publication process.

Wiley and Hindawi regrets that the usual quality checks did not identify these issues before publication and have since put additional measures in place to safeguard research integrity.

We wish to credit our own Research Integrity and Research Publishing teams and anonymous and named external researchers and research integrity experts for contributing to this investigation.

The corresponding author, as the representative of all authors, has been given the opportunity to register their agreement or disagreement to this retraction. We have kept a record of any response received.

References

[1] P. Zhang, "Research on Securities Portfolio Model Based on Genetic Optimization Neural Network," *Security and Communication Networks*, vol. 2022, Article ID 6476168, 10 pages, 2022.

Hindawi
Security and Communication Networks
Volume 2024, Article ID 9850571, 1 page
https://doi.org/10.1155/2024/9850571

Retraction

Retracted: Network Interconnection Security Buffer Technology for Power Monitoring System

Security and Communication Networks

Received 8 January 2024; Accepted 8 January 2024; Published 9 January 2024

This article has been retracted by Hindawi, as publisher, following an investigation undertaken by the publisher [1]. This investigation has uncovered evidence of systematic manipulation of the publication and peer-review process. We cannot, therefore, vouch for the reliability or integrity of this article.

Please note that this notice is intended solely to alert readers that the peer-review process of this article has been compromised.

Wiley and Hindawi regret that the usual quality checks did not identify these issues before publication and have since put additional measures in place to safeguard research integrity.

We wish to credit our Research Integrity and Research Publishing teams and anonymous and named external researchers and research integrity experts for contributing to this investigation.

The corresponding author, as the representative of all authors, has been given the opportunity to register their agreement or disagreement to this retraction. We have kept a record of any response received.

References

[1] J. Wang, J. Wu, W. Tao, W. Zhu, and W. Qiu, "Network Interconnection Security Buffer Technology for Power Monitoring System," *Security and Communication Networks*, vol. 2022, Article ID 6371062, 11 pages, 2022.

Hindawi
Security and Communication Networks
Volume 2024, Article ID 9847896, 1 page
https://doi.org/10.1155/2024/9847896

Retraction

Retracted: Performance Evaluation Method of Online Supply Chain Finance Logistics Enterprises Based on GARCH-VAR

Security and Communication Networks

Received 8 January 2024; Accepted 8 January 2024; Published 9 January 2024

This article has been retracted by Hindawi following an investigation undertaken by the publisher [1]. This investigation has uncovered evidence of one or more of the following indicators of systematic manipulation of the publication process:

(1) Discrepancies in scope

(2) Discrepancies in the description of the research reported

(3) Discrepancies between the availability of data and the research described

(4) Inappropriate citations

(5) Incoherent, meaningless and/or irrelevant content included in the article

(6) Manipulated or compromised peer review

The presence of these indicators undermines our confidence in the integrity of the article's content and we cannot, therefore, vouch for its reliability. Please note that this notice is intended solely to alert readers that the content of this article is unreliable. We have not investigated whether authors were aware of or involved in the systematic manipulation of the publication process.

Wiley and Hindawi regrets that the usual quality checks did not identify these issues before publication and have since put additional measures in place to safeguard research integrity.

We wish to credit our own Research Integrity and Research Publishing teams and anonymous and named external researchers and research integrity experts for contributing to this investigation.

The corresponding author, as the representative of all authors, has been given the opportunity to register their agreement or disagreement to this retraction. We have kept a record of any response received.

References

[1] T. Xia and J. Yang, "Performance Evaluation Method of Online Supply Chain Finance Logistics Enterprises Based on GARCH-VAR," *Security and Communication Networks*, vol. 2022, Article ID 4500430, 9 pages, 2022.

Hindawi
Security and Communication Networks
Volume 2024, Article ID 9829563, 1 page
https://doi.org/10.1155/2024/9829563

Retraction

Retracted: Prediction and Analysis of the Physical Test Scores Based on BP Neural Network and Principal Component Analysis Algorithm

Security and Communication Networks

Received 8 January 2024; Accepted 8 January 2024; Published 9 January 2024

This article has been retracted by Hindawi following an investigation undertaken by the publisher [1]. This investigation has uncovered evidence of one or more of the following indicators of systematic manipulation of the publication process:

(1) Discrepancies in scope
(2) Discrepancies in the description of the research reported
(3) Discrepancies between the availability of data and the research described
(4) Inappropriate citations
(5) Incoherent, meaningless and/or irrelevant content included in the article
(6) Manipulated or compromised peer review

The presence of these indicators undermines our confidence in the integrity of the article's content and we cannot, therefore, vouch for its reliability. Please note that this notice is intended solely to alert readers that the content of this article is unreliable. We have not investigated whether authors were aware of or involved in the systematic manipulation of the publication process.

In addition, our investigation has also shown that one or more of the following human-subject reporting requirements has not been met in this article: ethical approval by an Institutional Review Board (IRB) committee or equivalent, patient/participant consent to participate, and/or agreement to publish patient/participant details (where relevant).

Wiley and Hindawi regrets that the usual quality checks did not identify these issues before publication and have since put additional measures in place to safeguard research integrity.

We wish to credit our own Research Integrity and Research Publishing teams and anonymous and named external researchers and research integrity experts for contributing to this investigation.

The corresponding author, as the representative of all authors, has been given the opportunity to register their agreement or disagreement to this retraction. We have kept a record of any response received.

References

[1] J. Qu, "Prediction and Analysis of the Physical Test Scores Based on BP Neural Network and Principal Component Analysis Algorithm," *Security and Communication Networks*, vol. 2022, Article ID 5210810, 12 pages, 2022.

Hindawi
Security and Communication Networks
Volume 2024, Article ID 9829542, 1 page
https://doi.org/10.1155/2024/9829542

Retraction

Retracted: Model Construction of Hierarchical Polarization Characteristics Combined with Social E-Commerce Consumer Behavior

Security and Communication Networks

Received 8 January 2024; Accepted 8 January 2024; Published 9 January 2024

This article has been retracted by Hindawi following an investigation undertaken by the publisher [1]. This investigation has uncovered evidence of one or more of the following indicators of systematic manipulation of the publication process:

(1) Discrepancies in scope
(2) Discrepancies in the description of the research reported
(3) Discrepancies between the availability of data and the research described
(4) Inappropriate citations
(5) Incoherent, meaningless and/or irrelevant content included in the article
(6) Manipulated or compromised peer review

The presence of these indicators undermines our confidence in the integrity of the article's content and we cannot, therefore, vouch for its reliability. Please note that this notice is intended solely to alert readers that the content of this article is unreliable. We have not investigated whether authors were aware of or involved in the systematic manipulation of the publication process.

In addition, our investigation has also shown that one or more of the following human-subject reporting requirements has not been met in this article: ethical approval by an Institutional Review Board (IRB) committee or equivalent, patient/participant consent to participate, and/or agreement to publish patient/participant details (where relevant).

Wiley and Hindawi regrets that the usual quality checks did not identify these issues before publication and have since put additional measures in place to safeguard research integrity.

We wish to credit our own Research Integrity and Research Publishing teams and anonymous and named external researchers and research integrity experts for contributing to this investigation.

The corresponding author, as the representative of all authors, has been given the opportunity to register their agreement or disagreement to this retraction. We have kept a record of any response received.

References

[1] Q. Zhang and J. Yang, "Model Construction of Hierarchical Polarization Characteristics Combined with Social E-Commerce Consumer Behavior," *Security and Communication Networks*, vol. 2022, Article ID 9666677, 11 pages, 2022.

Hindawi
Security and Communication Networks
Volume 2024, Article ID 9827176, 1 page
https://doi.org/10.1155/2024/9827176

Retraction

Retracted: Software Security Testing through Coverage in Deep Neural Networks

Security and Communication Networks

Received 8 January 2024; Accepted 8 January 2024; Published 9 January 2024

This article has been retracted by Hindawi following an investigation undertaken by the publisher [1]. This investigation has uncovered evidence of one or more of the following indicators of systematic manipulation of the publication process:

(1) Discrepancies in scope

(2) Discrepancies in the description of the research reported

(3) Discrepancies between the availability of data and the research described

(4) Inappropriate citations

(5) Incoherent, meaningless and/or irrelevant content included in the article

(6) Manipulated or compromised peer review

The presence of these indicators undermines our confidence in the integrity of the article's content and we cannot, therefore, vouch for its reliability. Please note that this notice is intended solely to alert readers that the content of this article is unreliable. We have not investigated whether authors were aware of or involved in the systematic manipulation of the publication process.

Wiley and Hindawi regrets that the usual quality checks did not identify these issues before publication and have since put additional measures in place to safeguard research integrity.

We wish to credit our own Research Integrity and Research Publishing teams and anonymous and named external researchers and research integrity experts for contributing to this investigation.

The corresponding author, as the representative of all authors, has been given the opportunity to register their agreement or disagreement to this retraction. We have kept a record of any response received.

References

[1] W. Fu and L. Wang, "Software Security Testing through Coverage in Deep Neural Networks," *Security and Communication Networks*, vol. 2022, Article ID 2834982, 7 pages, 2022.

Hindawi
Security and Communication Networks
Volume 2024, Article ID 9826419, 1 page
https://doi.org/10.1155/2024/9826419

Retraction

Retracted: Application of User Experience Gene Extraction Model Based on Industrial Design

Security and Communication Networks

Received 8 January 2024; Accepted 8 January 2024; Published 9 January 2024

This article has been retracted by Hindawi following an investigation undertaken by the publisher [1]. This investigation has uncovered evidence of one or more of the following indicators of systematic manipulation of the publication process:

(1) Discrepancies in scope

(2) Discrepancies in the description of the research reported

(3) Discrepancies between the availability of data and the research described

(4) Inappropriate citations

(5) Incoherent, meaningless and/or irrelevant content included in the article

(6) Manipulated or compromised peer review

The presence of these indicators undermines our confidence in the integrity of the article's content and we cannot, therefore, vouch for its reliability. Please note that this notice is intended solely to alert readers that the content of this article is unreliable. We have not investigated whether authors were aware of or involved in the systematic manipulation of the publication process.

Wiley and Hindawi regrets that the usual quality checks did not identify these issues before publication and have since put additional measures in place to safeguard research integrity.

We wish to credit our own Research Integrity and Research Publishing teams and anonymous and named external researchers and research integrity experts for contributing to this investigation.

The corresponding author, as the representative of all authors, has been given the opportunity to register their agreement or disagreement to this retraction. We have kept a record of any response received.

References

[1] Z. Yu, "Application of User Experience Gene Extraction Model Based on Industrial Design," *Security and Communication Networks*, vol. 2022, Article ID 7366480, 14 pages, 2022.

Hindawi
Security and Communication Networks
Volume 2024, Article ID 9823136, 1 page
https://doi.org/10.1155/2024/9823136

Retraction

Retracted: Intelligent Planning of Tourist Routes Based on Cloud Computing and Marching Algorithm

Security and Communication Networks

Received 8 January 2024; Accepted 8 January 2024; Published 9 January 2024

This article has been retracted by Hindawi following an investigation undertaken by the publisher [1]. This investigation has uncovered evidence of one or more of the following indicators of systematic manipulation of the publication process:

(1) Discrepancies in scope

(2) Discrepancies in the description of the research reported

(3) Discrepancies between the availability of data and the research described

(4) Inappropriate citations

(5) Incoherent, meaningless and/or irrelevant content included in the article

(6) Manipulated or compromised peer review

The presence of these indicators undermines our confidence in the integrity of the article's content and we cannot, therefore, vouch for its reliability. Please note that this notice is intended solely to alert readers that the content of this article is unreliable. We have not investigated whether authors were aware of or involved in the systematic manipulation of the publication process.

Wiley and Hindawi regrets that the usual quality checks did not identify these issues before publication and have since put additional measures in place to safeguard research integrity.

We wish to credit our own Research Integrity and Research Publishing teams and anonymous and named external researchers and research integrity experts for contributing to this investigation.

The corresponding author, as the representative of all authors, has been given the opportunity to register their agreement or disagreement to this retraction. We have kept a record of any response received.

References

[1] J. Lu, "Intelligent Planning of Tourist Routes Based on Cloud Computing and Marching Algorithm," *Security and Communication Networks*, vol. 2022, Article ID 8793392, 14 pages, 2022.

Hindawi
Security and Communication Networks
Volume 2024, Article ID 9818032, 1 page
https://doi.org/10.1155/2024/9818032

Retraction

Retracted: Enterprise Financial Risk Analysis Based on Improved Model *C*-Means Clustering Algorithm

Security and Communication Networks

Received 8 January 2024; Accepted 8 January 2024; Published 9 January 2024

This article has been retracted by Hindawi following an investigation undertaken by the publisher [1]. This investigation has uncovered evidence of one or more of the following indicators of systematic manipulation of the publication process:

(1) Discrepancies in scope

(2) Discrepancies in the description of the research reported

(3) Discrepancies between the availability of data and the research described

(4) Inappropriate citations

(5) Incoherent, meaningless and/or irrelevant content included in the article

(6) Manipulated or compromised peer review

The presence of these indicators undermines our confidence in the integrity of the article's content and we cannot, therefore, vouch for its reliability. Please note that this notice is intended solely to alert readers that the content of this article is unreliable. We have not investigated whether authors were aware of or involved in the systematic manipulation of the publication process.

Wiley and Hindawi regrets that the usual quality checks did not identify these issues before publication and have since put additional measures in place to safeguard research integrity.

We wish to credit our own Research Integrity and Research Publishing teams and anonymous and named external researchers and research integrity experts for contributing to this investigation.

The corresponding author, as the representative of all authors, has been given the opportunity to register their agreement or disagreement to this retraction. We have kept a record of any response received.

References

[1] J. Sun and Y. Jiao, "Enterprise Financial Risk Analysis Based on Improved Model *C*-Means Clustering Algorithm," *Security and Communication Networks*, vol. 2022, Article ID 1109813, 12 pages, 2022.

Hindawi
Security and Communication Networks
Volume 2024, Article ID 9816525, 1 page
https://doi.org/10.1155/2024/9816525

Retraction

Retracted: Application of Long-Term and Short-Term Memory Neural Network in Technical Evaluation of Hurdle Track and Field

Security and Communication Networks

Received 8 January 2024; Accepted 8 January 2024; Published 9 January 2024

This article has been retracted by Hindawi following an investigation undertaken by the publisher [1]. This investigation has uncovered evidence of one or more of the following indicators of systematic manipulation of the publication process:

(1) Discrepancies in scope
(2) Discrepancies in the description of the research reported
(3) Discrepancies between the availability of data and the research described
(4) Inappropriate citations
(5) Incoherent, meaningless and/or irrelevant content included in the article
(6) Manipulated or compromised peer review

The presence of these indicators undermines our confidence in the integrity of the article's content and we cannot, therefore, vouch for its reliability. Please note that this notice is intended solely to alert readers that the content of this article is unreliable. We have not investigated whether authors were aware of or involved in the systematic manipulation of the publication process.

In addition, our investigation has also shown that one or more of the following human-subject reporting requirements has not been met in this article: ethical approval by an Institutional Review Board (IRB) committee or equivalent, patient/participant consent to participate, and/or agreement to publish patient/participant details (where relevant).

Wiley and Hindawi regrets that the usual quality checks did not identify these issues before publication and have since put additional measures in place to safeguard research integrity.

We wish to credit our own Research Integrity and Research Publishing teams and anonymous and named external researchers and research integrity experts for contributing to this investigation.

The corresponding author, as the representative of all authors, has been given the opportunity to register their agreement or disagreement to this retraction. We have kept a record of any response received.

References

[1] Z. Liu, "Application of Long-Term and Short-Term Memory Neural Network in Technical Evaluation of Hurdle Track and Field," *Security and Communication Networks*, vol. 2022, Article ID 3095032, 11 pages, 2022.

Hindawi
Security and Communication Networks
Volume 2024, Article ID 9816081, 1 page
https://doi.org/10.1155/2024/9816081

Retraction

Retracted: Engineering Management Model Analysis Using Partial Differential Equation Hilbert Space

Security and Communication Networks

Received 8 January 2024; Accepted 8 January 2024; Published 9 January 2024

This article has been retracted by Hindawi following an investigation undertaken by the publisher [1]. This investigation has uncovered evidence of one or more of the following indicators of systematic manipulation of the publication process:

(1) Discrepancies in scope
(2) Discrepancies in the description of the research reported
(3) Discrepancies between the availability of data and the research described
(4) Inappropriate citations
(5) Incoherent, meaningless and/or irrelevant content included in the article
(6) Manipulated or compromised peer review

The presence of these indicators undermines our confidence in the integrity of the article's content and we cannot, therefore, vouch for its reliability. Please note that this notice is intended solely to alert readers that the content of this article is unreliable. We have not investigated whether authors were aware of or involved in the systematic manipulation of the publication process.

In addition, our investigation has also shown that one or more of the following human-subject reporting requirements has not been met in this article: ethical approval by an Institutional Review Board (IRB) committee or equivalent, patient/participant consent to participate, and/or agreement to publish patient/participant details (where relevant).

Wiley and Hindawi regrets that the usual quality checks did not identify these issues before publication and have since put additional measures in place to safeguard research integrity.

We wish to credit our own Research Integrity and Research Publishing teams and anonymous and named external researchers and research integrity experts for contributing to this investigation.

The corresponding author, as the representative of all authors, has been given the opportunity to register their agreement or disagreement to this retraction. We have kept a record of any response received.

References

[1] C. Han, "Engineering Management Model Analysis Using Partial Differential Equation Hilbert Space," *Security and Communication Networks*, vol. 2022, Article ID 5853721, 8 pages, 2022.

Hindawi
Security and Communication Networks
Volume 2024, Article ID 9815745, 1 page
https://doi.org/10.1155/2024/9815745

Retraction

Retracted: Decision Model of Wireless Communication Scheme Evaluation via Interval Number

Security and Communication Networks

Received 8 January 2024; Accepted 8 January 2024; Published 9 January 2024

This article has been retracted by Hindawi following an investigation undertaken by the publisher [1]. This investigation has uncovered evidence of one or more of the following indicators of systematic manipulation of the publication process:

(1) Discrepancies in scope

(2) Discrepancies in the description of the research reported

(3) Discrepancies between the availability of data and the research described

(4) Inappropriate citations

(5) Incoherent, meaningless and/or irrelevant content included in the article

(6) Manipulated or compromised peer review

The presence of these indicators undermines our confidence in the integrity of the article's content and we cannot, therefore, vouch for its reliability. Please note that this notice is intended solely to alert readers that the content of this article is unreliable. We have not investigated whether authors were aware of or involved in the systematic manipulation of the publication process.

Wiley and Hindawi regrets that the usual quality checks did not identify these issues before publication and have since put additional measures in place to safeguard research integrity.

We wish to credit our own Research Integrity and Research Publishing teams and anonymous and named external researchers and research integrity experts for contributing to this investigation.

The corresponding author, as the representative of all authors, has been given the opportunity to register their agreement or disagreement to this retraction. We have kept a record of any response received.

References

[1] M. Li, Y. Ouyang, W. Kang, X. Che, and R. Ye, "Decision Model of Wireless Communication Scheme Evaluation via Interval Number," *Security and Communication Networks*, vol. 2022, Article ID 5916061, 10 pages, 2022.

Hindawi
Security and Communication Networks
Volume 2024, Article ID 9807516, 1 page
https://doi.org/10.1155/2024/9807516

Retraction

Retracted: A Table Tennis Motion Correction System Based on Human Motion Feature Recognition

Security and Communication Networks

Received 8 January 2024; Accepted 8 January 2024; Published 9 January 2024

This article has been retracted by Hindawi following an investigation undertaken by the publisher [1]. This investigation has uncovered evidence of one or more of the following indicators of systematic manipulation of the publication process:

(1) Discrepancies in scope

(2) Discrepancies in the description of the research reported

(3) Discrepancies between the availability of data and the research described

(4) Inappropriate citations

(5) Incoherent, meaningless and/or irrelevant content included in the article

(6) Manipulated or compromised peer review

The presence of these indicators undermines our confidence in the integrity of the article's content and we cannot, therefore, vouch for its reliability. Please note that this notice is intended solely to alert readers that the content of this article is unreliable. We have not investigated whether authors were aware of or involved in the systematic manipulation of the publication process.

Wiley and Hindawi regrets that the usual quality checks did not identify these issues before publication and have since put additional measures in place to safeguard research integrity.

We wish to credit our own Research Integrity and Research Publishing teams and anonymous and named external researchers and research integrity experts for contributing to this investigation.

The corresponding author, as the representative of all authors, has been given the opportunity to register their agreement or disagreement to this retraction. We have kept a record of any response received.

References

[1] L. Han, "A Table Tennis Motion Correction System Based on Human Motion Feature Recognition," *Security and Communication Networks*, vol. 2022, Article ID 7049429, 8 pages, 2022.

Hindawi
Security and Communication Networks
Volume 2024, Article ID 9805652, 1 page
https://doi.org/10.1155/2024/9805652

Retraction

Retracted: Optimization of Substation Alarm Information Processing Based on BP Neural Network

Security and Communication Networks

Received 8 January 2024; Accepted 8 January 2024; Published 9 January 2024

This article has been retracted by Hindawi following an investigation undertaken by the publisher [1]. This investigation has uncovered evidence of one or more of the following indicators of systematic manipulation of the publication process:

(1) Discrepancies in scope

(2) Discrepancies in the description of the research reported

(3) Discrepancies between the availability of data and the research described

(4) Inappropriate citations

(5) Incoherent, meaningless and/or irrelevant content included in the article

(6) Manipulated or compromised peer review

The presence of these indicators undermines our confidence in the integrity of the article's content and we cannot, therefore, vouch for its reliability. Please note that this notice is intended solely to alert readers that the content of this article is unreliable. We have not investigated whether authors were aware of or involved in the systematic manipulation of the publication process.

Wiley and Hindawi regrets that the usual quality checks did not identify these issues before publication and have since put additional measures in place to safeguard research integrity.

We wish to credit our own Research Integrity and Research Publishing teams and anonymous and named external researchers and research integrity experts for contributing to this investigation.

The corresponding author, as the representative of all authors, has been given the opportunity to register their agreement or disagreement to this retraction. We have kept a record of any response received.

References

[1] T. Han, "Optimization of Substation Alarm Information Processing Based on BP Neural Network," *Security and Communication Networks*, vol. 2022, Article ID 6501238, 8 pages, 2022.

Hindawi
Security and Communication Networks
Volume 2024, Article ID 9792589, 1 page
https://doi.org/10.1155/2024/9792589

Retraction

Retracted: Analysis of Risk Assessment of Overseas Infrastructure Projects Integrating BP-ANN Algorithm

Security and Communication Networks

Received 8 January 2024; Accepted 8 January 2024; Published 9 January 2024

This article has been retracted by Hindawi following an investigation undertaken by the publisher [1]. This investigation has uncovered evidence of one or more of the following indicators of systematic manipulation of the publication process:

(1) Discrepancies in scope

(2) Discrepancies in the description of the research reported

(3) Discrepancies between the availability of data and the research described

(4) Inappropriate citations

(5) Incoherent, meaningless and/or irrelevant content included in the article

(6) Manipulated or compromised peer review

The presence of these indicators undermines our confidence in the integrity of the article's content and we cannot, therefore, vouch for its reliability. Please note that this notice is intended solely to alert readers that the content of this article is unreliable. We have not investigated whether authors were aware of or involved in the systematic manipulation of the publication process.

Wiley and Hindawi regrets that the usual quality checks did not identify these issues before publication and have since put additional measures in place to safeguard research integrity.

We wish to credit our own Research Integrity and Research Publishing teams and anonymous and named external researchers and research integrity experts for contributing to this investigation.

The corresponding author, as the representative of all authors, has been given the opportunity to register their agreement or disagreement to this retraction. We have kept a record of any response received.

References

[1] C. Li and J. Zhou, "Analysis of Risk Assessment of Overseas Infrastructure Projects Integrating BP-ANN Algorithm," *Security and Communication Networks*, vol. 2022, Article ID 7864665, 13 pages, 2022.

Hindawi
Security and Communication Networks
Volume 2024, Article ID 9784640, 1 page
https://doi.org/10.1155/2024/9784640

Retraction

Retracted: Anonymization of Quasi-Sensitive Attribute Sets in Aggregated Dataset

Security and Communication Networks

Received 8 January 2024; Accepted 8 January 2024; Published 9 January 2024

This article has been retracted by Hindawi, as publisher, following an investigation undertaken by the publisher [1]. This investigation has uncovered evidence of systematic manipulation of the publication and peer-review process. We cannot, therefore, vouch for the reliability or integrity of this article.

Please note that this notice is intended solely to alert readers that the peer-review process of this article has been compromised.

Wiley and Hindawi regret that the usual quality checks did not identify these issues before publication and have since put additional measures in place to safeguard research integrity.

We wish to credit our Research Integrity and Research Publishing teams and anonymous and named external researchers and research integrity experts for contributing to this investigation.

The corresponding author, as the representative of all authors, has been given the opportunity to register their agreement or disagreement to this retraction. We have kept a record of any response received.

References

[1] Y. Li, S. Yuan, Y. Yuan, C. Chen, and J. Yu, "Anonymization of Quasi-Sensitive Attribute Sets in Aggregated Dataset," *Security and Communication Networks*, vol. 2022, Article ID 9721817, 16 pages, 2022.

Hindawi
Security and Communication Networks
Volume 2024, Article ID 9780872, 1 page
https://doi.org/10.1155/2024/9780872

Retraction

Retracted: A K-Means Clustering Algorithm for Early Warning of Financial Risks in Agricultural Industry

Security and Communication Networks

Received 8 January 2024; Accepted 8 January 2024; Published 9 January 2024

This article has been retracted by Hindawi following an investigation undertaken by the publisher [1]. This investigation has uncovered evidence of one or more of the following indicators of systematic manipulation of the publication process:

(1) Discrepancies in scope

(2) Discrepancies in the description of the research reported

(3) Discrepancies between the availability of data and the research described

(4) Inappropriate citations

(5) Incoherent, meaningless and/or irrelevant content included in the article

(6) Manipulated or compromised peer review

The presence of these indicators undermines our confidence in the integrity of the article's content and we cannot, therefore, vouch for its reliability. Please note that this notice is intended solely to alert readers that the content of this article is unreliable. We have not investigated whether authors were aware of or involved in the systematic manipulation of the publication process.

In addition, our investigation has also shown that one or more of the following human-subject reporting requirements has not been met in this article: ethical approval by an Institutional Review Board (IRB) committee or equivalent, patient/participant consent to participate, and/or agreement to publish patient/participant details (where relevant).

Wiley and Hindawi regrets that the usual quality checks did not identify these issues before publication and have since put additional measures in place to safeguard research integrity.

We wish to credit our own Research Integrity and Research Publishing teams and anonymous and named external researchers and research integrity experts for contributing to this investigation.

The corresponding author, as the representative of all authors, has been given the opportunity to register their agreement or disagreement to this retraction. We have kept a record of any response received.

References

[1] X.-T. Li and X.-H. Duan, "A K-Means Clustering Algorithm for Early Warning of Financial Risks in Agricultural Industry," *Security and Communication Networks*, vol. 2022, Article ID 3751539, 9 pages, 2022.

Hindawi
Security and Communication Networks
Volume 2024, Article ID 9762740, 1 page
https://doi.org/10.1155/2024/9762740

Retraction

Retracted: Statistical Analysis of Employment Education in Colleges and Universities Based on Improved Clustering Algorithm

Security and Communication Networks

Received 8 January 2024; Accepted 8 January 2024; Published 9 January 2024

This article has been retracted by Hindawi following an investigation undertaken by the publisher [1]. This investigation has uncovered evidence of one or more of the following indicators of systematic manipulation of the publication process:

(1) Discrepancies in scope

(2) Discrepancies in the description of the research reported

(3) Discrepancies between the availability of data and the research described

(4) Inappropriate citations

(5) Incoherent, meaningless and/or irrelevant content included in the article

(6) Manipulated or compromised peer review

The presence of these indicators undermines our confidence in the integrity of the article's content and we cannot, therefore, vouch for its reliability. Please note that this notice is intended solely to alert readers that the content of this article is unreliable. We have not investigated whether authors were aware of or involved in the systematic manipulation of the publication process.

Wiley and Hindawi regrets that the usual quality checks did not identify these issues before publication and have since put additional measures in place to safeguard research integrity.

We wish to credit our own Research Integrity and Research Publishing teams and anonymous and named external researchers and research integrity experts for contributing to this investigation.

The corresponding author, as the representative of all authors, has been given the opportunity to register their agreement or disagreement to this retraction. We have kept a record of any response received.

References

[1] B. Liu, "Statistical Analysis of Employment Education in Colleges and Universities Based on Improved Clustering Algorithm," *Security and Communication Networks*, vol. 2022, Article ID 5776831, 12 pages, 2022.

Hindawi
Security and Communication Networks
Volume 2024, Article ID 9759083, 1 page
https://doi.org/10.1155/2024/9759083

Retraction

Retracted: Path Selection Strategy of Communication Network Based on Graph Convolutional Neural Network

Security and Communication Networks

Received 8 January 2024; Accepted 8 January 2024; Published 9 January 2024

This article has been retracted by Hindawi following an investigation undertaken by the publisher [1]. This investigation has uncovered evidence of one or more of the following indicators of systematic manipulation of the publication process:

(1) Discrepancies in scope

(2) Discrepancies in the description of the research reported

(3) Discrepancies between the availability of data and the research described

(4) Inappropriate citations

(5) Incoherent, meaningless and/or irrelevant content included in the article

(6) Manipulated or compromised peer review

The presence of these indicators undermines our confidence in the integrity of the article's content and we cannot, therefore, vouch for its reliability. Please note that this notice is intended solely to alert readers that the content of this article is unreliable. We have not investigated whether authors were aware of or involved in the systematic manipulation of the publication process.

Wiley and Hindawi regrets that the usual quality checks did not identify these issues before publication and have since put additional measures in place to safeguard research integrity.

We wish to credit our own Research Integrity and Research Publishing teams and anonymous and named external researchers and research integrity experts for contributing to this investigation.

The corresponding author, as the representative of all authors, has been given the opportunity to register their agreement or disagreement to this retraction. We have kept a record of any response received.

References

[1] X. Zhang, "Path Selection Strategy of Communication Network Based on Graph Convolutional Neural Network," *Security and Communication Networks*, vol. 2022, Article ID 9548441, 14 pages, 2022.

Hindawi
Security and Communication Networks
Volume 2023, Article ID 9892320, 1 page
https://doi.org/10.1155/2023/9892320

Retraction

Retracted: Construction of University English Informatization Learning Environment Based on ESP Teaching Mode

Security and Communication Networks

Received 19 September 2023; Accepted 19 September 2023; Published 20 September 2023

This article has been retracted by Hindawi following an investigation undertaken by the publisher [1]. This investigation has uncovered evidence of one or more of the following indicators of systematic manipulation of the publication process:

(1) Discrepancies in scope

(2) Discrepancies in the description of the research reported

(3) Discrepancies between the availability of data and the research described

(4) Inappropriate citations

(5) Incoherent, meaningless and/or irrelevant content included in the article

(6) Peer-review manipulation

The presence of these indicators undermines our confidence in the integrity of the article's content and we cannot, therefore, vouch for its reliability. Please note that this notice is intended solely to alert readers that the content of this article is unreliable. We have not investigated whether authors were aware of or involved in the systematic manipulation of the publication process.

Wiley and Hindawi regrets that the usual quality checks did not identify these issues before publication and have since put additional measures in place to safeguard research integrity.

We wish to credit our own Research Integrity and Research Publishing teams and anonymous and named external researchers and research integrity experts for contributing to this investigation.

The corresponding author, as the representative of all authors, has been given the opportunity to register their agreement or disagreement to this retraction. We have kept a record of any response received.

References

[1] L. Feng, "Construction of University English Informatization Learning Environment Based on ESP Teaching Mode," *Security and Communication Networks*, vol. 2022, Article ID 5462618, 12 pages, 2022.

Hindawi
Security and Communication Networks
Volume 2023, Article ID 9854917, 1 page
https://doi.org/10.1155/2023/9854917

Retraction

Retracted: Multitarget Tracking Algorithm in Intelligent Analysis of Football Movement Training Stance

Security and Communication Networks

Received 13 September 2023; Accepted 13 September 2023; Published 14 September 2023

This article has been retracted by Hindawi following an investigation undertaken by the publisher [1]. This investigation has uncovered evidence of one or more of the following indicators of systematic manipulation of the publication process:

(1) Discrepancies in scope

(2) Discrepancies in the description of the research reported

(3) Discrepancies between the availability of data and the research described

(4) Inappropriate citations

(5) Incoherent, meaningless and/or irrelevant content included in the article

(6) Peer-review manipulation

The presence of these indicators undermines our confidence in the integrity of the article's content and we cannot, therefore, vouch for its reliability. Please note that this notice is intended solely to alert readers that the content of this article is unreliable. We have not investigated whether authors were aware of or involved in the systematic manipulation of the publication process.

Wiley and Hindawi regrets that the usual quality checks did not identify these issues before publication and have since put additional measures in place to safeguard research integrity.

We wish to credit our own Research Integrity and Research Publishing teams and anonymous and named external researchers and research integrity experts for contributing to this investigation.

The corresponding author, as the representative of all authors, has been given the opportunity to register their agreement or disagreement to this retraction. We have kept a record of any response received.

References

[1] C. Li and Q. Peng, "Multitarget Tracking Algorithm in Intelligent Analysis of Football Movement Training Stance," *Security and Communication Networks*, vol. 2022, Article ID 6579066, 8 pages, 2022.

Hindawi
Security and Communication Networks
Volume 2023, Article ID 9819712, 1 page
https://doi.org/10.1155/2023/9819712

Retraction

Retracted: Economic Globalization and Corporate Accounting Risks: An Analysis of Enterprise Risk Management Based on Big Data

Security and Communication Networks

Received 8 August 2023; Accepted 8 August 2023; Published 9 August 2023

This article has been retracted by Hindawi following an investigation undertaken by the publisher [1]. This investigation has uncovered evidence of one or more of the following indicators of systematic manipulation of the publication process:

(1) Discrepancies in scope

(2) Discrepancies in the description of the research reported

(3) Discrepancies between the availability of data and the research described

(4) Inappropriate citations

(5) Incoherent, meaningless and/or irrelevant content included in the article

(6) Peer-review manipulation

The presence of these indicators undermines our confidence in the integrity of the article's content and we cannot, therefore, vouch for its reliability. Please note that this notice is intended solely to alert readers that the content of this article is unreliable. We have not investigated whether authors were aware of or involved in the systematic manipulation of the publication process.

Wiley and Hindawi regrets that the usual quality checks did not identify these issues before publication and have since put additional measures in place to safeguard research integrity.

We wish to credit our own Research Integrity and Research Publishing teams and anonymous and named external researchers and research integrity experts for contributing to this investigation.

The corresponding author, as the representative of all authors, has been given the opportunity to register their agreement or disagreement to this retraction. We have kept a record of any response received.

References

[1] Y. Zhang, "Economic Globalization and Corporate Accounting Risks: An Analysis of Enterprise Risk Management Based on Big data," *Security and Communication Networks*, vol. 2022, Article ID 8673357, 11 pages, 2022.

Hindawi
Security and Communication Networks
Volume 2023, Article ID 9865347, 1 page
https://doi.org/10.1155/2023/9865347

Retraction

Retracted: Measurement of Economic Fluctuations Based on High-Frequency Financial Time Series

Security and Communication Networks

Received 8 August 2023; Accepted 8 August 2023; Published 9 August 2023

This article has been retracted by Hindawi following an investigation undertaken by the publisher [1]. This investigation has uncovered evidence of one or more of the following indicators of systematic manipulation of the publication process:

(1) Discrepancies in scope

(2) Discrepancies in the description of the research reported

(3) Discrepancies between the availability of data and the research described

(4) Inappropriate citations

(5) Incoherent, meaningless and/or irrelevant content included in the article

(6) Peer-review manipulation

The presence of these indicators undermines our confidence in the integrity of the article's content and we cannot, therefore, vouch for its reliability. Please note that this notice is intended solely to alert readers that the content of this article is unreliable. We have not investigated whether authors were aware of or involved in the systematic manipulation of the publication process.

Wiley and Hindawi regrets that the usual quality checks did not identify these issues before publication and have since put additional measures in place to safeguard research integrity.

We wish to credit our own Research Integrity and Research Publishing teams and anonymous and named external researchers and research integrity experts for contributing to this investigation.

The corresponding author, as the representative of all authors, has been given the opportunity to register their agreement or disagreement to this retraction. We have kept a record of any response received.

References

[1] H. Zhang, "Measurement of Economic Fluctuations Based on High-Frequency Financial Time Series," *Security and Communication Networks*, vol. 2022, Article ID 9310697, 18 pages, 2022.

Hindawi
Security and Communication Networks
Volume 2024, Article ID 9890863, 1 page
https://doi.org/10.1155/2024/9890863

Retraction

Retracted: A Secure and Efficient Multi-Object Grasping Detection Approach for Robotic Arms

Security and Communication Networks

Received 8 January 2024; Accepted 8 January 2024; Published 9 January 2024

This article has been retracted by Hindawi following an investigation undertaken by the publisher [1]. This investigation has uncovered evidence of one or more of the following indicators of systematic manipulation of the publication process:

(1) Discrepancies in scope

(2) Discrepancies in the description of the research reported

(3) Discrepancies between the availability of data and the research described

(4) Inappropriate citations

(5) Incoherent, meaningless and/or irrelevant content included in the article

(6) Manipulated or compromised peer review

The presence of these indicators undermines our confidence in the integrity of the article's content and we cannot, therefore, vouch for its reliability. Please note that this notice is intended solely to alert readers that the content of this article is unreliable. We have not investigated whether authors were aware of or involved in the systematic manipulation of the publication process.

In addition, our investigation has also shown that one or more of the following human-subject reporting requirements has not been met in this article: ethical approval by an Institutional Review Board (IRB) committee or equivalent, patient/participant consent to participate, and/or agreement to publish patient/participant details (where relevant).

Wiley and Hindawi regrets that the usual quality checks did not identify these issues before publication and have since put additional measures in place to safeguard research integrity.

We wish to credit our own Research Integrity and Research Publishing teams and anonymous and named external researchers and research integrity experts for contributing to this investigation.

The corresponding author, as the representative of all authors, has been given the opportunity to register their agreement or disagreement to this retraction. We have kept a record of any response received.

References

[1] H. Wang, J. Cheng, Y. Xu, S. Ni, Z. Yang, and J. Li, "A Secure and Efficient Multi-Object Grasping Detection Approach for Robotic Arms," *Security and Communication Networks*, vol. 2023, Article ID 7723164, 16 pages, 2023.

Hindawi
Security and Communication Networks
Volume 2023, Article ID 7723164, 16 pages
https://doi.org/10.1155/2023/7723164

Research Article

A Secure and Efficient Multi-Object Grasping Detection Approach for Robotic Arms

Hui Wang,[1,2] **Jieren Cheng**,[1] **Yichen Xu**,[1,2] **Sirui Ni**,[1] **Zaijia Yang**,[1] **and Jiangpeng Li**[1]

[1]*School of Computer Science and Technology, School of Information and Communication Engineering, Hainan University, Haikou, China*
[2]*RobAI-Lab, Hainan University, Haikou, China*

Correspondence should be addressed to Jieren Cheng; cjr22@163.com

Received 18 August 2022; Accepted 10 October 2022; Published 1 June 2023

Academic Editor: Fang Liu

Robot grasping is one of the most important abilities of modern intelligent robots, especially industrial robots. However, most of the existing robot arm's grasp detection work is highly dependent on their edge computing ability, and the safety problems in the process of grasp detection are not considered enough. In this paper, we propose a new robotic arm grasping detection model with an edge-cloud collaboration method. With the scheme of multi-object multi-grasp, our model improves the mission success ratio of grasping. The model can not only complete the compression of full-resolution images but also achieve image compression at a limited bit rate. The image compression ratio reaches 2.03%; the structural difference value is higher than 0.91, and our average detection speed reaches 13.62 fps. Furthermore, we have packaged our model as a functional package of the ROS operating system, which can be easily used in actual robotic arm operations. Our solution can be fully applied to other work of robots to promote the development of the field of robotics.

1. Introduction

Grasping ability is one of the most important abilities of modern intelligent robots, especially for industrial robots, which will bring great power to society [1]. As the most common basic action of robots in work, robotic autonomous grasping has great application prospects. Because of its significance, robotic autonomous grasping has been studied for a long time. Recently, robot grasping has made rapid progress due to the rapid development of deep learning. There are many tasks in robot grasping, including object localization, pose estimation, grasp detection, and motion planning. Among these tasks, grasp detection is a key task in the computer vision and robotics disciplines and has been the subject of considerable research.

However, there are still numerous challenges to this task. On the one hand, the algorithm requires hardware computing power. With the widespread use of deep learning algorithms in grasp detection, deep learning models are deployed directly at the edge (robotic arms). And the hardware computing power is often not well executed, leading to delays and errors in data processing and grasp configuration. At present, most of the robotic arm's grasp detection work is calculated directly at the edge, only with the help of local computing power. This leads to the low efficiency of image detection, and cannot meet the requirements of automatic grasp. On the other hand, security issues in the process of grasp detection are often ignored, leading to the leakage of critical information. In recent years, there are also some studies that try to use cloud computing to solve the problem of insufficient local computing power. They upload the image data directly to the cloud (or fog), and with the help of the cloud's powerful computing power, this way greatly improves the efficiency of grasping. However, the direct transmission of data may lead to the problem of privacy leakage, while the transmission of real-time RGB images is often a major challenge for network bandwidth.

In this work, we propose a robotic arm grasping detection model with an edge-cloud collaboration method. Figure 1

shows the execution flow of our technology model. We use an encoder to compress the images grasped by the camera locally and upload them to the cloud. The uploaded encoded information does not occupy local computing resources, and since it occupies less bandwidth and requires less network configuration, it is more suitable for real scenarios' deployment. In the cloud, our model reconstructs the image by a corresponding decoder, after which it performs a two-stage multi-object grasp detection and returns the obtained grasp configuration to the local side.

The encoding and decoding network of our model is implemented by a GAN (Generative Adversarial Network), which consists of a generator and a discriminator. The generator continuously learns the real image distribution and generates a more realistic image to fool the discriminator. At the same time, the discriminator needs to discriminate the authenticity of the received images. Through the constant confrontation between the generator and the discriminator, they form a min-max game; both sides continuously optimize themselves during the training process until they reach equilibrium. Compared with other methods, GAN can achieve compression for full-resolution images and compression for images with extreme code ratios, which has wide applicability. Also, the reconstructed images have sharper textures and get better picture results. In our model, the decoder is used as the generator and is trained together with the encoder. The customization of the model is very flexible. Besides, it can set the compression ratio by adjusting the feature map size and the number of channels before and after compression. When working, the encoder will be reserved locally, and RGB images will be extracted as feature maps for compression and upload. In the cloud, the images will be reconstructed by the decoder.

The main contribution of this paper is to propose a safe and efficient multi-object grasping detection scheme for robotic arms. This scheme has three advantages:

(1) High fidelity: We have achieved good results on DIV2K, flickr30k, Cornell, and OCID datasets. The compression ratio can be achieved, and the structural loss of the reconstructed image after the transmission is less than 7%, and there is almost no difference in the result of grasp detection before and after compression.

(2) Strong security: Transmitting the compressed tensor to the server instead of the original image. This method avoids the leakage of production information or privacy. Compared with traditional image compression algorithms such as JPEG and JP2000, the uploaded data is difficult to be decrypted and is highly reliable. Theoretically, without the corresponding decoder parameters, there is no way to reconstruct the picture even if the transmission information is intercepted.

(3) High execution efficiency: First, the local side of the operation is offloaded in the cloud, and the limited local arithmetic power is complemented by the arithmetic power provided by the cloud. Second, the compressed information occupies less bandwidth and is transmitted faster. Third, the lightweight neural network fits the actual application scenario.

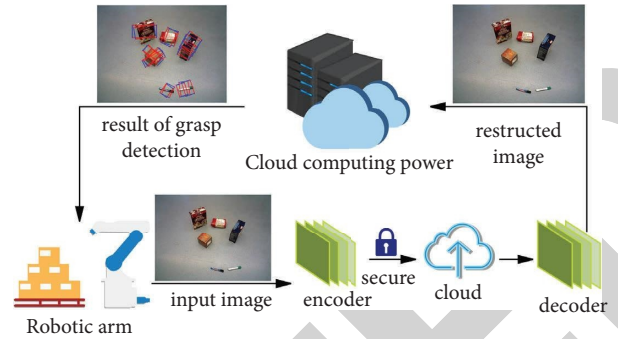


Figure 1: The figure shows how the robot arm unloads the local grasp detection task to the cloud. Our model realizes secure and high-fidelity transmission through this encoder-decoder structure. The image is collected locally, and transmitted to the cloud after being compressed. The reconstructed image will be obtained by the decoder in the cloud. Use cloud computing capabilities to assist in grasp detection and return the results to the robot arm.

2. Related Work

The method of achieving automatic grasping of the robotic arm has been improving over the course of long-term research. The traditional methods of perception-based grasping, reconstructing 3D models of objects, and analyzing the geometric features and forces of models, it has gradually expanded to the use of deep learning network models for image object detection and pose estimation [2].

The work uses the CNN (FAST R-CNN VGG16) network model to complete the pose estimation after image detection. This work proves the practicality of the object in the case of obscuration through experiments [3]. Another work proposes a multimodal model method for image detection using ResNet for RGB, which has better performance than VGG16 [4]. Others use deep learning networks to calibrate and control the behaviour of robotic arms.

Leoni's work is based on the RNN network model; through the sensor data to learn and train the robot's grasping behaviour, thus making sure the system can achieve the goals [5].

Several works use RL technology to optimize and train a robot's gripping ability. After a lot of training, these methods have achieved good experimental results in limited scenes. However, in more complex and practical scenarios, the scalability of RL is still unknown [6].

It is worth noting that the work of Chu et al. [7] on multi-object grasping detection has achieved good results in recent years. Our work is based on the model they proposed.

Due to the demand for computing power in deep learning, the use of cloud edge fog computing is also more applied in robot-related fields. For example, in the work of Sarker et al. [8] the use of offload cloud computing work reduces the energy consumption and hardware requirements of the robot. This treatment reduces a lot of pressure on the hardware part of the robot and the robotic arm.

Kumar et al. [9] builds a cloud computing framework. Through this framework, any robot can call the infinite computing power of the cloud to calculate. Deng et al. [10] proposed a set of invocation algorithms for fog computation. This method can allocate resources more reasonably and efficiently in a limited computing power environment that is closer to the actual situation.

The processing of cloud edge fog often relies on the stability of the connection and relatively high bandwidth. And in practical application scenarios, the compression of images is an essential part.

Some traditional image compression algorithms can achieve certain results in conventional scenes. Dhawan's summary had already analyzed the advantages and disadvantages of methods such as JPEG. However, this method does not present a good direction for further improvement [11].

Compared with traditional algorithms, the direction of image compression using deep learning has yielded many results.

Johannes et al. use the CNN network as a decoder to deal with image compression problems and obtain good theoretical data. This method is processed by the convolutional neural network, which reduces the amount of both computation and image compression data [12]. But in the case of practical applications, end-to-end joint optimization is often difficult to complete high-effect compression and high-quality reconstruction of the image at the same time.

In addition to this, the limited sensory field of the convolutional kernel makes the training often fail to achieve the expectation. This is because the achievement of full-resolution compression tends to increase the difficulty of training network structures.

Toderici et al. use the LSTM network model and the CNN + RNN network model for image compression [13, 14]. And the network model built by using the LSTM network framework is more robust for different pictures. However, experiments have shown that the training of the model is quite complex. Besides, the image correlation relationship cannot be well grasped, and it can only be limited to small-size pictures.

On the other hand, we studied the application of VAE networks in image compression. By increasing the mass ratio factor of VAE, linear proportion and other methods achieved a fairly good compression effect [15, 16]. However, since VAE networks learn the general and original picture by calculating the mean squared error, the resulting image is more likely to have the edge blur problem.

Rippel et al. was the first to propose the application of GAN networks to image compression [17]. The decoded data is processed and generated by using a GAN network, and it is opposed to the discriminator supported by the real data. The model can not only complete the compression of full-resolution images but also achieve image compression at a limited bit rate. This results in a reconstructed image with a clear texture for better visual sensory effects.

A large number of applications of cloud, edge, and fog computing systems have spawned a very urgent information security problem. In [18], for example, the authors analyze the data security issues posed by cloud computing. In addition, the review of Randeep and Jagroo [19] points to the security issues that cloud computing can bring. They summarize techniques for overcoming data privacy issues and define pixel key patterns and image steganography techniques for overcoming data security issues.

Some work [20–22] discussed the security of medical information in cloud storage and data sharing environments and gave some feasible solutions. Overall, these studies highlight the security of information (communications) under the cloud computing system.

To sum up, most of the existing robot arm's grasp detection work is highly dependent on their edge computing ability, and the safety problems in the process of grasp detection are not considered enough.

3. Methodology

The RGB image is grasped by the local camera and sent out by the edge side after encoding and compression. The cloud side receives the data, and then the decoder reconstructs the image for grasp detection. The parameters of the encoder and decoder are obtained using generative adversarial networks for training. Two tasks are completed in the grasp detection phase: grasp proposals and grasp configuration, the former determines the location of the object and the latter configures the grasp angle. The system flowchart is shown in Figure 2 and comprises a number of components, which we will be introduced below.

3.1. Image Compression Part. In this section, we will focus on feature extraction, network architecture design, and customized loss function.

3.1.1. Feature Extraction and Compression. Our model uses global generative compression for image compression. Before encoding and decoding, the input image is first passed through two layers of convolution to achieve feature extraction and image compression. We found that by adjusting the number of feature channels and feature map size output here, we could not only balance the processing speed and image compression quality, but also easily change its compression ratio.

We preprocess the image so that the input image is an RGB image with a height of 210 and a width of 150. The encoded image obtained by the encoder is a feature map of 52×37 of 2, 4, 8, and 16 channels; the corresponding compression ratios are 32.58%, 16.29%, 8.14%, and 4.07%, respectively. The calculation of the compression ratio is given by equation (1). It represents the ratio of the parametric quantities of the output tensor $R^{C_c \times H_c \times W_c}$ to the input image $R^{C_i \times H_i \times W_i}$. The reconstructed images are similar to the original images, whose structural similarity index is greater than 0.93.

$$\text{Compression ratio} = \frac{C_c \times H_c \times W_c}{C_i \times H_i \times W_i} \times 100\%. \quad (1)$$

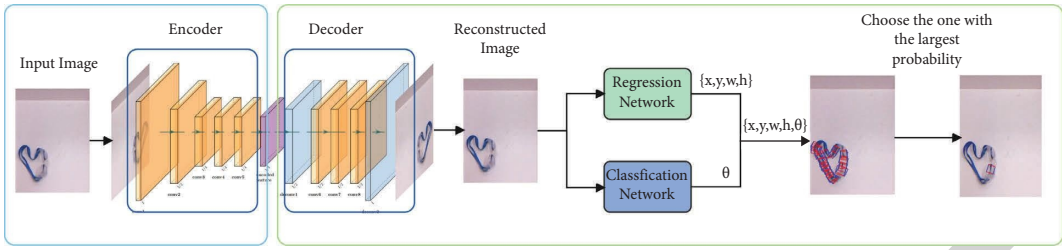


Figure 2: The figure shows the general technical flowchart of our approach. The input image is collected at the edge, compressed by the encoder, and then uploaded to the cloud. The image will be reconstructed by the decoder in the cloud. Then grasp parameters are obtained through classification and regression networks to get the bounding box. According to the probability, the most likely bounding box is selected as the final result of grasp detection. The blue box and green box in the figure represent the edge end and cloud end, respectively.

The number of parameters for different compression ratios is shown in Table 1, and the detailed results under different compression ratios will be given in the experimental section. In Figure 3, we show the reconstructed image results under different compression ratios.

3.1.2. Network Architectures. In order to make the network structure as simple as possible, here we have built a lightweight generator advertising network that is similar to DCGAN [23]. The network consists of a generator and a discriminator. It uses a decoder as a generator and trains the encoder and decoder by using the same loss function in training. During training, the goal of the generator is to try to generate real images to deceive the discriminator. And the goal of the discriminator is to try to separate the images generated by the generator from the real images and then paste the 0 and 1 labels, respectively.

After the encoding stage, we only upload the tensor generated by the encoding network to the cloud without anything else. On the cloud, we use the decoder to restore the tensor to a reconstructed image. In the encoder (compressor network), we used three consecutive layers of simple residual layers (ResNet [24]) for encoding. Correspondingly, in the decoder (decompressor network), the two upsample and three layers of residual layers are crossed, and eventually received a reconstructed image. We implemented upsample with transposed convolution and restored the dimensions of the output picture. In the encoding and decoding network, we use LeakyReLU as the activation function and use Tan*h* in the last layer. In the convolution block during the encoding and decoding phases, we keep the size of the feature map constant by setting the stride and padding, which reduces the loss of information. For the discriminator, we built a simple model based on a combination of convolution and dropout layers.

3.1.3. Loss Function. Generally, in GAN, we tend to use L1 loss (MAE) and L2 loss (MSE) to train discriminators for binary classification problems. However, it cannot be ignored that the simple use of L1 loss for judgment often fails to accurately reflect the level of detail of the image compression and restoration. Structural loss is also a structural loss consideration in image compression tasks. To consider both, we divide the loss function into two parts, namely, the adversarial loss and the structural loss weighting add up to the final loss function.

Table 1: Number of parameters before and after image compression.

Input image	Compressed tensor	Compression ratio (%)
94500	30784	32.58
94500	15392	16.29
94500	7296	8.14
94500	3648	4.07

There are many types of loss functions based on deep learning image algorithms, such as L1 loss and L2 loss. However, for image compression and restoration work, these two loss functions are not easy to recover for the detailed structure of the image and are not enough to intuitively express people's cognitive feelings. In addition, there is also PSNR (peak signal-to-noise ratio) as a common evaluation criterion, but it has a common problem with L1 and L2: their principle is based on pixel-by-pixel comparison differences, without considering human visual perception, so the PSNR index is high, not necessarily representing image quality.

So here we use MSSIM [25] as a structural loss, which is based on SSIM. SSIM is a commonly used image quality evaluation index, which is based on the assumption that the human eye will extract the structural similarity variables when viewing the image. Its final loss value is obtained by comprehensively considering the brightness, contrast, and structural similarity variables. For images x and y, their SSIM is calculated as follows:

$$l(x,y) = \frac{2\mu_x\mu_y + C_1}{\mu_x^2 + \mu_y^2 + C_1}, \tag{2}$$

$$c(x,y) = \frac{2\sigma_x\sigma_y + C_2}{\sigma_x^2 + \sigma_y^2 + C_2}, \tag{3}$$

$$s(x,y) = \frac{\sigma_{xy} + C_3}{\sigma_x\sigma_y + C_3}. \tag{4}$$

In equation (2)–(4), $l(x,y)$ is used to estimate luminance by mean, $c(x,y)$ is used to estimate contrast with variance, and $s(x,y)$ is used to estimate structural similarity with

(a) (b)

Figure 3: Results of reconstructed images: (a) the column is the original image and (b) the three columns are the reconstructed images with 32.58%, 16.29%, and 8.14% compression, respectively.

covariance. The SSIM definition is shown in equation (5), where α, β, and γ are used to adjust the weights of each portion. By default, we set all three of them to 1, and then, we can get equation (6)

$$\mathrm{SSIM}(x, y) = [l(x, y)]^{\alpha} \cdot [c(x, y)]^{\beta} \cdot [s(x, y)]^{\gamma}, \quad (5)$$

$$\mathrm{SSIM}(x, y) = \frac{\left(2\mu_x\mu_y + C_1\right)\left(2\sigma_{xy} + C_2\right)}{\left(\mu_x^2 + \mu_y^2 + C_1\right)\left(\sigma_x^2 + \sigma_y^2 + C_2\right)}. \quad (6)$$

MSSIM takes the reference image and the distortion image as input and divides the image into N blocks by sliding window. Then it will weight the mean, variance, and covariance of each window, and the weight w_{ij} meets the $\sum_{i=0}^{n}\sum_{j=0}^{n} w_{ij}$. We usually use the Gaussian kernel to calculate the structural similarity SSIM of the corresponding block and use the average value as a final structural similarity measure of the two images. Let's suppose the original image is scale 1, and the highest scale is scale M obtained by the M-1 iteration. For the j^{th} scale, only the contrast $c(x, y)$ and the structural similarity $s(x, y)$ will be calculated. Brightness similarity $l(x, y)$ is calculated only in Scale M. The final result is to link the results of the various scales:

$$\mathrm{MSSIM}(x, y) = \left[l_M(x, y)\right]^{\alpha_M} \cdot \prod_{j=1}^{M} \left[c_j(x, y)\right]^{\beta_j} \cdot \left[s_j(x, y)\right]^{\gamma_j}. \quad (7)$$

Hang et al. [26] demonstrates the quality of these loss functions through three experiments. It shows that MSSIM is more appropriate in comparison. In order to make the output image gain higher quality and easier training, here we use the loss function combined with MSSIM and L1 loss.

3.2. Grasp Detection Part. The entire grasp detection task is divided into two tasks: grasp proposals and grasp configuration. The former determines the location of the object, and the latter configures the angle of the grasp.

3.2.1. Grasp Proposals. Grasp proposals are implemented by using the two-stage detection algorithm and consist of two branches: regression and classification. The model chose the ResNet-50 network as the backbone of model. First, the location of the bounding box is determined by regression, which generates the region proposals, avoiding the time-consuming sliding window method and directly predicting the region proposals on the entire image.

These region proposals will make feature extraction through RPN (Region Proposal Network) [27], and the region frame proposals classification is completed when the region frame proposals extraction is performed. The classification process classifies region features into background and object.

When the RPN network generates a region proposal, the position of the object is preliminarily predicted. During this time, the two links of regional classification and location refinement are completed. As soon as it obtains the region proposals, the ROI pooling layer will accurately refine and regress the position of the region proposals.

After the region target corresponds to the features on the feature map, the characteristics of the region proposals will be further represented through a fully connected layer. Later, the category of the region target and the refinement of the region target position will be completed by classification and regression, so the real category of the object will be obtained. While the regression will get the specific coordinate position of the current target, which is represented as a rectangular box represented by four parameters.

3.2.2. Grasp Configuration. The determination of the grasp configuration is achieved through classification. Grasp orientation coordinate θ divides the direction of the grasp into 20 classes and chooses the class directly with the highest confidence level to grasp.

There is a non-grasp direction class in classes. If the confidence level of the output is lower than that of the non-grasp direction class, this grasp recommendation is considered to be ungraspable in that direction. Setting non-

grasp classes instead of setting specific thresholds will be a better way to handle multi-object and multi-grasp component tasks.

The final output is shown in Figure 4. In the figure's output bounding box, the red line represents the open length of a two-fingered gripper, while the blue line represents the parallel plates of the gripper.

In this scheme, the loss function is designed to be two parts: the grass proposal loss L_{gpn} and the grasp configuration loss $L_{\text{gcr\_reg}}$. As shown in equation (7), $L_{\text{gp\_cls}}$ is the cross-entropy loss of the grasp direction classification, and the $L_{\text{gp,eg}}$ and weight λ are the L1 regression loss of the grasp recommendation. In the case of no grasping, $p_i^* = 0$. Correspondingly, the $p_i^* = 1$ when it can be grasped. The parameter t_i^*, and p_i^* are corresponding to the ground truth.

$$L_{\text{gpn}}\left(\left\{(p_i, t_i)_{i=1}^{\text{I}}\right\}\right) = \sum_i L_{gp\_cls}(p_i, p_i^*) + \lambda \sum_i p_i^* L_{gp\_reg}(t_i, t_i^*). \tag{8}$$

Equation (8) defines the loss function that executes the fetch configuration prediction. In this equation, $L_{\text{gp\_cls}}$ is the cross-entropy loss of the grasp orientation classification, and ρ_l is the confidence level of each classification. $L_{\text{gcr\_reg}}$ is the regression loss of the bounding box, and the β_c records the corresponding prediction of the grasp bounding box. β_c^* is the correct bounding box. λ_2 is the relative weight.

$$L_{\text{gpn}}\left(\left\{(\rho_l, \beta_l)_{i=1}^{\text{C}}\right\}\right) = \sum_i L_{gcr\_cls}(p_l) + \lambda_2 \sum_c 1_{c\neq 0}(c) L_{gcr\_reg}(\beta_i, \beta_i^*). \tag{9}$$

The total loss consists of the addition of L_{gpn} and $L_{\text{gcr\_reg}}$, as shown in equation (9):

$$L_{\text{total}} = L_{\text{gpn}} + L_{\text{gcr}}. \tag{10}$$

4. Experimental

4.1. Experimental Environment. The training environment of the model is an Intel (R) Xeon (R) platinum 8255c, 47 GB memory, 12 cores computer equipped with 24 g video memory GeForce RTX™ 3090 graphics card. The computer system environment is the Ubuntu 20.04 operating system. Later, the test experiment was conducted on another GeForce RTX ™ 2080 Ti graphics card.

4.2. Dataset and Data Preprocessing. We used the Flickr30k [28] dataset alone for training the image compression reconstruction, and then validated on all four datasets, Flickr30k, DIV2k [29], Cornell [30], and OCID [31]. The image reconstruction achieved good results on both PSNR and SSIM values. The grasping training and validation were then performed using the OCID dataset with 92% accuracy in general.

Figure 4: Results of grasp detection output. The red line represents the open length of a two-fingered gripper, while the blue line represents the parallel plates of the gripper.

Flickr30k: Flickr30k is the first image description dataset that contains 158,915 descriptions and 31,783 images. This dataset is based on the previous Flickr8k dataset and focuses on describing everyday human activities. Of these, 25,426 images were used for training, and 6,357 images each were used for validation and testing.

Div2k: The DIV2K dataset is a commonly used dataset for superresolution image reconstruction. The dataset contains 1000 2K resolution images, including 800 training images, 100 validation images, and 100 test images. And the low-resolution images with 2, 3, 4, and 8 reduction factors are provided.

Cornell: The Cornell grasping dataset is a required dataset for robotic autonomous grasping tasks. The dataset contains 885 RGB-D images of 640×480 px size with 240 graspable objects. The correct grasping candidate is given by a manually annotated rectangular box. Each object corresponds to multiple images with different orientations or poses, and each image is labelled with multiple ground truth grasps, corresponding to the many possible ways of grasping the object.

OCID: We use the OCID_grasp dataset part, which is composed of 1763 selected RGB-D images, of which there are more than 75,000 hand-annotated grasp candidates.

4.3. Training Schedule. We train the whole network for 10 epochs on a single GeForce RTX™ 3090. The initial learning ratio is set to 0.0002. The batch size is set to 30, and the log is output every 50 batches. The input image is first cropped to 210×160 sizes.

4.4. Evaluation Metric

4.4.1. Compressed Image Quality Metrics. PSNR (peak-signal-to-noise ratio) PSNR is defined as equation (11), MAX_I^2 which is the maximum possible pixel value of the image, and MSE is the mean square error of each pixel point of the two images. The minimum value of PSNR is 0, and the larger the PSNR, the smaller the difference between the two images. We test 100 images and finally take the average as the final value.

$$\text{PSNR} = 10 \cdot \log_{10}\left(\frac{\text{MAX}_I^2}{\text{MSE}}\right). \tag{11}$$

SSIM (Structure Similarity Index Measure) equation (6) is the definition of SSIM. SSIM is based on the assumption that the human eye extracts structured information from an image and integrates the differences between two images in terms of luminance, contrast, and structure. SSIM ≤ 1, the larger the SSIM, the more similar the two images are. We test 100 images and finally take the average as the final value.

4.4.2. Grasping Accuracy Metrics. The accuracy of the grasping parameters is evaluated by comparing the closeness of the grasp candidate to ground truth.

A grasp candidate is considered as successful grasp detection after satisfying the following two metrics:

(1) The difference between the angle of predicted grasp g_p and ground truth g_t does not exceed 30°

(2) Intersection over Union (IoU) of g_p and g_t is greater than 25%, which means

$$\text{IoU} = \frac{\left|g_p \cap g_t\right|}{\left|g_p \cup g_t\right|} > 0.25. \tag{12}$$

4.5. Comparative Experiment

4.5.1. Image Compression Quality Experiment. We conducted compression encoding experiments on the pictures of the Flickr30k, Cornell, and DIV2K datasets, respectively. The encoding tensor sizes obtained under different datasets and different compression ratios are shown in Table 2. The data in Table 2 shows that the magnitude of the compression tensor is proportional to the compression ratio and satisfies the previously derived formula to present a linear relationship.

We select 200 images from each of the three datasets of the Flickr30k, Cornell, and DIV2K, and divide them into 2 : 3 batches according to the complexity of the images. The reconstructed image is compared with the original image at different compression ratios. The reconstructed image is compared with the original image at different compression ratios. We get their PSNR and SSIM values and average them to get Tables 3 and 4. The data in Tables 3 and 4 show that our model has achieved good results under picture inputs of different complexity. The average values of PSNR and SSIM reached 35.576 and 0.948, respectively.

In Tables 3 and 4, we use eleven compression ratios to test the image compression and reconstruction effects under different compression ratios. The results show that when the compression ratio is above 4.07%, the accuracy will not decrease too much with the decrease of the compression ratio. When the compression ratio is 2.03% or less, the loss gradually manifests. The results show that our model has strong feature extraction ability and a large range of customizable compression ratios.

With the increase of the compression ratio, the image reconstruction quality increases sublinearly and finally tends to a higher value. From the comparison of eleven groups of values, it can be seen that by weighing the compression ratio and image quality, from the image reconstruction quality index, 8.14% and 16.29% are the best compression ratio settings of the network. The data in the table shows that the SSIM value of image reconstruction on the three datasets is greater than 0.82 under these two radios. The Cornell dataset in the actual grasping environment has the highest score, with a PSNR of 31.768 and an average SSIM of 0.948, which is sufficient to meet the needs of grasping. However, in the actual process of grasping and detecting, the requirements for images are not the same as those for human eyes. We will conduct further experiments in combination with grasping in the two experiments of the grasp detection accuracy experiment and the network architecture experiment.

Table 2: Output tensor size of the encoder with different compression ratios.

Compression ratio (%)	Flickr30k (kB)	Cornell (kB)	DIV2K (kB)
2.03	15.5	74.8	74.8
4.07	30.3	148	148
8.14	60	297	297
16.29	119	593	593
32.58	237	1187	1187

4.5.2. Grasp Detection Accuracy Experiment. In order to evaluate the effect of encoding and decoding on grasp detection, we compared the results of grasping detection using the original image and the reconstructed image. The results are shown in Figure 5.

We can see from Figure 5 that under the compression ratio of 8.14%, the accuracy does not decrease too much after being compressed. At the same time, the processing speed of our grasp detection algorithm can reach 13.62 fps in the implementation environment.

The Cornell dataset provides images and grasp labels from multiple angles of each object. We carry out the grasp detection experiment based on the same object from multiple angles. Figure 6 shows the effect. Our model can accurately mark the bounding box at different angles.

We detect the accuracy of the multi-object grasp task in the environment of a single object, less than ten objects, and more than ten objects. Count the number of successful grasp detections and calculate the grasp accuracy. The results are shown in Table 4. The results show that when the number of objects is less than 5, our model can basically achieve 100% error-free detection on the OCID dataset. Figure 7 shows the performance of our model on the OCID dataset.

4.5.3. Network Architectures Experiment. In order to reasonably design the parameters of the neural networks, we carried out parameter optimization experiments from the two dimensions of network depth and the number of channels.

We designed different models with two, three, and five convolution blocks of network architectures respectively for image reconstruction experiments. The results are shown in Figure 8 and Table 5, to compare the effect of the number of

Table 3: PSNR of different dataset.

Compression ratio (%)	DIV2K			Flickr30K			Cornell		
	High complexity	Low complexity	Average	High complexity	Low complexity	Average	High complexity	Low complexity	Average
32.58	24.48	30.31	27.98	21.31	29.78	26.392	34.785	36.10	35.5
16.29	24.885	30.26	28.108	22.29	29.56	26.652	31.41	32.01	31.768
8.14	24.16	29.31	27.248	21.82	28.31	25.714	29.93	30.41	30.216
4.07	22.265	27.98	25.692	19.7	25.85	23.39	31.57	32.66	32.226
2.03	19.515	24.44	22.472	19.52	24.44	22.472	26.875	27.91	27.496
0.99	18.255	22.67	20.9	17.31	22.34	20.328	29.535	30.44	30.078
0.50	15.55	20.51	18.528	15.91	19.02	17.776	24.38	26.86	25.866
0.13	15.175	18.92	17.422	14.90	18.45	17.03	22.49	24.26	23.552
0.06	16.225	21.21	19.218	15.46	18.49	17.276	19.475	19.11	19.254
0.04	13.09	16.41	15.084	14.26	17.91	16.446	11.915	11.43	11.626
0.03	10.875	14.99	13.344	12.24	13.59	13.05	11.915	11.43	11.626

Table 4: SSIM of different dataset.

Compression ratio (%)	DIV2K			Flickr30K			Cornell		
	High complexity	Low complexity	Average	High complexity	Low complexity	Average	High complexity	Low complexity	Average
32.58	0.83	0.86	0.86	0.75	0.85	0.81	0.945	0.95	0.948
16.29	0.835	0.89	0.868	0.78	0.86	0.828	0.945	0.95	0.948
8.14	0.805	0.87	0.846	0.75	0.82	0.792	0.945	0.95	0.948
4.07	0.66	0.81	0.752	0.64	0.87	0.778	0.935	0.94	0.938
2.03	0.48	0.7	0.612	0.51	0.78	0.672	0.905	0.92	0.914
0.99	0.545	0.61	0.586	0.47	0.59	0.542	0.885	0.89	0.888
0.50	0.365	0.46	0.422	0.49	0.6	0.556	0.845	0.87	0.858
0.13	0.33	0.43	0.39	0.35	0.48	0.428	0.825	0.83	0.83
0.06	0.405	0.49	0.458	0.37	0.53	0.466	0.77	0.80	0.79
0.04	0.27	0.34	0.312	0.305	0.478	0.408	0.555	0.56	0.556
0.03	0.225	0.29	0.262	0.23	0.35	0.302	0.555	0.56	0.556

encoder-decoder network layers on the model effect. By comparing these figures and tables, it can be concluded that the reconstructed image of the three-layer convolution block model is better than that of the two-layer coding block network. However, for the five-layer network, considering the operation speed and guarantee ratio, we think that three layers are the better network layers.

Comparison of reconstructed image quality under different channel numbers is shown in the appendix. The image is blurred at a low compression ratio, but it can still be detected and judged. With the increase in compression ratio, the result of grasp detection is close to the original image. The three lines from top to bottom are the input image, the reconstructed image, and the result with the label. It can be concluded from these five groups of pictures that the compression ratio of 0.13% and above is similar to the original picture, which can ensure the accuracy of grasping.

Cornell datasets are all composed of a single object target, which is less difficult to grasp. To further refine our choice of compression ratio, we performed the same experiment on the multi-object grasp dataset, OCID. In the case of fewer objects and fewer stacking occlusions, the grasping detection accuracy does not change too much with the reduction of the compression ratio. However, when the number of objects increases and numerous stacks appear, the influence of different compression ratios on the results gradually appears. As shown in Figure 9 the first line is the result of the grasp detection of the original image, and the eight lines below are the results under the compression ratios of 16.29%, 4.07%, 0.99%, 0.5%, 0.13%, 0.05%, 0.04%, and 0.03% (additional images are shown in figure *X* in the appendix). When the compression ratio is relatively large, the reduction of the compression ratio does not mean the reduction of the accuracy. In some cases, the interference of impurities may even be eliminated to improve the accuracy of grasping detection. However, we can clearly see that when the compression ratio is reduced to 0.5%, it is difficult to distinguish the stacked occluded objects. When the compression ratio reaches 0.03% of the limit, it is impossible to perform grasping detection. Therefore, we think that the compression ratio of at least 0.5% should be selected for multi-object grasp detection.

In conclusion, we can draw a conclusion. In the case of a single object or objects without stack occlusion, the compression ratio of 0.13% or above has high accuracy. In a complex scene where multiple objects or objects are stacked and blocked, a compression ratio of 0.5% or above is required.

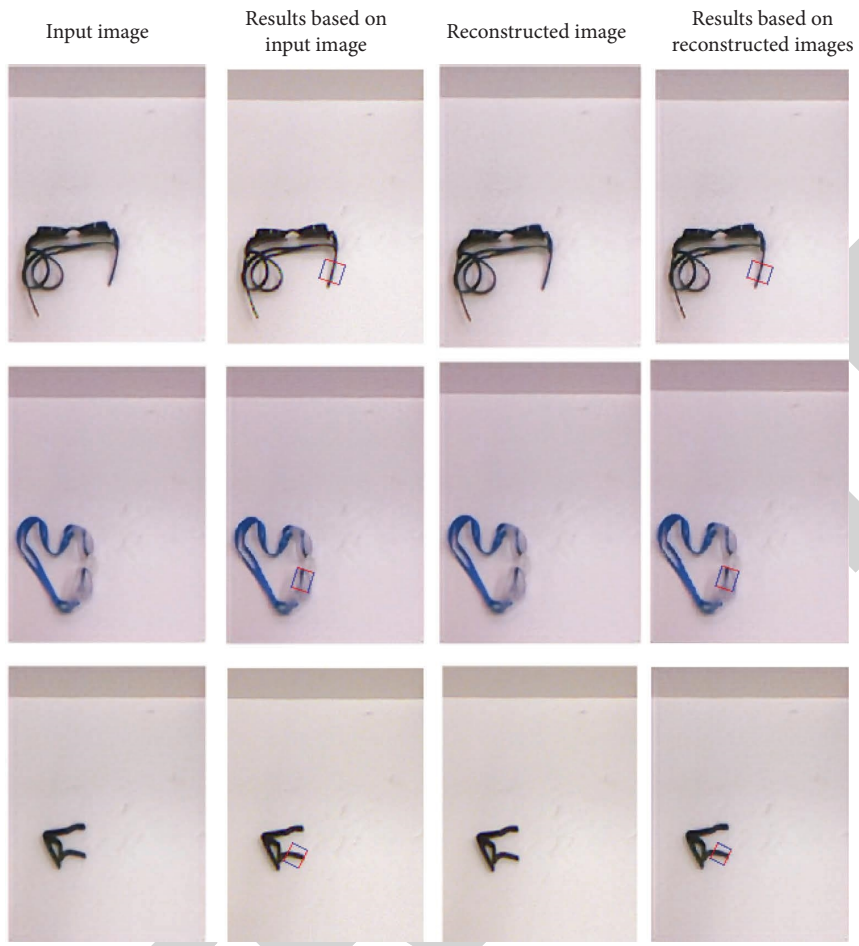


Figure 5: The first column is the original input pictures. The second column is the result of grasp detection based on the original image. The third column shows the compressed and reconstructed image. The fourth column is the result of the grasp detection based on the compressed and reconstructed image. It can be seen from the figure that the loss of compression accuracy is little, and grasping accuracy has not been greatly affected.

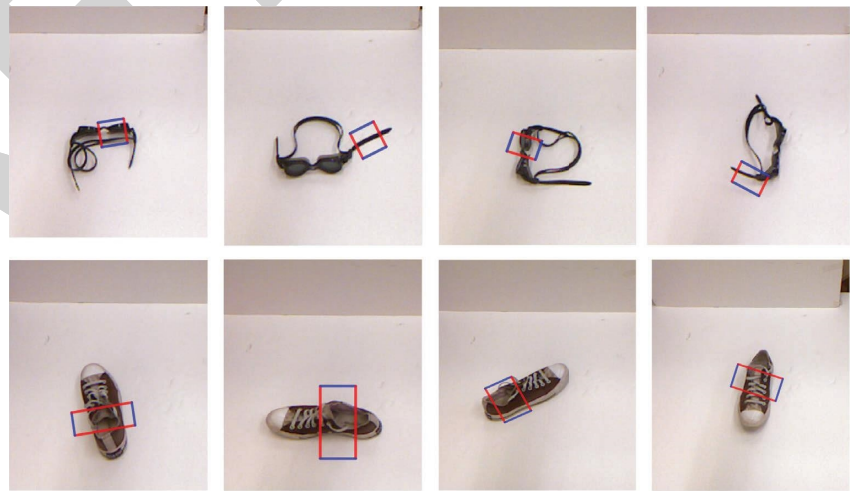


Figure 6: Grasp detection experiment based on the same object from multiple angles. The figure shows that our model can accurately mark the bounding box in different directions.

Figure 7: Performance of our model on the OCID dataset. In the output bounding box, the red line represents the open length of a two-fingered gripper, while the blue line represents the parallel plates of the gripper.

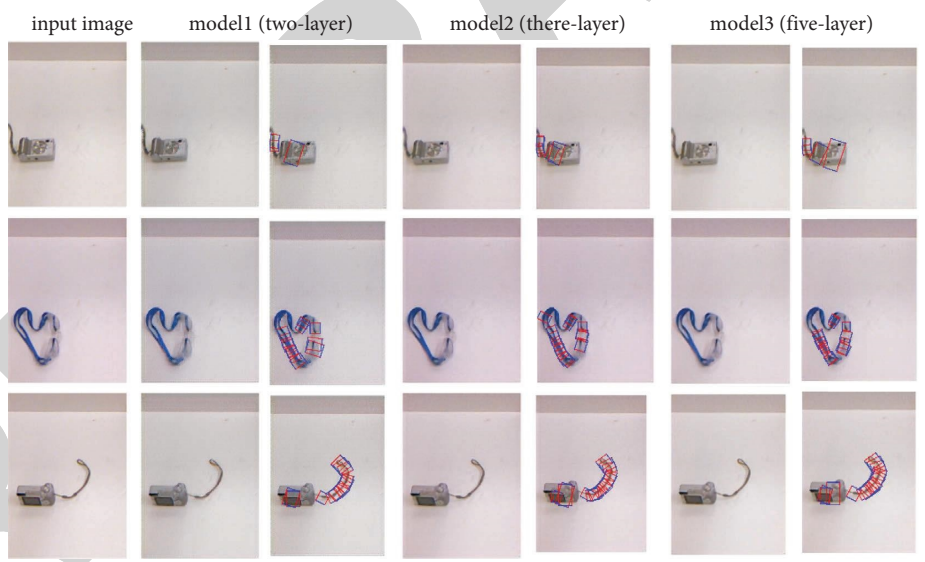


Figure 8: Reconstruction and grasp detection result of different models. As the number of convolution layers increases, feature extraction becomes more sufficient, and the quality of reconstructed pictures becomes better.

4.5.4. Changing Uplink Rate Environment Experiment. In practical application situations, the network environment often fluctuates and brings bandwidth changes. With the deterioration of the network environment, the network transmission delay will increase. This makes it necessary for us to choose flexibly among various schemes according to the actual situation. We design experiments to verify how to choose under different network speed conditions.

There are several schemes in the experiment:

(a) Pure Edge Offloading (EO): All received pictures will be transmitted to the edge server for calculation and then the data will be returned to the local.

(b) Pure On-device Processing (MO): All the received frames will be directly calculated locally and will not be transmitted to the server.

Table 5: Comparison of different models.

Number of convolution layers	PSNR	SSIM
2-layer	28.346	0.9
3-layer	31.768	0.948
5-layer	35.438	0.952

Figure 9: The first line is the result of the grasp detection of the original image, and the lines below are the results under the compression ratio of 16.29%, 4.07%, 0.99%, 0.5%, 0.13%, 0.05%, 0.04%, and 0.03%. From top to bottom, the loss of pictures due to compression gradually increases, which slowly affects the bounding box results of grasp detection.

(c) Collaborative scheme (Collaboration): Preprocess the acquired image locally by encoding and compression, then transmit it to the edge for calculation and finally return to the mobile device.

(d) Our model: According to the real-time uplink network speed, improve the grasp scheme and select the optimal scheme under different network speeds.

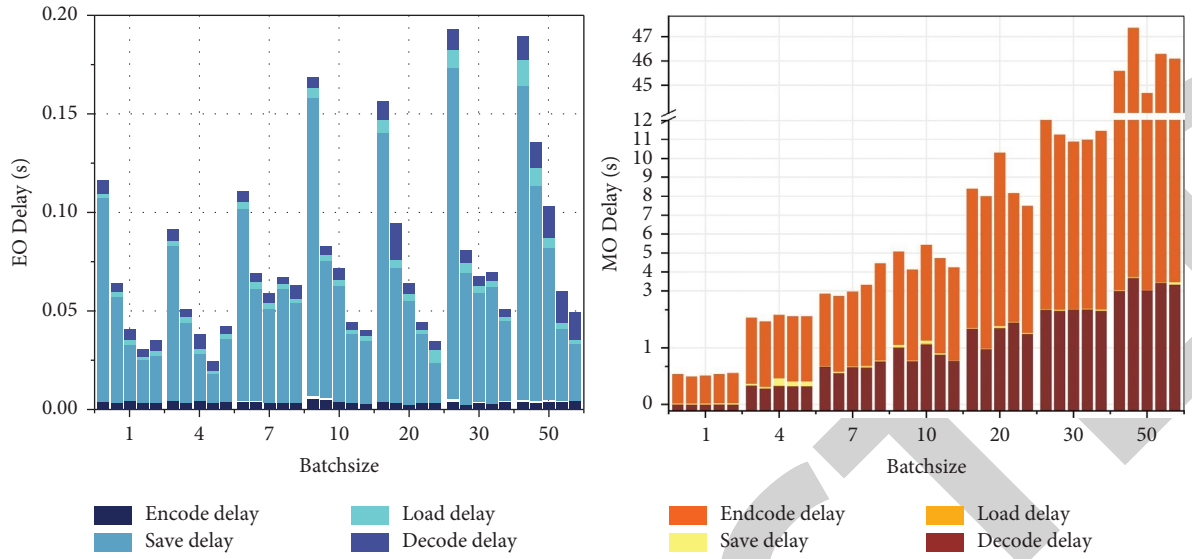


Figure 10: Delay under EO and MO. The overall delay consists of four parts: encode delay, save delay, load delay, and decode delay.

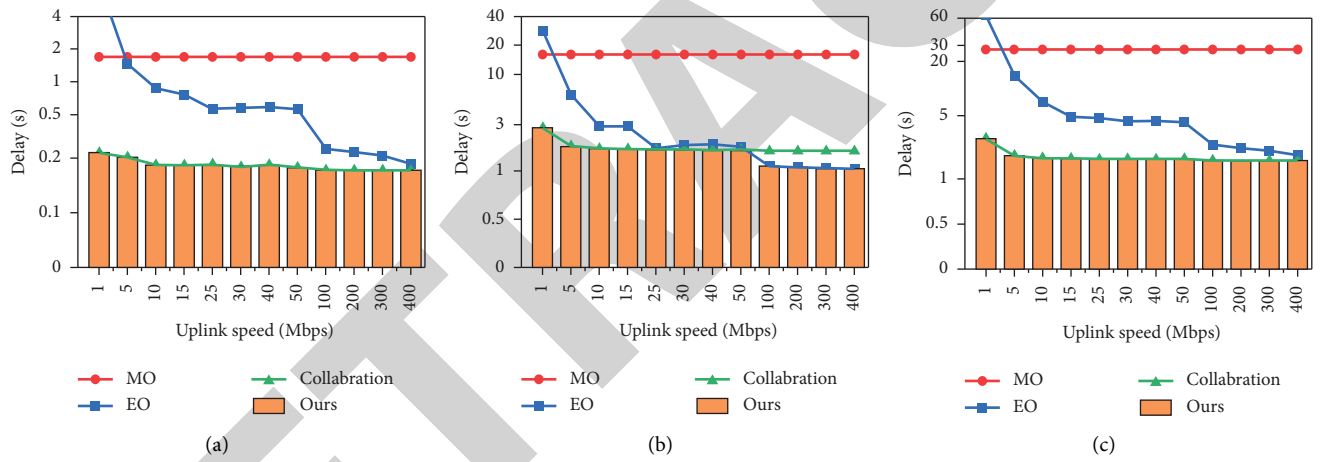


Figure 11: Comparison of the overall delay time of four schemes under different network bandwidths. From (a) to (c), the overall delay time for batch sizes of 1, 4, 10 is shown in sequence.

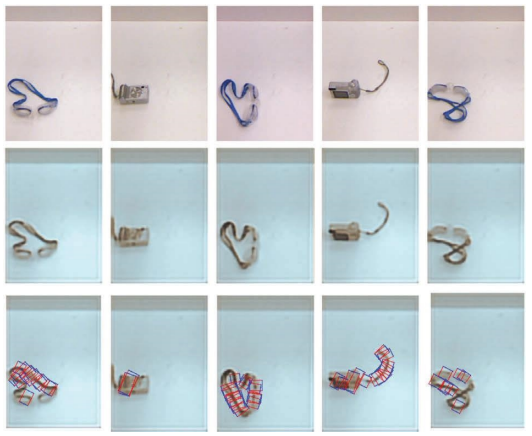


Figure 12: Grasp detection result under 0.2% compression ratio. Under this compression ratio, the grasp detection has high accuracy.

Figure 13: Grasp detection result under 0.13% compression ratio. The image is blurred, but it can still be used for grasp detection.

Figure 14: Grasp detection result under 0.06% compression ratio. The loss of image reconstruction becomes large, and some objects cannot be correctly recognized.

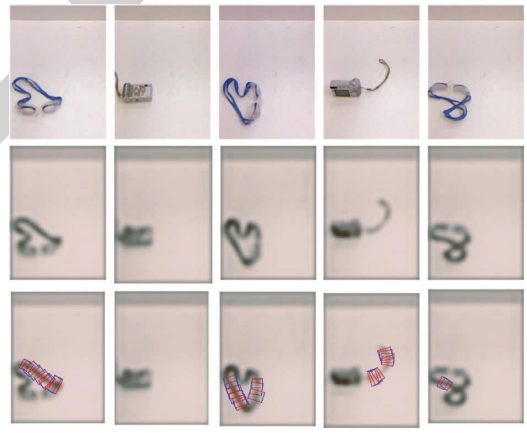


Figure 15: Grasp detection result under 0.05% compression ratio. The image is more blurred, but most objects can still be grasped correctly.

We test the delay on different devices and get Figure 10. The x-axis in the figure represents the number of file frames transmitted in a batch, the compression rate in each group decreases in turn, and the y-axis is the delay time. EO in Figure 10 shows that the time for encoding on the CPU is much less than that for decoding. MO in Figure 10 shows that the decoding speed on the GPU is faster so that the reconstruction takes less time than the loading and saving operation of the model. It can be seen that encoding on the CPU and decoding on the GPU are feasible and can make

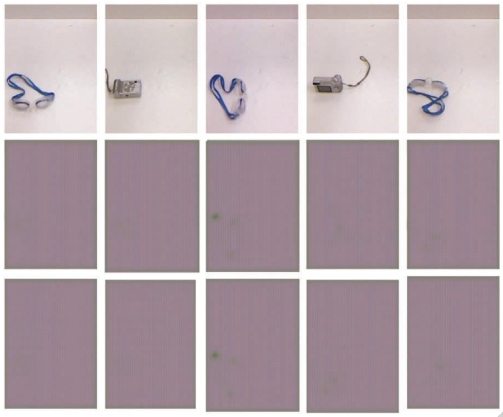


Figure 16: Grasp detection result under 0.04% compression ratio. At this compression ratio, single-object grasp detection cannot be performed.

Figure 17: The first line is the result of the grasp detection of the original image, and the lines below are the results under the compression ratio of 16.29%, 4.07%, 0.99%, 0.5%, 0.13%, 0.05%, 0.04%, and 0.03%. From top to bottom, the loss of pictures due to compression gradually increases, which slowly affects the bounding box results of grasp detection.

good use of resources. In order to increase efficiency, we explore the impact of the number of frames transmitted at the same time on latency. It is worth noting that the delay of mobile devices fluctuates greatly due to the number of files. The lower compression rate and the smaller tensor volume are beneficial to speed up the loading of the data obtained by the edge server.

We chose a fixed compression rate of 2.03% for transmission experiments under different network bandwidths. Figure 10 shows the delay rates of the four schemes under different network bandwidths. It can be seen that the effects of EO and MO vary greatly in different network conditions. The collaboration method can achieve a balanced result between the two. In most cases, the collaboration method can already achieve a good effect and greatly improve the latency of other solutions. However, in some cases, as shown in Figure 11, when the delay of file transfer does not become the key factor, it is possible that EO and MO will achieve better results than the collaboration scheme. So we established a linear model to switch between these three network models, seeking results that are more suitable for multiple factors and situations.

5. Conclusion

We propose a new grasping detection model and perform grasping detection in RGB images. With the scheme of multi-object multi-grasp, our model improves the mission success ratio of grasping. With the help of edge-cloud collaboration, the computing task is transferred to the cloud with powerful computing power, which greatly improves the speed and accuracy of grasp detection. The encoder and decoder trained by GAN enable the image to be encrypted while compressing, ensuring the security of privacy. The model proves that the combination of autonomous robot grasping and edge-cloud collaboration has great prospects. The model achieves 92% accuracy on the OCID dataset, the image compression ratio reaches 2.03%, the structural difference value is higher than 0.91, and the average detection speed reaches 13.62 fps. Furthermore, we have packaged our model as a functional package of the ROS operating system, which can be easily used in actual robotic arm operations. In the future, we will improve compression, and refine the distribution of tasks between on-premises and the cloud to further improve the efficiency of the model. At the same time, our solution can be fully applied to other work of robots to promote the development of the field of robotics. This work is also potential in some other fields, such as federated learning [32–34], cloud-edge cooperate robotics [35, 36], data collection [37], and smart city.

Appendix

A. Grasp Detection Result under Different Compression Ratios

The comparison of reconstructed image quality under different channel numbers is shown in Figures 12–16. The three lines from top to bottom are the input image, the reconstructed image, and the labelled result. By comparing these five groups of images, it is proven that in a single object grasping task, a low compression ratio can still achieve good results. Until the compression ratio is as low as 0.06%, it begins to appear that the detected object cannot be recognized and grasped. The results of the multi-object grasp detection task are shown in Figure 17.

Data Availability

All data included in this study are available from the first author or corresponding author upon reasonable request.

Conflicts of Interest

The authors declare that there are no conflicts of interest.

Acknowledgments

This work was supported by Hainan Provincial Natural Science Foundation of China (Grant No. 620MS021), the Key Research and Development Program of Hainan Province (Grant No. ZDYF2021GXJS003, ZDYF2020040), the Major Science and Technology Project of Hainan Province (Grant No. ZDKJ2020012), National Natural Science Foundation of China (NSFC) (Grant No. 62162022, 62162024), the Key Laboratory of PK System Technologies Research of Hainan, Science and Technology Development Center of the Ministry of Education Industry-University-Research Innovation Fund (2021JQR017).

References

[1] J. Sanchez, J.-A. Corrales, B.-C. Bouzgarrou, and Y. Mezouar, "Robotic manipulation and sensing of deformable objects in domestic and industrial applications: a survey," *The International Journal of Robotics Research*, vol. 37, no. 7, pp. 688–716, 2018.

[2] A. Bicchi and V. Kumar, "Robotic grasping and contact: A review," in *Proceedings 2000 ICRA Millennium conference IEEE international conference on robotics and automation. Symposia proceedings (Cat. No. 00CH37065)*, pp. 348–353, San Francisco, CA, USA, April 2000.

[3] C. Zhihong, Z. Hebin, W. Yanbo, L. Binyan, and L. Yu, "A vision-based robotic grasping system using deep learning for garbage sorting," in *Proceedings of the 36th Chinese control conference (CCC)*, pp. 11 223–11 226, Dalian, China, July 2017.

[4] S. Kumra and C. Kanan, "Robotic grasp detection using deep convolutional neural networks," in *Proceedings of the IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS)*, pp. 769–776, Vancouver, BC, Canada, September 2017.

[5] F. Leoni, M. Guerrini, C. Laschi, D. Taddeucci, P. Dario, and A. Starita, "Implementing robotic grasping tasks using a biological approach," in *Proceedings. 1998 IEEE International Conference on Robotics and Automation (Cat. No.98CH36146)*, pp. 2274–2280, Leuven, Belgium, May 1998.

[6] D. Quillen, E. Jang, O. Nachum, C. Finn, J. Ibarz, and S. Levine, "Deep reinforcement learning for vision-based robotic grasping: A simulated comparative evaluation of off-policy methods," in *Proceedings of the IEEE International*

Hindawi
Security and Communication Networks
Volume 2023, Article ID 9819712, 1 page
https://doi.org/10.1155/2023/9819712

Retraction

Retracted: Economic Globalization and Corporate Accounting Risks: An Analysis of Enterprise Risk Management Based on Big Data

Security and Communication Networks

Received 8 August 2023; Accepted 8 August 2023; Published 9 August 2023

This article has been retracted by Hindawi following an investigation undertaken by the publisher [1]. This investigation has uncovered evidence of one or more of the following indicators of systematic manipulation of the publication process:

(1) Discrepancies in scope

(2) Discrepancies in the description of the research reported

(3) Discrepancies between the availability of data and the research described

(4) Inappropriate citations

(5) Incoherent, meaningless and/or irrelevant content included in the article

(6) Peer-review manipulation

The presence of these indicators undermines our confidence in the integrity of the article's content and we cannot, therefore, vouch for its reliability. Please note that this notice is intended solely to alert readers that the content of this article is unreliable. We have not investigated whether authors were aware of or involved in the systematic manipulation of the publication process.

Wiley and Hindawi regrets that the usual quality checks did not identify these issues before publication and have since put additional measures in place to safeguard research integrity.

We wish to credit our own Research Integrity and Research Publishing teams and anonymous and named external researchers and research integrity experts for contributing to this investigation.

The corresponding author, as the representative of all authors, has been given the opportunity to register their agreement or disagreement to this retraction. We have kept a record of any response received.

References

[1] Y. Zhang, "Economic Globalization and Corporate Accounting Risks: An Analysis of Enterprise Risk Management Based on Big data," *Security and Communication Networks*, vol. 2022, Article ID 8673357, 11 pages, 2022.

Hindawi
Security and Communication Networks
Volume 2022, Article ID 8673357, 11 pages
https://doi.org/10.1155/2022/8673357

Review Article

Economic Globalization and Corporate Accounting Risks: An Analysis of Enterprise Risk Management Based on Big Data

Yantai Zhang

School of Economics and Trade, Henan Polytechnic Institute, Nanyang, Henan 473000, China

Correspondence should be addressed to Yantai Zhang; 1992003@hnpi.edu.cn

Received 8 June 2022; Revised 22 July 2022; Accepted 29 July 2022; Published 14 October 2022

Academic Editor: Zhiping Cai

Economic globalization has become an unavoidable result of the rapid development of global economy. However, while economic globalization brings speed development and convenience to businesses, it also brings risks and challenges. With the advancement of network technology, Big Data has become increasingly intertwined with people's lives. Big Data is gradually being applied to the method of people's lives, in business, medical care, science and technology, production, and life. The production of Big Data for enterprises provides a large amount of data and information analysis library and for the management of enterprises provides a lot of convenience. Business management has also changed with the addition of big data. It is the top priority of enterprise development and survival to cope with the current economic and information globalization era which brings hidden dangers and risks. Based on the background of economic globalization and Big Data, this study analyzes the importance of enterprise risk management in the context of Big Data. This study mainly adopts the literature method and survey method to summarize what problems exist in enterprise risk management, highlights the causes of the problems in enterprise risk management, and gives corresponding solutions according to the existing problems. This paper aims at the study of enterprise risk management in the big environment, hoping to have certain suggestions and guidance for the relevant enterprises.

1. Introduction

As the term "economic globalization" suggests, the world's economies have started to interact and integrate, but this process is abstract and complex in nature. Economic globalization is a byproduct of the prompt productivity growth and is ultimately caused by it [1, 2]. As economic globalization continues to advance, a greater number of its byproducts are visible in our daily lives and increasingly permeate our production processes. Economic globalization has greatly facilitated people's lives, from importing and exporting national energy to the smallest necessities in supermarkets. However, there are also risks; for instance, due to economic globalization, developing countries may become richer while underdeveloped regions may become even poorer. The challenges and risks are growing daily. In short, the impact of economic globalization is huge; from economic to political and military, for the whole country, seizing the opportunity can be swift development, or the opportunity will face the result of "superiority and elimination" over. Therefore, for better development, enterprises must seize the opportunity, meet the risks and challenges, find their own problems, and avoid problems [3].

Along with the development of network technology, Big Data is gradually applied to various fields of people's life because of its advantages of having a large amount of data storage and very fast processing speed. Enterprises started to incorporate Big Data into their own management model as a result of the emergence of the Big Data era. However, at the same time, as these hidden dangers emerged, the convenience of them also emerged. And ever more dishonest individuals started to take advantage of Big Data's vulnerability by using it and the network to steal the proprietary information of the company [4].

For the enterprise, along with the prompt development of the economy and the speedy depth of economic globalization, the relevant economic policies also follow the continuous adjustment and update; because of its greater

uncertainty, the risk of enterprise management is increasing day by day, so enterprises need to keep pace with the times, change the traditional thinking and management mode, and adapt to the requirements of the times; in order not to be innovative and reformed out, the only way to make the enterprise in a favorable position is to improve its own management system [5]. With the change of social environment, the generation and widespread use of Big Data, enterprises should adopt reasonable means and measures to use these convenient and scientific tools and then find useful resources from Big Data analysis to facilitate their own development and bring them profits while avoiding the related risk factors [6].

In conclusion, economic globalization and the gradual deepening and development of Big Data bring not only convenience and development but also risks and challenges to enterprises. In this situation, it is very necessary to study and explore the risk management models and methods of enterprises. The study of enterprise risk management based on Big Data provides a rational analysis and a reliable way for enterprises to enhance their own risk management capabilities, so it is of great research significance and practical importance [7].

2. Research Background

Many experts and scholars have discussed the main topics in this study, and the research in this area has produced a wealth of findings. In particular, the analysis of the general environment and the problems of enterprise risk management is particularly thorough. Experts and scholars have also expressed their own opinions regarding the improvement measures, based on the research of experts and scholars in this area [8].

In the analysis of the background of Big Data, the following views mainly exist. Along with the development of network technology, Big Data is gradually applied to various fields of people's production and life because of its advantages of having a large amount of data storage and extremely fast processing speed. Generally speaking, the arrival of Big Data Era has both advantages and disadvantages. The advantage is that Big Data technology provides a sharing platform for enterprise for information resources, reduces the expenditure of enterprise management informationization, greatly facilitates the management of enterprises, and makes the management faster. The disadvantage is that the security of management information system is not effectively guaranteed, and the existing data protection capability of enterprises cannot compete with hacking technology, and there is the risk of information leakage, etc. [9].

In this context of the problems of enterprise risk management, experts and scholars are of the opinion that, in the general environment, there is a greater difficulty in enterprise risk management, there are a large number of risks in business, financing, investment, information management, and enterprises in the context of Big Data, and there is no system and early warning measures in enterprise risk management, no correct understanding, and no attention to risk management; in addition to the lack of corresponding, there is a lack of technical management personnel and the relevant technical personnel lack risk control awareness to prevent risks because they do not pay attention to the risk management of the enterprise and the drawbacks of Big Data, which seriously affect the risk management of the enterprise, etc.

Regarding the specific measures and methods to solve the problem, there are several views as follows: enterprises need to change their traditional concepts, build their own risk management system, train specialized technical personnel, and form their own risk management department to supervise and prevent, and enterprises must take tough measures to deal with the problem of data insecurity caused by Big Data, such as the core staff involved in the company's data information ; the core staff involved in the company's data and information must sign a confidentiality agreement to strictly prevent employees from leaking information, strengthen their own information management system enterprises should learn from advanced management experience, improve the enterprise's management system, adopt an appropriate management model, and find out the system's shortcomings and risk events in order to ensure that the security of the data must be ensured properly [10].

To summarize, experts' research on enterprise risk management based on Big Data has been very thorough and has yielded rich research results, but it is clear that these studies still have a single research method and no reliable data to support the theoretical point of view and only rely on literature research, which is not combined with the practical, and the analysis is not thorough.

3. Materials and Methods

3.1. Main Structure of the Study. Firstly, this study analyzes the whole existing environment and background in detail and explains the necessity of researching the topic of enterprise risk management based on Big Data, then immediately summarizes the main results and contents of previous scholars and experts' research on enterprise risk management in the context of the big time, and finally combines its own understanding and research investigation to summarize the main problems of enterprise risk management and, at the same time, summarizes these. The study concludes with the following five sections. This study is written in five main sections [11].

Section 1 mainly analyzes the importance of enterprise risk management research in the context of quick economic development and extensive application of Big Data, which is particularly important and occupies an important position in the survival and development of enterprises [12].

In Section 2, because there are a surging number of domestic studies on risk management based on Big Data, many experts and scholars have different focuses to analyze and talk about this viewpoint, and all of them have different research results that are worthy of deeper investigation. Therefore, this section mainly elaborates and summarizes the unified expert scholars' discussion

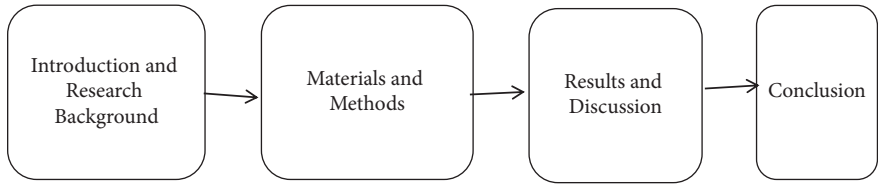


Figure 1: Flowchart of the research content.

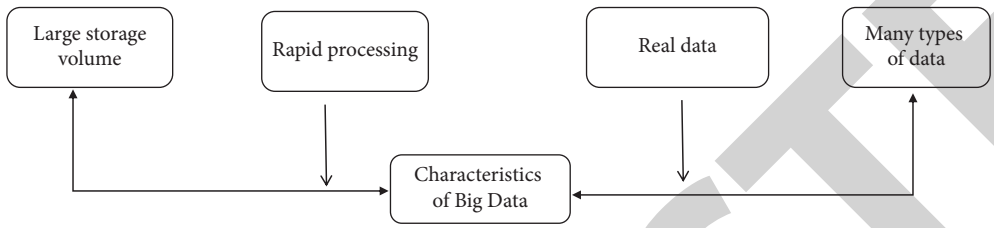


Figure 2: Characteristics of Big Data.

and research on this issue and lays the theoretical foundation for the following writing.

In Section 3, the main materials and research methods are used; the main concepts of this study is explained for understanding, and the main methods of the research are described and summarized [13].

In Section 4, the main problems in enterprise risk management are described, and the main problems that arise in enterprise risk management in the context of Big Data are summarized using the main research methods and their own summary overviews, as well as their own insights. According to the main problems that arise in risk management, corresponding solutions are given one by one and recommendations are given.

Section 5 summarizes the main content of this study and sublimates the theme of the study.

The main contents are shown in Figure 1.

3.2. Main Concepts

3.2.1. The Basic Theory of Big Data

(1) Big Data. Not only can a large amount of data be stored and a large number of data storage network system be formed, but also the data can be analyzed and processed extremely fast [14]. The term "Big Data" refers to the analysis and processing of numerous types of data with the prudent use of media such as computers and networks. It is a fast and convenient way to process information and is gradually applied to all aspects of life, bringing great convenience to people's lives, updating people's traditional views on data management, providing a more innovative and convenient way to store and process complicated data, and greatly improving people's work efficiency [15].

(2) Characteristics of Big Data. Big Data has four main characteristics, namely, large storage volume, instant information processing, real and effective data results, and many types of data [16]. Big Data can go through its own powerful information processing system to store a large amount of information, and because of its powerful system operation and processing function, it processes information and data very quickly. Unlike manual work, Big Data is difficult to falsify and make mistakes on data, thus ensuring the authenticity and correctness of data processing. There are four main features as shown in Figure 2.

(3) The Development of Big Data. The generation and development of Big Data cannot be separated from the popularity of network and computer technology. From the beginning to the present, the technology of Big Data has become increasingly mature, mainly divided into four different aspects as follows.

(1) The development of data sources of Big Data: due to the development of network technology, the data sources of Big Data have become numerous, from a single database to retrieval from multiple databases.

(2) The updating of processing speed and storage mode of Big Data: from simple indexed catalogs to the current subcategories, the search of Big Data has become faster, easier, and more accurate [17]. The search library is constantly updated to optimize the processing speed of Big Data, expand the data sources, and increase the storage capacity.

(3) The transformation of Big Data in the calculation method: from simple data calculation to the possibility of data analysis, graphical combination, and mixed calculation, a great progress has been made in the calculation method.

(4) The security of Big Data has been improved: early on, in the development of Big Data applications, there were many security issues and numerous malicious hackers breaking in and stealing data. Now, Big Data has encrypted and protected the data files and limited the number of accesses, which, to a certain extent, has circumvented the possibility of these risks, making Big Data a great progress in this aspect.

Table 1: List of the development direction of Big Data.

Content	Development direction
Data source	Single to complex
Processing speed and mode	Simple to precise
Calculation method	Simple to complex
Security	Increasing degree of encryption

To sum up, the development direction of Big Data is shown in Table 1.

3.2.2. The Basic Theory of Enterprise Risk Management. Classification of enterprise risks: there are two types of dynamic risks and static risks.

(1) Enterprise Dynamic Risk. Dynamic risk is with uncertainty. In the management side of the enterprise, because of the uncertainty of the human decision of the manager, the risk in management becomes part of the dynamic risk of the enterprise. The market is also unstable, so the risk is also dynamic, and the market policy is constantly changing, the risk may occur at any time [18]. In terms of production life, it is difficult to ensure that production life can be carried out normally because it is affected by a variety of unstable factors, so this part of the risk is also uncontrollable and dynamic. Overall, the dynamic risk of the enterprise is divided into three parts: the enterprise management aspect, the market aspect, and the production aspect of life.

(2) Static Risk of Enterprise. In the case of stable market and economic policies, etc., there are still some irresistible risk factors, which is the static risk, for example, force majeure natural disasters, human work negligence, work errors, and other factors caused by risk events.

(3) Enterprise Risk Management. A management mode is to predict and analyze the possible risks within the enterprise and then take reasonable risk management measures such as risk avoidance, loss control, risk transfer, and risk retention to deal with the risks in a reasonable way, so as to minimize the losses and risks of the enterprise, so that the enterprise can operate and survive well [19].

(4) Measures of Enterprise Risk Management. There are four main types, as shown in Figure 3.

(1) Risk avoidance: take measures to avoid the risks that may occur

(2) Risk loss control: effective control of losses caused by risk events that have already occurred

(3) Risk transfer: rationalize the transfer of existing risk events

(4) Risk retention: some risks must be retained, and various steps must be taken to lower the frequency of risk events and lower losses, as risks cannot be reasonably controlled by avoidance and transfer alone

(5) The Links of Risk Management. Identification, assessment, control, and documentation are the four main components of risk management, which complement each other and are indispensable. So far, the theory and system of risk assessment are relatively well developed [20]. Risk assessment can be controlled by applying the corresponding technical means to assess the size of risks, so risk assessment is one of the most basic steps of risk management. The links of risk management are shown in Figure 4.

The characteristics of risk management in the context of Big Data: there are three characteristics of comprehensiveness, early warning, and complexity.

(1) Comprehensiveness: Big Data has a powerful data repository and a wide range of data sources that can provide enterprises with rich information data such as reports, graphics, audio and video information, allowing enterprises to fully utilize it to analyze and manage risks from multiple perspectives and in a comprehensive manner.

(2) Early warning: Big Data has a very fast data processing speed, which can provide enterprises with the required data information in a timely manner, so as to avoid the risk problems caused by the untimely provision of information, reduce losses and impacts, and give enterprises the ability to anticipate risks in advance, thus avoiding the occurrence of risk events [21].

(3) Complexity: Big Data is complex and risky. Big Data requires very close screening to extract valuable data, and the complexity of its computing system is difficult to estimate. Once an error occurs in the system, it can lead to unpredictable risk problems.

The significance of risk management for enterprises is as follows:

(1) Conducting effective risk management allows enterprises to carry out better production and operation activities so that they can better understand their own risk events, so as to avoid risks, reduce the corresponding risk losses, and ensure that they can take timely remedial measures to minimize losses when risk events occur.

(2) It can improve the economic efficiency and revenue of the enterprise. Effective risk management allows the enterprise to make correct decisions suitable for market changes, avoiding the occurrence of risk events caused by poor decisions, reducing certain economic losses, thus improving the enterprise's revenue and increasing its profit, and providing security for the enterprise's operation and development.

(3) It is beneficial for the enterprise to establish a good social image.

3.2.3. Main Formula. According to the basic theory of financial management, the following formula can be used to measure the enterprise's fundamental risk [22].

Basis risk = operating leverage × financial leverage × revenue volatility × economic relevance.

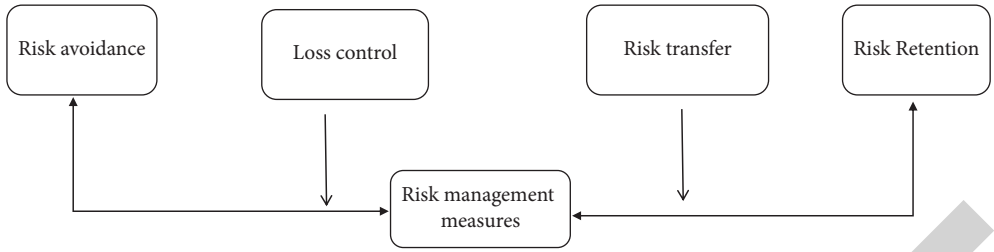


Figure 3: Risk management measures.

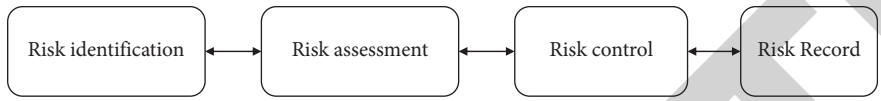


Figure 4: The links of risk management.

Operating leverage = (EBIT + fixed costs)/EBIT.

EBIT = revenue − production costs − selling and administrative expenses − depreciation − R&D expenses.

The key point of this formula (EBIT) is that companies with high fixed costs tend to be riskier.

Financial leverage = (EBITDA)/(EBITDA − finance costs)

This formula can be that, with fixed leverage, lower finance costs can increase EBITDA.

Revenue volatility and economic correlation: in simple terms, revenue volatility is best over a long period of time, preferably the standard deviation of primary operating income in a split year. The optimal range of basis risk is 0.1–0.3.

3.3. Main Research Methodology. This study mainly adopts the following three methods to form the main framework and main ideas of their papers.

(1) Literature reading method: it is mainly formed by reading a lot of literature and combining it with our own understanding.

(2) Survey method: we visit a certain enterprise to see if the risk management of the enterprise in the Big Data environment has several problems summarized in the literature method

(3) Argumentative method: an enterprise is used as a case study to analyze in detail the content and response measures of enterprise risk management under Big Data

3.4. Introduction to the Research Enterprise. Through the literature reading method, reading a large amount of relevant literature and the survey visit method, we visited a local enterprise and summarized and analyzed the following major problems of enterprise risk management in the context of Big Data [23]. A systematic introduction of the surveyed enterprise: a small- and medium-sized enterprise, located in a new first-tier city was established in 2000, with 150 employees and a registered capital of RMB 100 million. The enterprise was established in the early stage to catch up with the fast development of the market economy, the enterprise development flourished, and the production scale of the enterprise also grew and contributed a lot to the national economy. Because of the small size of the company, the cost and operating risks are relatively small, and the management is relatively easy; because of the small size of the company and the establishment of a short period of time, the company's various departments are not correspondingly perfect and business capabilities are not mature, especially in the risk management of the number of specialized departments responsible for less; coupled with the company's main staff of one person in several positions, functional departments are not perfect. With the expansion of the company's scale and business and the change of the market environment, a series of risk problems are exposed. The following is a detailed introduction to the situation of enterprise A.

With the in-depth development of Big Data, the utilization of enterprise A about Big Data is increasing year by year. From Figure 5, we can see that the utilization of Big Data in enterprise A from 2000 to 2022 has increased from 5% to 60%, which proves that the utilization of Big Data in enterprise A is gradually increasing. With the rapid development of Big Data, the application of Big Data in enterprise A is also gradually increasing, but the utilization rate is still not high and not fully utilized [24].

From Figure 6, we can see that the number of people in the risk department of Enterprise A from 2000 to 2022 increased from 2 at the beginning to 8, increasing year by year. The number of people in risk management in Enterprise A is increasing, which proves that Enterprise A starts to pay much attention to risk management.

From Figure 7, we can see that the number of risk events in Enterprise A decreased from 10 to 5 from 2000 to 2022, which proves that, after the establishment of the risk management department in Enterprise A, the number of risk events became less, which shows that the risk management department has played a certain role in controlling the risk management events in this enterprise.

As shown in Figure 8, when the number of risk events is 10, the profit of enterprise A is 1 million yuan, and when the number of risks is 6, the profit of enterprise A is 1.2 million

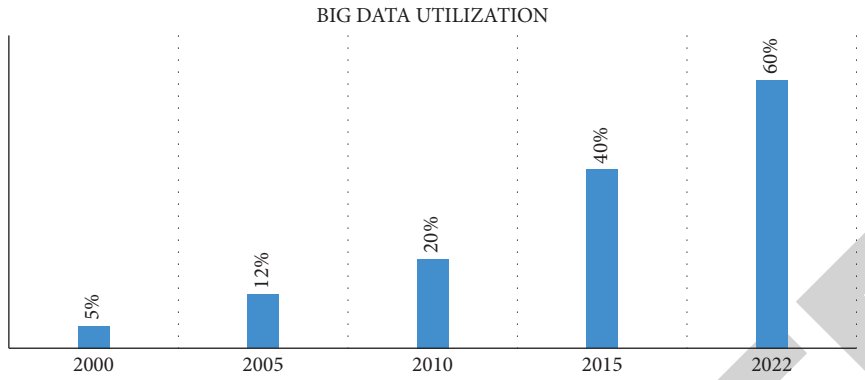


Figure 5: Utilization of Big Data.

Figure 6: Risk management department headcount chart.

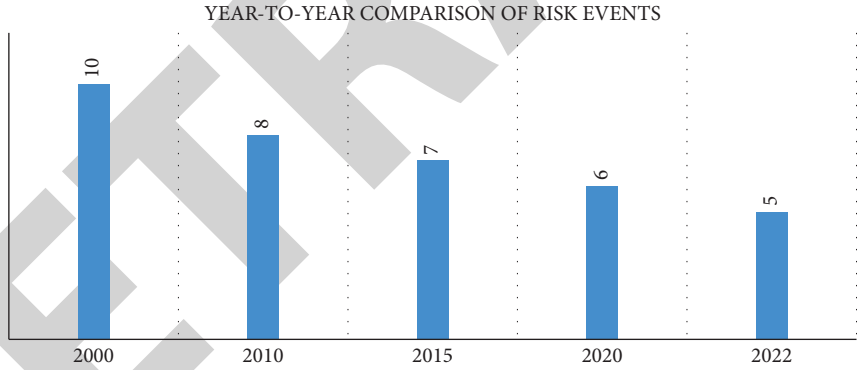


Figure 7: Change in the number of risk events.

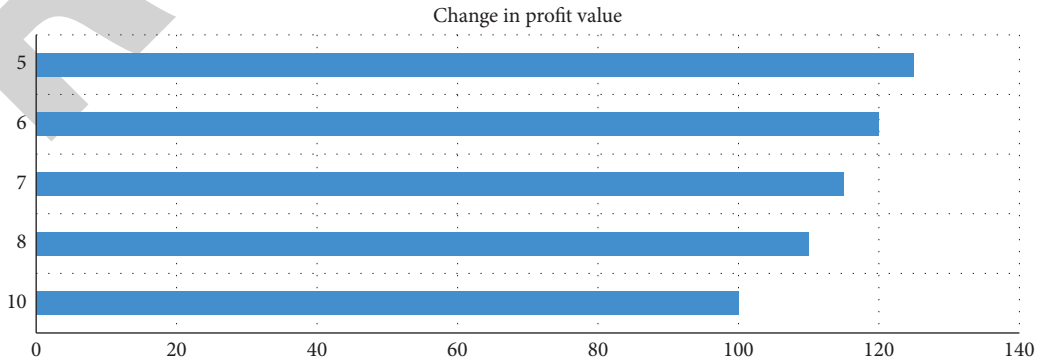


Figure 8: Profit with risk.

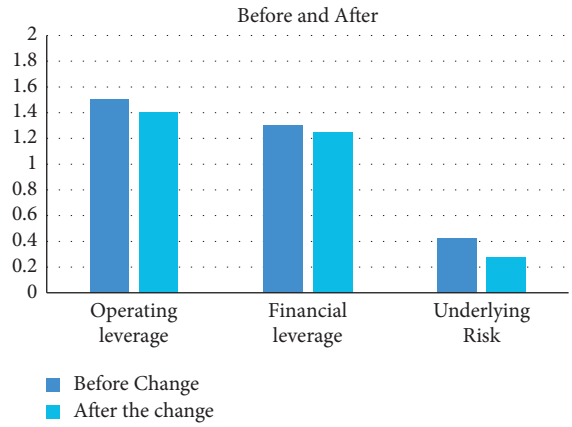


Figure 9: Comparison of risk factors.

yuan, so the profit of the enterprise each year and increases with the number of risk events, proving that the fewer risk events occur, the greater the profit of the enterprise, so we pay attention to risk management [25].

4. Results and Discussion

Under the premise of using Big Data, according to basis risk = operating leverage × financial leverage × revenue volatility × economic correlation), the comparative analysis of risk coefficients before and after the enterprise can be calculated as follows: operating leverage changed from 1.5 to 1.4, financial leverage changed from 1.3 to 1.25, and basis risk changed from 0.42 to 0.28 (Figure 9).

The following is a detailed description and analysis of the problems and causes of risk management in the context of Big Data in conjunction with the enterprise and related literature.

4.1. Problems and Causes of Enterprise Risk Management

4.1.1. Imperfect Risk Management System and Identification System. In the era of Big Data, although the enterprise has gradually used Big Data internally and adopted electronic information equipment to adapt to the development of the times, the enterprise still has the situation that the application of Big Data is not perfect and not in place, the management efficiency of the enterprise is low, the convenience of Big Data is not used to transfer information, and there is a lag in information resources, in addition to the lack of rationalization of internal resources and data. In addition, the lack of rationalization of internal resource data and the lack of smooth communication between relevant departments of the enterprise, which will lead to the speed of data processing, cannot keep up with the actual needs of the project when there are many projects; coupled with the company's various departments, we cannot achieve effective and cooperation and communication is not in place, intensifying the risk of chaos, increasing the possibility of risk problems in the company, and making the company's risk management more difficult. The company has no corresponding early warning measures for risk events, and once a risk event occurs, there is no timely communication and exchange, and the company lacks corresponding capabilities to predict and identify risks [26]. The company seems to have established a relevant risk management system and identification system, but it does not achieve the comprehensiveness of risk identification and lacks comprehensive application and analysis of risk events so that the company has great management loopholes in management, especially risk management [27]. In short, the imperfect risk management system and risk identification system within the enterprise and the loopholes in the enterprise risk management model are the main problems of enterprise risk management nowadays [28].

4.1.2. Managers Have Misconceptions about Risk Management and Do not Pay Attention to Risk Management. In today's world, the risks that businesses face are enormous, elusive, and unpredictable. For example, due to the widespread use of Big Data technology, the enterprise's financial management system and information management system may be compromised, resulting in data corruption, and these damages include not only the loss of enterprise data, but also, in severe cases, the risk of the theft of certain enterprise business secrets. The management of the enterprise may have a fluke mentality, but the security of Big Data is still very worthy of deep thought and examination; however, there is still a large part of the management only see the positive side of the convenience brought by Big Data, ignoring this part of the risk factors, and did not form the relevant response plan and preventive measures. Therefore, failure to detect problems such as information leakage in a timely manner can put a company at a disadvantage. It is a conventional concept in which enterprise risk is evaluated by the beta value, but this is only a purely idealized mathematical model, which is difficult to predict and measure the actual situation within the enterprise, so the conventional concept and data model are no longer suitable for the real needs, and it is necessary to keep pace with the times and to update the enterprise's own risk management model and concept. In corporate management, company leaders and executives focus more on cost management and performance management, putting cost at the forefront of the company's development, thus neglecting the management of risk [29]. Business leaders neglect risk management, put cost first, and thus fail to develop risk management measures at the strategic level. Undoubtedly, the survival and development of enterprises cannot be separated from the control and management of costs, but the management of risks is also particularly important; especially, in the context of the development of Big Data, it can be said that the policies and market information of the whole industry will change a lot; if you cannot obtain or adapt in advance, we will put the enterprise itself in a great risk, so the enterprise risk management should be based on Big Data. Therefore, the enterprise risk management should be re-adjusted and repositioned based on the Big Data and based on the whole environment to make corresponding adjustments and updates to adapt to the requirements of the whole

environment, to achieve the healthy survival and development of the enterprise. To sum up, the problem is that the managers cannot accurately understand the importance of enterprise risk management and focus on cost control, plus the addition of Big Data provides great convenience to enterprises, and the managers of enterprises ignore the risk factors of Big Data itself [30].

4.1.3. Lack of Professional Competence of Technical Personnel. The widespread use of Big Data is a huge challenge not only for enterprises themselves but also for professional and technical personnel because of the complex processing and storage requirements of Big Data, thus making Big Data security greatly reduced, which requires professional and technical personnel responsible for this area, with a keen insight and good professionalism and good supervision of equipment data. All personnel involved in the handling of confidential company data are required to maintain strict confidentiality. However, the relevant technical personnel in the enterprise lack risk prediction and identification ability, personal quality is not high, and the security of Big Data there is a fluke mentality, thus ignoring the corresponding risk, so that the enterprise in this aspect of risk management is at a disadvantage. The application of Big Data has brought great convenience to enterprise management; because of the fast processing speed and convenience, people began to rely too much on and trust the data processing results given by it, but the accuracy of Big Data is still worthy of deep investigation, the data sources of Big Data are more, and the data from different regions may be in a data processing database, so the accuracy of data processing is also open to question. The relevant technical personnel cannot just rely on the processing results of Big Data and trust the calculation data provided by Big Data, lacking rational research and thinking, so the relevant technical personnel must strictly require themselves and improve their ability to judge right and wrong in order to avoid certain risk losses. To conclude, technical managers do not have good specialization ability, good insight into risks, and professional ethics to cope with the addition of Big Data, which leads to frequent loopholes in enterprise risk management and certain problems in enterprise risk management that cannot be solved in time and is one of the main problems of enterprise risk management in the context of Big Data.

In summary, the above three problems are summarized in the literature and in practice and rationalized in terms of the system of risk management, the importance of personnel, and relevant technical personnel, but the causes of the problems are also worthy of deeper investigation, so the author summarizes the following reasons. (1) The enterprise is a small and medium-sized enterprise, with weak market competitiveness, short establishment, and limited capital, so it does not have a large amount of capital and money to invest in risk management. (2) The enterprise is small and the risks are greater than those of large state-owned enterprises, the staff reserve is not enough, one person may have several jobs, the functional departments are not perfect, the staff is lacking, and there are no extra human and material resources to invest in risk management. (3) In addition, the leadership team of the enterprise is not forward-looking enough and the attractiveness of the enterprise to specialized talents is not high enough, so there is a considerable lack of professional talents, as well as the leadership team is old; it is difficult to accept the addition of some new science and technology, so in the context of Big Data, risk management has quite a few problems.

4.2. Enterprise Risk Management Measures. Based on the above summarized problems of enterprise risk management in the general environment, there are several corresponding measures to solve them as follows.

4.2.1. Enterprises Need to Improve the Risk Management System and Early Warning Mechanism. In the context of the in-depth development of Big Data, enterprises should improve their risk management capabilities according to the development requirements of society and the times, which requires enterprises themselves to pay attention to the development of risk management work and the establishment of a set of risk management system in line with their own development. An organic whole needs to be formed from the top to the leadership of the company, down to the ordinary employees. The company should establish a risk management system that is adapted to the development of the company, implement it with responsibility, and integrate the risk management system into the normal management of the company. The company also needs to establish a set of risk warning and control system to grasp the possible risks and rationalize the analysis, so as to avoid risks and reduce the probability of risk events. The company should have a full and correct understanding of the risk management process and be able to take reasonable measures to minimize the losses caused by the occurrence of risks when they occur.

4.2.2. Transform the Concept and Pay Attention to Risk Management. With the frequent occurrence of risk problems, a mushrooming number of companies have started to pay attention to risk management from the initial pursuit of cost and profit maximization, but how to make the internal risk management work effectively and quickly is a big test for both companies and managers. The arrival of Big Data has brought a great deal of convenience to enterprises, but there are also some risk factors; how to use these facilities to avoid these risks is also an important issue for the survival and development of enterprises. Although the generation of Big Data will bring certain risks to the management of enterprises, the advantages of using Big Data within the enterprise can also provide very effective ways to deal with the occurrence of these risks; enterprises can use Big Data to understand their own operations and development more clearly, pay attention to the changes in market information in a timely manner, update the development direction and development concept, and find more favorable market information; the enterprise's senior managers can also implement better management through this powerful tool of Big Data; employees can also use this tool reasonably to

Table 2: Correspondence between problems and solution measures of enterprise risk management based on Big Data.

Problems	Solution measures
The enterprise risk management system and identification system are not perfect	Improve risk management system and early warning mechanism
Managers have a wrong understanding of risk management and do not pay attention to risk management	Transform the concept and pay attention to risk management
Lack of professional competence of technical personnel	Cultivate specialized talents

make the communication of various departments faster and more convenient, reducing the occurrence of news communication is not in place and not convenient; good communication and exchange between various departments can be carried out to improve efficiency. The concept can lead and change the action so that enterprises want to improve their risk management ability and need to start from improving the concept of risk management. Managers must convert the traditional ideology, pay attention to risk management, and learn to use the convenience of Big Data, in order to avoid the related risk problems to a certain extent.

4.2.3. Cultivating Specialized Talents. To better carry out risk management work, enterprises must pay attention to the cultivation of talents, which is the soul of the survival and development of enterprises. Having specialized talents enables not only better implementation of risk management policies but also efficient handling of the corresponding problems of risk management, which can enable enterprises to achieve better results in risk management. Enterprises need to provide specialized training for the professional and technical staff of risk control. Professional and technical staff must continually improve their professional skills and ethics, as well as their overall quality. It is also very important for workers in other departments to regularly attend lecture sessions on Big Data and network technology. Enterprises need to improve the participation of all employees in risk management, increase the amount of everyone's knowledge reserve, and make the concept of risk management deeply rooted in people's hearts. In addition, each department should work closely together, divide the work well, and implement the process of risk management implement the responsibility system to make sure that risk control is not a task of one person and one department, but it is a work that needs to be done together by everyone so that not only the efficiency of employees but also the overall risk control level of the enterprise can be improved.

5. Conclusion

In this study, through the analysis of the background of Big Data, combined with relevant research and studies, we have a certain understanding and knowledge of enterprise risk management in the Big Data environment and made theoretical analysis, mainly the following.

Background: enterprises face both opportunities and challenges as Big Data becomes more prevalent. The opportunities are that the use of Big Data can make enterprise management more convenient and work faster, and the challenge lies in whether enterprises can adapt to the changes brought by Big Data and whether they can cope with a series of risk problems that may be caused by Big Data.

The problems of enterprise risk management: the enterprise's risk management system and identification system have imperfect problems, the managers have misconceptions about risk management and do not pay attention to risk management, the enterprise lacks specialized technical personnel, and the technical personnel lack the corresponding ability and comprehensive quality.

Causes of the problem: the short establishment and limited capital of the company, among other reasons, result in not having a large amount of capital to invest in risk management; it is difficult to accept some new science and technology to join; these are the main reasons for the problems of enterprise risk management.

The solution to the problem: in response to these problems, enterprises need to improve the risk management system and early warning mechanism; relevant managers should transform their traditional concepts and pay attention to risk management; at the same time, enterprises should also train professional talents to manage and control risks. The problems and solutions of enterprise risk management based on Big Data are shown in Table 2.

To sum up, along with the in-depth development of Big Data, Big Data and network technology have gradually started to be applied to the daily production and life of enterprises, and information and resources have diversified. Because of the addition of Big Data, the management and production life of enterprises become more efficient and convenient; as the Big Data is also a double-edged sword to bring convenience, it also bring risks that cannot be ignored, which requires enterprises to pay attention to the management of risk.

Despite the fact that many businesses have their own risk management systems and risk management departments, there are still many issues with risk management in the context of Big Data. However, there are some shortcomings in this study, as the number of enterprises visited in this study is not enough and it is not representative of all enterprises, so it is a bit too one-sided. In addition, the literature read in this study has more references to the research conclusions of domestic experts and less references to foreign research results, so it has some limitations and one-sidedness.

Data Availability

The labeled dataset used to support the findings of this study can be obtained from the author upon request.

Conflicts of Interest

The author declares that there are no conflicts of interest.

Acknowledgments

This work was supported by Aba Science and Technology Bureau (19YYJSYJ0091).

References

[1] X. C. Tan, L. S. Kong, B. H. Gu, A. Zeng, and M. M. Niu, "Research on the carbon neutrality governance under a polycentric approach," *Advances in Climate Change Research*, vol. 13, no. 2, p. 10, 2022.

[2] Z. Wu, T. Lv, and Y. Guo, "An improved particle swarm optimization algorithm based on DFC&HRS," in *Proceedings of the SPIOT 2020: the 2020 international conference on machine learning and big data analytics for IoT security and privacy*, pp. 31–38, Switzerland, November 2020.

[3] W. Cai, M. Bai, and H. Davey, "Implementing environmental protection tax in China: an alternative framework," *Pacific Accounting Review*, vol. 34, no. 3, pp. 479–513, 2022.

[4] K. He, L. Yu, and Y. Chen, "Research on authority management and risk control of state-owned enterprises based on accounting matters," *Scientific Journal of Economics and Management Research*, vol. 4, no. 4, 2022.

[5] F. Harlow Alyssa, A. C. Stokes, R. Brooks Daniel, E. J. Benjamin, J. L. Barrington-Trimis, and C. S. Ross, "Cigarette Use and Combustible Cigarette Smoking Initiation among Youth: Accounting for Time-Varying Exposure and Time-dependent Confounding," *Epidemiology*, vol. 33, 2022.

[6] N. A. Makhutov and D. O. Reznikov, "Prior and posterior assessments of failure scenario probabilities and environmental risks at hazardous industrial facilities," *IOP Conference Series: Earth and Environmental Science*, vol. 988, no. 3, p. 6, 2022.

[7] R. Z. Anna and M. Lesław, "Accounting and market risk measures of polish energy companies," *Energies*, vol. 15, no. 6, 2022.

[8] H. Zhang, C. Zhang, and F. Hou, "Analysis of 8611 cases of adverse reaction reports of breviscapine for injection," *Medicinal Plant Research*, vol. 13, no. 1, pp. 44–51, 2022.

[9] T. Isabelle, L. Guénette, and Z. Arsène, "Depression and the risk of hospitalization in type 2 diabetes patients: a nested case-control study accounting for non-persistence to antidiabetic treatment," *Diabetes & Metabolism*, vol. 48, no. 4, 2022.

[10] S. Brèteau-Amores, M. Fortin, P. Andrés-Domenech, and N. Bréda, "Is Diversification a Suitable Option to Reduce Drought-Induced Risk of Forest Dieback? an Economic Approach Focused on Carbon Accounting," *Environmental Modeling & Assessment*, vol. 27, 2022.

[11] I. Safdar, M. Neel, and B. Odusami, "Accounting information and left-tail risk," *Review of Quantitative Finance and Accounting*, vol. 58, 2022.

[12] Y. Wu, "Artificial intelligence is the technical guarantee of network security. SPIOT 2020," in *Proceedings of the The 2020 International Conference on Machine Learning and Big Data Analytics for IoT Security and Privacy*, pp. 69–74, Springer Nature Switzerland AG, Switzerland, November 2020.

[13] J. K. McCloskey, J. L. Ellis, C. S. Uratsu et al., "Accounting for social risk does not eliminate race/ethnic disparities in COVID-19 infection among insured adults: a cohort study," *Journal of General Internal Medicine*, vol. 37, no. 5, pp. 1183–1190, 2022.

[14] Y. Evan, C. Stern Mariana, and at al, "Family History and Risk of Bladder Cancer: An Analysis Accounting for First- and Second-Degree Relatives," *Cancer prevention research*, vol. 15, 2022.

[15] R. Z. Anna, "Market and accounting measures of risk: the case of the frankfurt stock exchange," *Risks*, vol. 10, no. 1, 2022.

[16] T. T. Y. Alabdullah, "Management accounting insight via a new perspective on risk management-companies' profitability relationship," *International Journal of Intelligent Enterprise*, vol. 9, no. 2, p. 244, 2022.

[17] S. Buck, J. Sandqvist, E. N. Strid, H. J. Knibbe, P. Enthoven, and C. Wahlin, "Risk assessment of physical exposure among healthcare workers when performing patient handling-T," *Safety and Health at Work*, vol. 13, p. S215, 2022.

[18] S. N. K. Cdr, L. S. Ganesh, and C. Rajendran, "Management accounting tools for failure prevention and risk management in the context of Indian innovative start-ups: a contingency theory approach," *Journal of Indian Business Research*, vol. 14, no. 1, 2021.

[19] K. Smit, A. Zucker Robert, and K. Emmanuel, "Exposure to Parental Alcohol Use Is Associated with Adolescent Drinking Even when Accounting for Alcohol Exposure of Best Friend and Peers," *Alcohol and alcoholism*, vol. 57, 2021.

[20] K. M. Fewster, J. R. Guo, J. D. Zehr, J. M. Barrett, A. C. Laing, and J. P. Callaghan, "Strain response in the facet joint capsule during physiological joint rotation and translation following a simulated impact exposure: an in vitro porcine model," *Journal of Biomechanical Engineering*, vol. 144, no. 5, Article ID 051010, 2022.

[21] W. Wang, "Establishment of long-term mechanism for preventing poverty return through education in rural revitalization in southern Shaanxi," *Asian Agricultural Research*, vol. 14, no. 1, p. 6, 2022.

[22] L. Liu, "Retraction Note: o," *Arabian Journal of Geosciences*, vol. 14, no. 24, p. 2772, 2021.

[23] M. Jankowska Marta, J. A. Yang, N. Luo, C. Poon, and T. Benmarhnia, "Accounting for space, time, and behavior using GPS derived dynamic measures of environmental exposure," *Health & Place*, 2021.

[24] V. Stülpnagel Rul, P. Chayenne, and L. Sven, "Crash Risk and Subjective Risk Perception during Urban Cycling: Accounting for Cycling Volume," *Accident; analysis and prevention*, vol. 164, 2021.

[25] R. Ball, G. Sadka, and A. Tseng, "Correction to: using accounting earnings and aggregate economic indicators to estimate firm-level systematic risk," *Review of Accounting Studies*, vol. 27, 2021.

[26] Z. Jabi, R. Jorquera Ignacio, C. Trexler Joel, S. Orzechowski, L. Garner, and P. Frederick, "Accounting for Food Availability Reveals Contaminant-Induced Breeding Impairment, Food-Modulated Contaminant Effects, and Endpoint-Specificity of Exposure Indicators in Free Ranging Avian populations," *Science of the Total Environment*, vol. 791, 2021.

[27] C. Li, "The application of artificial intelligence and machine learning in financial stability," in *Proceedings of the SPIOT 2020: The 2020 International Conference on Machine Learning and Big Data Analytics for IoT Security and Privacy*, pp. 214–219, Springer Nature Switzerland AG, Switzerland, 2020.

[28] E. J. Oh, R. B. Parikh, C. Chivers, and J. Chen, "Two-stage approaches to accounting for patient heterogeneity in

Hindawi
Security and Communication Networks
Volume 2022, Article ID 9245516, 12 pages
https://doi.org/10.1155/2022/9245516

Research Article

Multiparty Threshold Private Set Intersection Protocol with Low Communication Complexity

Xiaopeng Yu,[1] **Fagen Li**,[2] **Wei Zhao**,[1] **Zhengyi Dai**,[3] **and Dianhua Tang**[1,2]

[1]*Science and Technology on Communication Security Laboratory, Chengdu 610041, China*
[2]*School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu 611731, China*
[3]*College of Computer, National University of Defense Technology, Changsha 410073, China*

Correspondence should be addressed to Dianhua Tang; tangdianhua86@163.com

Received 25 April 2022; Accepted 13 August 2022; Published 27 September 2022

Academic Editor: Arijit Karati

Multiparty threshold private set intersection (MP-TPSI) protocol allows n mutually untrusted parties $P_1, P_2, \ldots, P_n$ holding data sets $A_1, A_2, \ldots, A_n$ of size m respectively to jointly compute the intersection $I = A_1 \cap A_2 \cap \cdots \cap A_n$ over all their private data sets only if the size of intersection is larger than $(m - t)$, while ensuring that no other private information of the data sets other than the intersection is revealed, where t is the threshold. In the MP-TPSI protocol, multiple parties first decide whether the size of the intersection is larger than the threshold t; then, they compute the intersection if the size of the intersection is larger than the threshold t. However, the existing MP-TPSI protocols use different forms of evaluation polynomials in the cardinality testing and intersection computing phases, so that parties need to transmit and calculate a large number of evaluation values, which leads to high communication and computational complexity. In addition, the existing MP-TPSI protocols cannot guarantee the security and the correctness of the results, that is, an adversary can know the additional information beyond the intersection, and the elements that are not in the intersection are calculated as the intersection. To solve these issues, based on the threshold fully homomorphic encryption (TFHE) and sparse polynomial interpolation, we propose an MP-TPSI protocol. In the star network topology, the theoretical communication complexity of the proposed MP-TPSI protocol depends on the threshold t and the number of parties n, not on the size of set m. Moreover, the proposed MP-TPSI protocol outperforms other related MP-TPSI protocols in terms of computational and communication overheads. Furthermore, the proposed MP-TPSI protocol tolerates up to $n - 1$ corrupted parties in the semi-honest model, where no set of colluding parties can learn the input of an honest party in the strictest dishonest majority setting.

1. Introduction

The private set intersection (PSI) protocol [1] allows two mutually untrusted parties P_1 and P_2 holding data sets A_1 and A_2 to jointly compute the set intersection $I = A_1 \cap A_2$, and does not reveal anything except the intersection. PSI protocol has a large number of application scenarios, e.g., DNA matching [2], botnet detection [3], and private contact discovery [4]. Over the past few decades, in the semi-honest and malicious security model, a long line of work [5–23] has been made to effectively implement the PSI protocol. The main cryptographic primitives of the existing PSI protocols include: garbled circuits (GC) [24], oblivious transfer (OT) [25], homomorphic encryption (HE) [26] and pseudorandom functions (PRF) [27], etc. To support PSI among multiple parties, several multiparty PSI (MP-PSI) protocols [28–36] have been presented.

However, in certain application scenarios, such as vertical federated learning (VFL) [37], the MP-PSI protocol mentioned above cannot satisfy the requirements. Specifically, in vertical federated machine learning, the training data is distributed among multiple parties, and each party has different features of the same object, multiple parties want to combine different features of common samples to train a better machine learning model. It is worth noting that all parties are willing to perform multiparty entity alignment only when the number of sample intersection is large. If the number of sample intersection is too small, the sample

alignment will have no effect on improving the performance of the model, and the parties will not be interested in jointly computing the intersection of training samples. To meet such demands to determine whether the size of intersection is large enough before performing sample alignment, the multiparty threshold private set intersection (MP-TPSI) protocols [38–41] have been introduced, which enables n mutually distrusted parties $P_1, P_2, \ldots, P_n$ holding data sets $A_1, A_2, \ldots, A_n$ of size m respectively to jointly compute the intersection over all their private data sets only if the size of intersection is larger than $(m - t)$, while ensuring that no other private information of the data sets other than the intersection is revealed. The MP-TPSI protocol consists of two phases: the cardinality testing phase, where multiple parties decide whether the size of intersection is larger than a certain threshold t; and the intersection computing phase, where multiple parties calculate the intersection if the size of intersection is larger than a certain threshold t. Unfortunately, the existing MP-TPSI protocols [38–41] still have the heavy communication complexity. To solve this problem, using sparse polynomial interpolation and threshold fully homomorphic encryption (TFHE) [42], this paper proposes an MP-TPSI protocol with low communication complexity.

The main contributions are as follows:

(1) Firstly, in a star network topology where the designated party P_1 can communicate with each party P_i $(i = 2, 3, \ldots, n)$, using an evaluation method that represents the set as a polynomial, we construct an MP-TPSI protocol based on the TFHE. To reduce the communication and computational cost, we use the same form of evaluation polynomial in the cardinality testing and intersection computing phases, which enables the parties to transmit and compute only a small number of evaluation values.

(2) Secondly, in the proposed MP-TPSI protocol, the theoretical communication complexity of the designated party P_1 and each party P_i $(i = 2, 3, \ldots, n)$ are $\mathcal{O}(tn)$ and $\mathcal{O}(t)$, respectively, which are smaller than the existing MP-TPSI protocols [38–40] and TAHE-based MP-TPSI protocol [41]. In contrast to conventional MP-PSI protocols [28–36], the communication complexity of the proposed MP-TPSI protocol only depends on the threshold t and the number of parties n, not on the size of set m.

(3) Finally, we evaluate the proposed MP-TPSI protocol and the related TFHE-based MP-TPSI protocol [41] under $n \in \{2, 3, \cdots, 8\}$, $m \in \{2^{10}, 2^{11}, 2^{12}\}$, and $t \in \{2^9, 2^{10}, 2^{11}\}$. The experimental results demonstrate that, compared with the TFHE-based MP-TPSI protocol [41], the computational and communication costs in the proposed MP-TPSI protocol are reduced by nearly 92.0%–97.3% and 67.2%–67.3%, respectively. The security analysis illustrates that the proposed MP-TPSI protocol can achieve semi-honest security in the dishonest majority model where up to $n - 1$ parties can be allowed to corrupt.

The remainder of the study is organized as follows. We introduce some related works in Section 2. In Section 3, we review some preliminaries. In Section 4, our protocol is described in detail. The performance evaluation of our protocol is presented in Section 5. The security analysis of our protocol is shown in Section 6. Finally, we conclude in Section 7.

2. Related Works

Some works [28–36, 38–41] closely related to this study are introduced in this section. For ease of description, we summarize the theoretical communication complexity of [28–36, 38–41] in Table 1.

By representing the set as a polynomial, based on threshold additive HE (TAHE) that can be realized from Paillier encryption [43], Kissner et al. [28] implement the PSI operations in multiparty setting. Leveraging the Bloom filters (BF) [44] and exponential additive HE (AHE) [45], Miyaji et al. [29] presented a scalable MP-PSI protocol, they set a dealer to decrease the computational complexity of the parties. In a star network topology, based on the two-party protocol of [46], Hazay et al. [30] described the MP-PSI protocols in semi-honest and malicious settings. Kolesnikov et al. [31] proposed a method called oblivious programmable PRF (OPPRF), designed MP-PSI protocols based OPPRF in the semi-honest model, and further optimized it to the augmented-semi-honest model. Inbar et al. [32] extend the PSI construction of [12] to multiparty setting, and described the MP-PSI protocols for semi-honest and augmented-semi-honest settings in a star network topology. Setting the elements of its own set to the roots of a polynomial, based on the OLE, in a star network topology, Ghosh et al. [33] presented an approach to achieving secure MP-PSI. Lu et al. [34] proposed an MP-PSI protocol for VFL in a star network topology, which is able to compute the intersection in the event that some of the parties are offline. Combining of the star and path communication patterns which in the former, one party at the center can communicate with all other parties, and in the latter, each party can communicate with neighboring parties, Kavousi et al. [35] presented an efficient protocol for MP-PSI using oblivious PRF (OPRF). Based on the TAHE schemes and BF, in a star network topology, Bay et al. [36] proposed an MP-PSI protocol, which is secure in the semi-honest model. However, the communication and computational complexity of the MPSI protocol [28–36] mentioned above depend on the size of the input data set, which directly becomes a basic obstacle to efficiency.

Based on the AHE, Ghosh et al. [38] introduced an MP-TPSI protocol, which is the first MP-TPSI protocol with communication complexity that depend on threshold t, not on the set size m. However, Abadi et al. [47] pointed out that [38]'s protocol is not secure because an adversary can learn other information about the sets of honest parties beyond the intersection. Using the OPRF and hash function, Mahdavi et al. [39] introduced two constructions for the MP-TPSI protocol, namely $t - \mathrm{PSI}_0$ and $t - \mathrm{PSI}$, but the computational complexity is exponential in the threshold t,

Table 1: Theoretical communication complexity comparison.

Protocols	Communication complexity		Security model
	Designated party P_1	Party P_i $(i = 2, 3, \ldots, n)$	
[28]	$\mathcal{O}(mn)$	$\mathcal{O}(mw)$	Semi-honest
[29]	$\mathcal{O}(mn)$	$\mathcal{O}(m)$	Semi-honest
[30]	$\mathcal{O}(mn)$	$\mathcal{O}(m)$	Semi-honest
[30]	$\mathcal{O}((m + m\log m + n)n)$	$\mathcal{O}(m + m\log m + n)$	Malicious
[31]	$\mathcal{O}(mn)$	$\mathcal{O}(mn)$	Semi-honest
[31]	$\mathcal{O}(mn)$	$\mathcal{O}(m)$	Augmented-semi-honest
[32]	$\mathcal{O}(mnh)$	$\mathcal{O}(mnh)$	Semi-honest
[32]	$\mathcal{O}(mnh)$	$\mathcal{O}(mh)$	Augmented-semi-honest
[33]	$\mathcal{O}(n^2 + mn)$	$\mathcal{O}(m)$	Semi-honest
[34]	$\mathcal{O}(mn)$	$\mathcal{O}(mq)$	Semi-honest
[35]	$\mathcal{O}(mn)$	$\mathcal{O}(mk)$	Semi-honest
[36]	$\mathcal{O}(mn)$	$\mathcal{O}(m)$	Semi-honest
[38]	$\mathcal{O}(t^2n)$	$\mathcal{O}(t^2)$	Semi-honest
[39]	$\mathcal{O}(mnw)$	$\mathcal{O}(mnw)$	Semi-honest $(t - \mathrm{PSI}_0)$
[39]	$\mathcal{O}(tmnc)$	$\mathcal{O}(tmnc)$	Semi-honest $t - \mathrm{PSI}$
[40]	$\mathcal{O}(t^2n)$	$\mathcal{O}(t^2)$	Semi-honest
[41]	$\mathcal{O}(t^2n)$	$\mathcal{O}(t^2)$	Semi-honest (TAHE-based)
[41]	$\mathcal{O}(tn)$	$\mathcal{O}(t)$	Semi-honest (TFHE-based)

and thus have a poor performance. By employing the TAHE from Elgamal encryption [48] and Paillier encryption [43], Branco et al. [40] developed a protocol to securely compute linear algebra functions and proposed an MP-TPSI in a star network topology. Badrinarayanan et al. [41] pointed out that [38]'s protocol has a subtle issue, that is, elements that are not in the intersection may also be computed as elements in the intersection. To solve this issue, in the star network topology, they proposed the TAHE-based MP-TPSI and TFHE-based MP-TPSI protocols. However, their TFHE-based MP-TPSI protocol uses different forms of evaluation polynomials in the cardinality testing and intersection computing phases, which requires the transmission and calculation of a large number of evaluation values, and brings to heavy communication and computational cost.

3. Preliminaries

3.1. Notations. For ease of reading, the definitions of symbols in the proposed MP-TPSI protocol are described in Table 2.

Table 2: The definitions of the symbols.

Symbols	Definitions
P_i	The i-th party
A_i	The data set of party P_i
I	The intersection of $A_1, A_2, \cdots, A_n$
$\lvert I\rvert$	The size of the intersection I
n	The number of parties
m	The size of each set A_i
t	The threshold
x	The ciphertext of plaintext x
x_i	The partial decryption ciphertext of x
λ	The security parameter
$\mathrm{negl}(\lambda)$	The negligible function on λ

3.2. Security Model. We define the security of the proposed MP-TPSI protocol in universal composability (UC) framework [49]. Considering a multiparty protocol Π that realizes the ideal functionality $\mathcal{F}$, we can define the security of the protocol Π in the ideal/real world.

In an ideal world: n parties transmit all inputs to $\mathcal{F}$, and receive the computation result. Simulator $\mathcal{S}$ is regarded as an adversary in an ideal world, has complete control of the parties that are corrupted, and simulates $\mathcal{Z}$'s view of on the execution of the real protocol.

In a real world: n parties perform Π, Π is permitted to call an ideal functionality $\mathcal{G}$. Environment $\mathcal{Z}$ selects all inputs of n parties, simulates anything outside Π. $\mathcal{Z}$ can represent the adversary and corrupt any subset of the parties.

Assuming $\mathrm{Ideal}[\mathcal{Z}, \mathcal{S}, \mathcal{F}]$ and $\mathrm{Real}[\mathcal{Z}, \Pi, \mathcal{G}]$ are the output of $\mathcal{Z}$ in the ideal and real world, respectively, we define Π securely realizes $\mathcal{F}$, if there is a $\mathcal{S}$ so that for any $\mathcal{Z}$ we have

$$\left|\Pr[\mathrm{Ideal}[\mathcal{Z}, \mathcal{S}, \mathcal{F}] = 1] - \Pr[\mathrm{Real}[\mathcal{Z}, \Pi, \mathcal{G}] = 1]\right| \leq \mathrm{negl}(\lambda). \quad (1)$$

3.3. The definition of Threshold Fully Homomorphic Encryption. A TFHE scheme [42] consists of the distributed setup (TFHE.DisSet), encryption (TFHE.Enc), addition (TFHE.Add), multiplication (TFHE.Mul), partial decryption (TFHE.PartDec), and combination (TFHE.Comb) algorithms.$\mathrm{TFHE.DisSet}(1^\lambda, i) \longrightarrow (\mathrm{pk}, \mathrm{sk}_i)$: On input λ and party's number i, TFHE.DisSet algorithm returns the secret key share sk_i and public key pk for the party P_i.$\mathrm{TFHE.Enc}(\mathrm{pk}, x) \longrightarrow x$: On input pk and plaintext x, TFHE.Enc algorithm returns the ciphertext x.$\mathrm{TFHE.Add}(x_1, x_2) \longrightarrow x_1 + x_2$: On input the ciphertexts x_1 and x_2, TFHE.Add algorithm outputs the ciphertext $x_1 + x_2$.$\mathrm{TFHE.Mul}(x_1, x_2) \longrightarrow x_1 * x_2$: On input the ciphertexts x_1 and x_2, TFHE.Mul algorithm outputs the

Parameters: Each party P_i holds a data set A_i with m elements, and sets a threshold $T \in \mathbb{N}$, where $i \in \{1, 2, \cdots, n\}$.
Inputs: Each party P_i inputs a data set $A_i = \{a_{i,1}, a_{i,2}, \cdots, a_{i,m}\}$, where $a_{i,j} \in \mathbb{F}_p$ for each $j = 1, 2, \cdots, m$, $\mathbb{F}_p$ is a finite field.
Outputs: If $|A_i \backslash I| \leq T$, each party P_i outputs $true$, otherwise outputs $false$.

Figure 1: Ideal functionality $\mathcal{F}_{\text{MP–TPSI–CT}}$ for MP-TPSI cardinality testing.

Parameters: Each party P_i holds a data set A_i with m elements, and sets a threshold $T \in \mathbb{N}$, where $i \in \{1, 2, \cdots, n\}$.
Inputs: Each party P_i inputs a data set $A_i = \{a_{i,1}, a_{i,2}, \cdots, a_{i,m}\}$, where $a_{i,j} \in \mathbb{F}_p$ for each $j = 1, 2, \cdots, m$, $\mathbb{F}_p$ is a finite field.
Outputs: Each party P_i outputs intersection $I = A_1 \cap A_2 \cap \cdots \cap A_n$ or none $\perp$.

Figure 2: Ideal functionality $\mathcal{F}_{\text{MP–TPSI–C}}$ for MP-TPSI computing.

ciphertext $x_1 * x_2$.TFHE.PartDec$(\text{sk}_i, y) \longrightarrow y_i$: On input the secret key share sk_i and ciphertext y, TFHE.PartDec algorithm outputs the partial decryption ciphertext y_i.TFHE.Comb$(y_1, y_2, \cdots, y_n) \longrightarrow y$: On input a set of partial decryption ciphertexts $y_1, y_2, \cdots, y_n$, TFHE.Comb algorithm outputs the plaintext $y = y_1 + y_2 + \cdots + y_n$.

3.4. Functionality. Ideal functionality $\mathcal{F}_{\text{MP–TPSI–CT}}$ for MP-TPSI cardinality testing: In a star network topology, for n parties $\text{P}_1, \text{P}_2, \cdots, \text{P}_n$ holding data sets $A_1, A_2, \cdots, A_n$ of equal size m, respectively, the goal of the $\mathcal{F}_{\text{MP–TPSI–CT}}$ is to execute a multiparty protocol Π, at the end of Π, every party P_i can know whether if its data set A_i and intersection $I = A_1 \cap A_2 \cap \cdots \cap A_n$ differ by at most t, namely $|I| \geq m - t$. The formal definition of $\mathcal{F}_{\text{MP–TPSI–CT}}$ is depicted in Figure 1.

Ideal functionality $\mathcal{F}_{\text{MP–TPSI–C}}$ for MP-TPSI computing: In a star network topology, for n parties $\text{P}_1, \text{P}_2, \cdots, \text{P}_n$ holding data sets $A_1, A_2, \cdots, A_n$ of equal size m, respectively, the goal of the $\mathcal{F}_{\text{MP–TPSI–C}}$ is to execute an multiparty protocol Π, at the end of Π, either every party P_i outputs an intersection $I = A_1 \cap A_2 \cap \cdots \cap A_n$ or outputs none $\perp$. The formal definition of $\mathcal{F}_{\text{MP–TPSI–C}}$ is described Figure 2.

4. Multiparty Threshold Private Set Intersection

In a star network topology where party P_1 to be the designated party that can communicate with other parties $\text{P}_2, \text{P}_3, \cdots, \text{P}_n$, suppose n, parties $\text{P}_1, \text{P}_2, \cdots, \text{P}_n$ with input sets $A_1, A_2, \cdots, A_n$ of equal size m, respectively, based on TFHE with distributed setup, we propose an MP-TPSI protocol, in which each party P_i can compute the intersection $I = A_1 \cap A_2 \cap \cdots \cap A_n$ only if $|I| \geq m - t$. The proposed MP-TPSI protocol is formally described in Figure 3.

4.1. Correctness. MP-TPSI cardinality testing: First we consider the situation where the MP-TPSI cardinality testing outputs true. Based on the correctness of the TFHE, we only need to illustrate $b = 0$ only if $|A_i/I| \leq t$ for any $i = 1, 2, \cdots, n$. Observe the rational interpolation polynomial

$$\begin{aligned} y_1(x) &= \frac{a_{A_1}(x) + a_{A_2}(x) + \cdots + a_{A_n}(x)}{a_{A_1}(x)} \\ &= \frac{a_{A_1\backslash I}(x) + a_{A_2\backslash I}(x) + \cdots + a_{A_n\backslash I}(x)}{a_{A_1\backslash I}(x)} \\ &= \frac{\sum_{i=1}^{n}\left(r_i \cdot \prod_{a_{i,j} \in A_i\backslash I}\left(x - a_{i,j}\right)\right)}{r_1 \cdot \prod_{a_{1,j} \in A_1\backslash I}\left(x - a_{1,j}\right)}, \end{aligned} \tag{2}$$

we can see that the degree of numerator $a_{A_1\backslash I}(x) + a_{A_2\backslash I}(x) + \cdots + a_{A_n\backslash I}(x)$ and denominator $a_{A_1\backslash I}(x)$ is at most t, and the degree of rational polynomial $y_1(x)$ is at most $2t$. Therefore, $y_1(x)$ can be computed from a total of $2t + 1$ evaluation values, and the equation $y_1(x)|_{x=z} = f(z)/a_{A_1}(z) = a_{A_1}(z) + a_{A_2}(z) + \cdots + a_{A_n}(z)/\ a_{A_1}(z)$ holds. Next, we consider the situation where the MP-TPSI cardinality testing outputs false. From the above equation, we can observe that $\gcd(a_{A_1\backslash I}(x) + a_{A_2\backslash I}(x) + \cdots + a_{A_n\backslash I}(x), a_{A_1\backslash I}(x)) = 1$. Since $|A_i\backslash I| \geq (t + 1)$, the degree of $a_{A_1\backslash I}(x) + a_{A_2\backslash I}(x) + \cdots + a_{A_n\backslash I}(x)$ and $a_{A_1\backslash I}(x)$ are at least $t + 1$, the degree of rational polynomial $y_1(x)$ is at least $2t + 3$, and hence calculating $y_1(x)$ requires at least $2t + 3$ evaluation values. However, there are only $2t + 1$ evaluation values in the MP-TPSI cardinality testing. Therefore, the equation $y_1(x)|_{x=z} = f(z)/a_{A_1}(z) = a_{A_1}(z) + a_{A_2}(z) + \cdots + a_{A_n}(z)/a_{A_1}(z)$ does not hold. From the above analysis, we are able to obtain that the MP-TPSI cardinality testing is correct.

MP-TPSI computing: If $|A_i\backslash I| > t$ for any $i = 1, 2, \cdots, n$, the MP-TPSI computing quits after the MP-TPSI cardinality testing. If $|A_i\backslash I| \leq t$, observe the rational interpolation polynomial

$$\begin{aligned} y_i(x) &= \frac{a_{A_1}(x) + a_{A_2}(x) + \cdots + a_{A_n}(x)}{a_{A_i}(x)} \\ &= \frac{a_{A_1\backslash I}(x) + a_{A_2\backslash I}(x) + \cdots + a_{A_n\backslash I}(x)}{a_{A_i\backslash I}(x)} \\ &= \frac{\sum_{i=1}^{n}\left(r_i \cdot \prod_{a_{i,j} \in A_i\backslash I}\left(x - a_{i,j}\right)\right)}{r_i \cdot \prod_{a_{1,j} \in A_1\backslash I}\left(x - a_{1,j}\right)}, \end{aligned} \tag{3}$$

we can see that the degree of numerator $a_{A_1\backslash I}(x) + a_{A_2\backslash I}(x) + \cdots + a_{A_n\backslash I}(x)$ and denominator $a_{A_i\backslash I}(x)$ are at most t, and hence $y_i(x)$ is a random polynomial with degree at most $2t + 1$. Since $\gcd(a_{A_1\backslash I}(x) + a_{A_2\backslash I}(x) + \cdots + a_{A_n\backslash I}(x), a_{A_i\backslash I}(x)) = 1$, no

Initialization: Each party P_i runs the TFHE.DisSet algorithm to get the secret key sk_i and the public key pk. P_1 chooses threshold $t \in \mathbb{N}$ and test value $z \in \mathbb{F}$, and sends t and z to each party P_i $(i = 2, 3, \cdots, n)$.

MP-TPSI Cardinality Testing:

(1) Each party P_i encodes its data set $A_i = \{a_{i,1}, a_{i,2}, \cdots, a_{i,m}\}$ as a rational polynomial $a_{A_i}(x) = r_i \cdot \prod_{a_{i,j} \in A_i} (x - a_{i,j})$, where $r_i \in \mathbb{F}$ is a uniformly random scalar, $a_{i,j} \in \mathbb{F}$.

(2) Each party P_i computes the encrypted test value $[\![a_{A_i}(z)]\!] = \mathrm{TFHE.Enc}(\mathrm{pk}, a_{A_i}(z))$, and sends it to P_1.

(3) Each party P_i computes the encrypted evaluation values $\{[\![a_{A_i}(k)]\!] = \mathrm{TFHE.Enc}(\mathrm{pk}, a_{A_i}(k)) | k \in [2t+1]\}$, and sends them to P_1.

(4) Party P_1 computes the encrypted test value $[\![f(z)]\!] = [\![a_{A_1}(z)]\!] + [\![a_{A_2}(z)]\!] + \cdots + [\![a_{A_n}(z)]\!]$, computes the encrypted evaluation values $\{[\![f(k)]\!] = [\![a_{A_1}(k)]\!] + [\![a_{A_2}(k)]\!] + \cdots + [\![a_{A_n}(k)]\!] | k \in [2t+1]\}$, computes the encrypted evaluation values $\{[\![y_1(k)]\!] = \frac{[\![f(k)]\!]}{a_{A_1}(k)} | k \in [2t+1]\}$, computes the encrypted interpolation polynomial $[\![y_1(x)]\!]$ from the encrypted evaluation values $\{(k, [\![y_1(k)]\!]) | k \in [2t+1]\}$, computes the encrypted test value $[\![y_1(z)]\!] = \frac{[\![f(z)]\!]}{a_{A_1}(z)}$, computes the encrypted prediction value $[\![b]\!] = [\![y_1(x)]\!]|_{x=z} - [\![y_1(z)]\!]$, and sends $[\![b]\!]$ to each party P_i $(i = 2, 3, \cdots, n)$.

(5) Each party P_i computes the partial decryption ciphertext $[\![b]\!]_i = \mathrm{TFHE.PartDec}(\mathrm{sk}_i, [\![b]\!])$, and sends it to P_1.

(6) Party P_1 computes the plaintext $b = \mathrm{TFHE.Comb}([\![b]\!]_1, [\![b]\!]_2, \cdots, [\![b]\!]_n)$, and sends it to each party P_i $(i = 2, 3, \cdots, n)$. If $b = 0$, each party P_i outputs $true$ and performs the next phase, otherwise outputs $false$ and aborts.

MP-TPSI Computing:

(1) Party P_1 sends the encrypted evaluation values $\{[\![f(k)]\!] | k \in [2t+1]\}$ to each party P_i $(i = 2, 3, \cdots, n)$.

(2) Each party P_i computes the partial decryption ciphertexts $\{[\![f(k)]\!]_i = \mathrm{TFHE.PartDec}(\mathrm{sk}_i, [\![f(k)]\!]) | k \in [2t+1]\}$, and sends them to P_1.

(3) Party P_1 computes the plaintexts $\{f(k) = \mathrm{TFHE.Comb}([\![f(k)]\!]_1, [\![f(k)]\!]_2, \cdots, [\![f(k)]\!]_n) | k \in [2t+1]\}$, and sends them to each party P_i $(i = 2, 3, \cdots, n)$.

(4) Each party P_i interpolates $y_i(x)$ to be the degree $2t$ rational polynomial from $2t+1$ evaluation values $\{(k, \frac{f(k)}{a_{A_i}(k)}) | k \in [n]\}$. Let the gcd of the denominator and numerator of $y_i(x)$ is 1 and D_i be the set of roots of the denominator of $y_i(x)$, each party P_i obtains the intersection $I = A_i \backslash D_i$.

Figure 3: Multiparty threshold private set intersection.

other terms will be canceled out in the numerator and denominator. Therefore, based on the correctness of the TFHE, each party P_i is able to interpolate the rational random polynomial $y_i(x)$ by utilizing $2t+1$ evaluation values. Finally, each P_i can easily compute intersection I from the set $A_i \backslash I$ of the roots of the denominator of polynomial $y_i(x)$.

5. Performance Evaluation

The proposed MP-TPSI protocol is an improvement of the TFHE-based MP-TPSI protocol [41], so we evaluate the proposed MP-TPSI protocol and the TFHE-based MP-TPSI protocol [41]. In the star network topology, we implement the proposed MP-TPSI protocol on top of the lattice-based multiparty HE library Lattigo [50] that implements the full-RNS BFV scheme [51] and its multiparty versions in Go. We run all experiments on a 32-core Intel Xeon CPU with 256 GB of RAM. For the multiparty BFV scheme in Go, to ensure 128 bits security, we choose that polynomial-degree is 4096, ciphertext-modulus is 109 bits, and plaintext-modulus is 17 bits. For ease of comparison, we perform all experiments on the same machine with 16 threads, emulate the networks latency by utilizing the Linux *tc* command, and consider a LAN with a 10 Gbps throughput and 0.2 ms round-trip time. It is worth noting that the authors of [41]

Table 3: Comparison of computational cost.

Set size	Threshold	Protocols	Computation cost (seconds)						
			$n = 2$	$n = 3$	$n = 4$	$n = 5$	$n = 6$	$n = 7$	$n = 8$
$m = 2^{10}$	$t = 2^9$	[41]	395.48	410.51	437.93	489.15	555.43	641.92	792.88
		Ours	29.97	32.12	35.18	38.60	42.17	45.67	49.43
$m = 2^{11}$	$t = 2^{10}$	[41]	919.64	964.69	1011.61	1095.70	1277.49	1478.64	1821.63
		Ours	49.54	52.09	55.35	60.91	75.03	80.12	86.56
$m = 2^{12}$	$t = 2^{11}$	[41]	2815.10	3077.36	3307.96	3593.90	4177.39	4864.73	6011.38
		Ours	92.23	100.14	108.83	121.60	134.56	147.71	161.87

did not implement their TFHE-based MP-TPSI protocol, for a fair comparison, we implement the TFHE-based MP-TPSI protocol [41] in the same experimental environment.

5.1. Analysis of Computational Cost. The computational cost of the proposed MP-TPSI protocol and the TFHE-based MP-TPSI protocol [41] under $n \in \{2, 3, \cdots, 8\}$, $m \in \{2^{10}, 2^{11}, 2^{12}\}$, and $t \in \{2^9, 2^{10}, 2^{11}\}$ are shown in Table 3. All running times are shown as an average of 10 experiments.

As shown in Figure 4, compared with the TFHE-based MP-TPSI protocol [41], the proposed MP-TPSI protocol has a better performance in terms of computational cost. Specifically, under $m = 2^{10}$ and $t = 2^9$, for $n \in \{2, 3, \cdots, 8\}$, the computational cost in the proposed MP-TPSI protocol is almost reduced by 92.4%, 92.2%, 92.0%, 92.1%, 92.4%, 92.9%, and 93.8%, respectively, compared with the TFHE-based MP-TPSI protocol [41]. Under $m = 2^{11}$ and $t = 2^{10}$, with regard to $n \in \{2, 3, \cdots, 8\}$, the proposed MP-TPSI protocol decreases by almost 94.6%, 94.6%, 94.5%, 94.4%, 94.1%, 94.6% and 95.2% respectively in computational cost in comparison with the TFHE-based MP-TPSI protocol [41]. Under $m = 2^{12}$ and $t = 2^{11}$, regarding $n \in \{2, 3, \cdots, 8\}$, the proposed MP-TPSI protocol reduces the computational cost by almost 96.7%, 96.7%, 96.7%, 96.6%, 96.8%, 97.0%, and 97.3%, respectively, than the TFHE-based MP-TPSI protocol [41].

5.2. Analysis of Communication Cost. In a star network topology, according to the selected parameters in Section 5.1, we can obtain the size of ciphertext, partial decryption ciphertext and plaintext are $|x| = 2 \times 4096 \times 109$ bits, $|x_i| = 4096 \times 109$ bits, and $|x| = 4096 \times 17$ bits, respectively. The comparison of communication cost between the proposed MP-TPSI protocol and the TFHE-based MP-TPSI protocol [41] are shown in Table 4.

For the TFHE-based MP-TPSI protocol [41], n parties first run the MPSI cardinality testing. Each P_i $(i = 2, 3, \cdots, n)$ sends $(2t + 3)$ ciphertexts $\{e_{i,j} | j \in [2t + 3]\}$ and one ciphertext e_i' to P_1. P_1 returns one ciphertext b to each P_i $(i = 2, 3, \cdots, n)$. Each P_i $(i = 2, 3, \cdots, n)$ sends one partial decryption ciphertext b: sk_i to P_1. P_1 returns one plaintext b to each P_i $(i = 2, 3, \cdots, n)$. If the MP-TPSI cardinality testing passes, n parties then run the MP-TPSI computing. Each P_i $(i = 2, 3, \cdots, n)$ sends $(3t + 4)$ ciphertexts $\{R_i(j) | j \in [3t + 4]\}$ to P_1. P_1 returns $(3t + 4)$ ciphertexts $\{e_{i,j} | j \in [3t + 3]\}$ to each P_i $(i = 2, 3, \cdots, n)$. Each P_i $(i = 2, 3, \cdots, n)$ sends $(3t + 4)$ ciphertexts $\{v_{i,j} | j \in [3t + 3]\}$ to P_1. P_1 returns $(3t + 4)$ ciphertexts $\{v_j | j \in [3t + 3]\}$ to each P_i $(i = 2, 3, \cdots, n)$. Each P_i $(i = 2, 3, \cdots, n)$ sends $(3t + 4)$ partial decryption ciphertexts $\{v_j : sk_i | j \in [3t + 4]\}$ to P_1. P_1 returns $(3t + 4)$ plaintexts $\{v_j | j \in [3t + 3]\}$ to each P_i $(i = 2, 3, \cdots, n)$. Therefore, the communication cost of the designated party P_1 is $(n - 1) \times (6t + 9) \times |x| + (n - 1) \times (3t + 5) \times |x|$ (namely, $\mathcal{O}(tn)$), the communication cost of each P_i $(i = 2, 3, \cdots, n)$ is $(8t + 12) \times |x| + (3t + 5) \times |x_i|$ (namely, $\mathcal{O}(t)$), and the total communication cost is $(n - 1) \times ((14t + 21) \times |x| + (3t + 5) \times |x_i| + (3t + 5) \times |x|)$ bits.

For our MP-TPSI protocol, n parties first run the MP-TPSI cardinality testing. Each P_i $(i = 2, 3, \cdots, n)$ sends $(2t + 1)$ ciphertexts $\{a_{A_i}(k) | k \in [2t + 1]\}$ and one ciphertext $a_{A_i}(z)$ to P_1. P_1 returns one ciphertext b to each P_i $(i = 2, 3, \cdots, n)$. Each P_i $(i = 2, 3, \cdots, n)$ sends one partial decryption ciphertext b_i to P_1. P_1 returns one plaintext b to each P_i $(i = 2, 3, \cdots, n)$. If the MP-TPSI cardinality testing passes, n parties then run the MP-TPSI computing. P_1 returns $(2t + 1)$ ciphertexts $\{f(k) | k \in [2t + 1]\}$ to each P_i $(i = 2, 3, \cdots, n)$. Each P_i $(i = 2, 3, \cdots, n)$ sends $(2t + 1)$ partial decryption ciphertexts $\{f(k)_i | k \in [2t + 1]\}$ to P_1. P_1 returns $(2t + 1)$ plaintexts $\{f(k) | k \in [2t + 1]\}$ to each P_i $(i = 2, 3, \cdots, n)$. Therefore, the communication cost of the designated party P_1 is $(n - 1) \times (2t + 9) \times |x| + (n - 1) \times (2t + 2) \times |x|$ (namely, $\mathcal{O}(tn)$), the communication cost of each P_i $(i = 2, 3, \cdots, n)$ is $(2t + 2) \times |x| + (2t + 2) \times |x_i|$ (namely, $\mathcal{O}(t)$), the total communication cost is $(n - 1) \times ((4t + 4) \times |x| + (2t + 2) \times |x_i| + (2t + 2) \times |x|)$ bits.

As shown in Figure 5, compared with the TFHE-based MP-TPSI protocol [41], the proposed MP-TPSI protocol has a better performance in terms of communication cost. Specifically, when comparing with $m = 2^{10}$ and $t = 2^9$, for $n \in \{2, 3, \cdots, 8\}$ parties, the communication cost in the proposed MP-TPSI protocol is almost reduced by 67.3%, 67.3%, 67.3%, 67.3%, 67.3%, 67.3%, and 67.3%, respectively, compared with the TFHE-based MP-TPSI protocol [41]. When comparing with $m = 2^{11}$ and $t = 2^{10}$, with regard to $n \in \{2, 3, \cdots, 8\}$ parties, the proposed MP-TPSI protocol decreases by almost 67.2%, 67.2%, 67.2%, 67.2%, 67.2%, 67.2%, and 67.2%, respectively, in communication cost in comparison with the TFHE-based MP-TPSI protocol [41]. When comparing with $m = 2^{12}$ and $t = 2^{11}$, regarding $n \in \{2, 3, \cdots, 8\}$ parties, the proposed MP-TPSI protocol reduces the communication cost by almost 67.2%, 67.2%, 67.2%, 67.2%, 67.2%, 67.2% and 67.2% respectively than the TFHE-based MP-TPSI protocol [41].

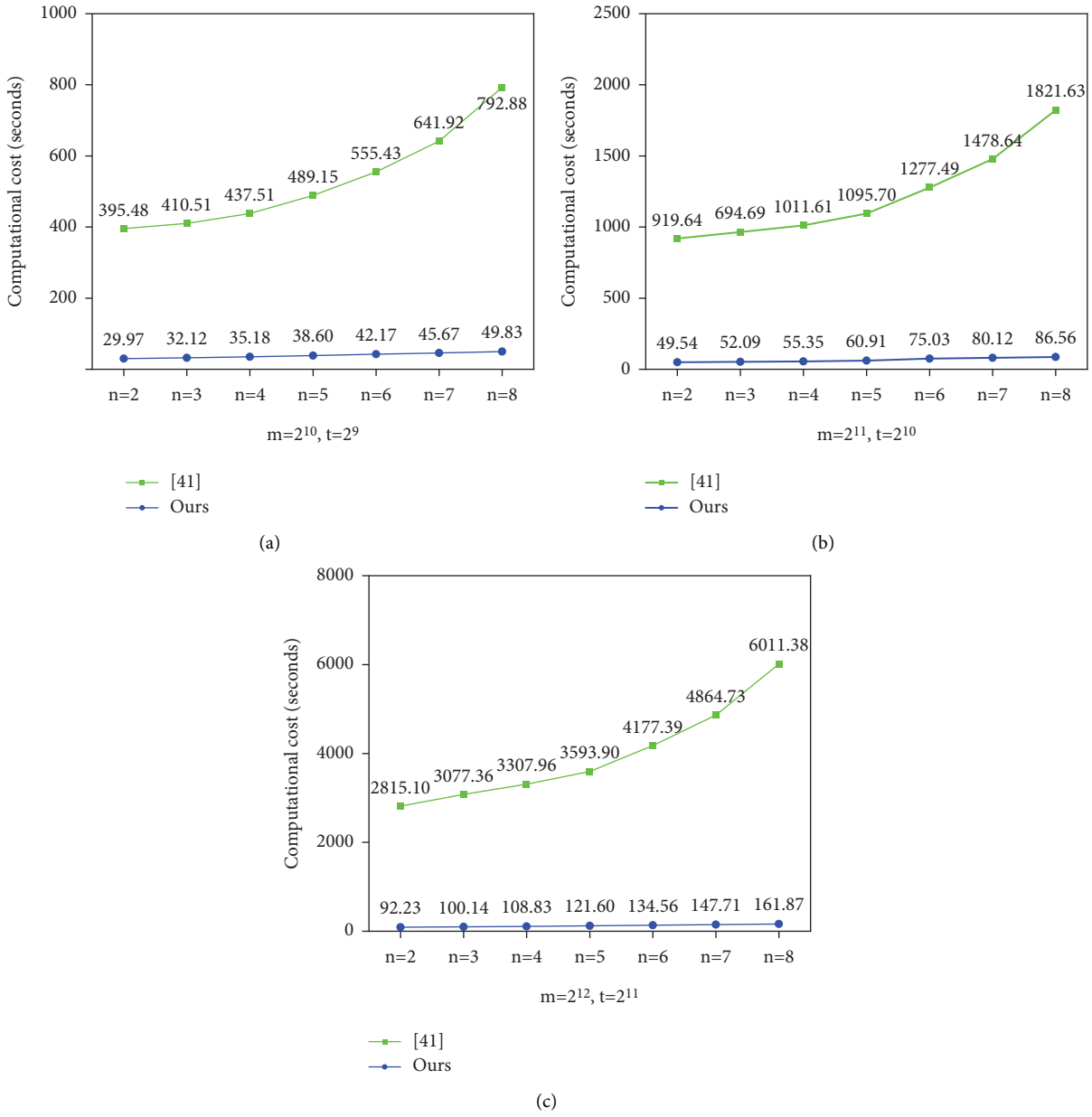


Figure 4: Comparison of computational cost.

Table 4: Comparison of communication costs.

Set size	Threshold	Protocols	Communication cost (GB)						
			$n = 2$	$n = 3$	$n = 4$	$n = 5$	$n = 6$	$n = 7$	$n = 8$
$m = 2^{10}$	$t = 2^9$	[41]	0.84	1.68	2.52	3.36	4.20	5.04	5.88
		Ours	0.27	0.55	0.82	1.10	1.37	1.65	1.92
$m = 2^{11}$	$t = 2^{10}$	[41]	1.68	3.35	5.03	6.71	8.39	10.06	11.74
		Ours	0.55	1.10	1.65	2.20	2.75	3.30	3.85
$m = 2^{12}$	$t = 2^{11}$	[41]	3.35	6.70	10.06	13.41	16.76	20.11	23.46
		Ours	1.10	2.20	3.29	4.39	5.49	6.59	7.69

6. Security Analysis

In security model, we assume an environment $\mathcal{Z}$ who is able to corrupt the set $\mathcal{A}^*$ of $n^* < n$ parties, a simulator $\mathcal{S}$ knows the output value $w \in \{\text{true}, \text{false}\}$ of the ideal functionality $\mathcal{F}_{\text{MP-TPSI-CT}}$. If $w = \text{true}$, $\mathcal{S}$ sets $b = 0$, otherwise sets $b = 1$. $\mathcal{S}$ also has the output value I or $\perp$ of the ideal functionality $\mathcal{F}_{\text{MP-TPSI-C}}$. In addition, for each corrupt party $\mathcal{A}_i \in \mathcal{A}^*$, $\mathcal{S}$

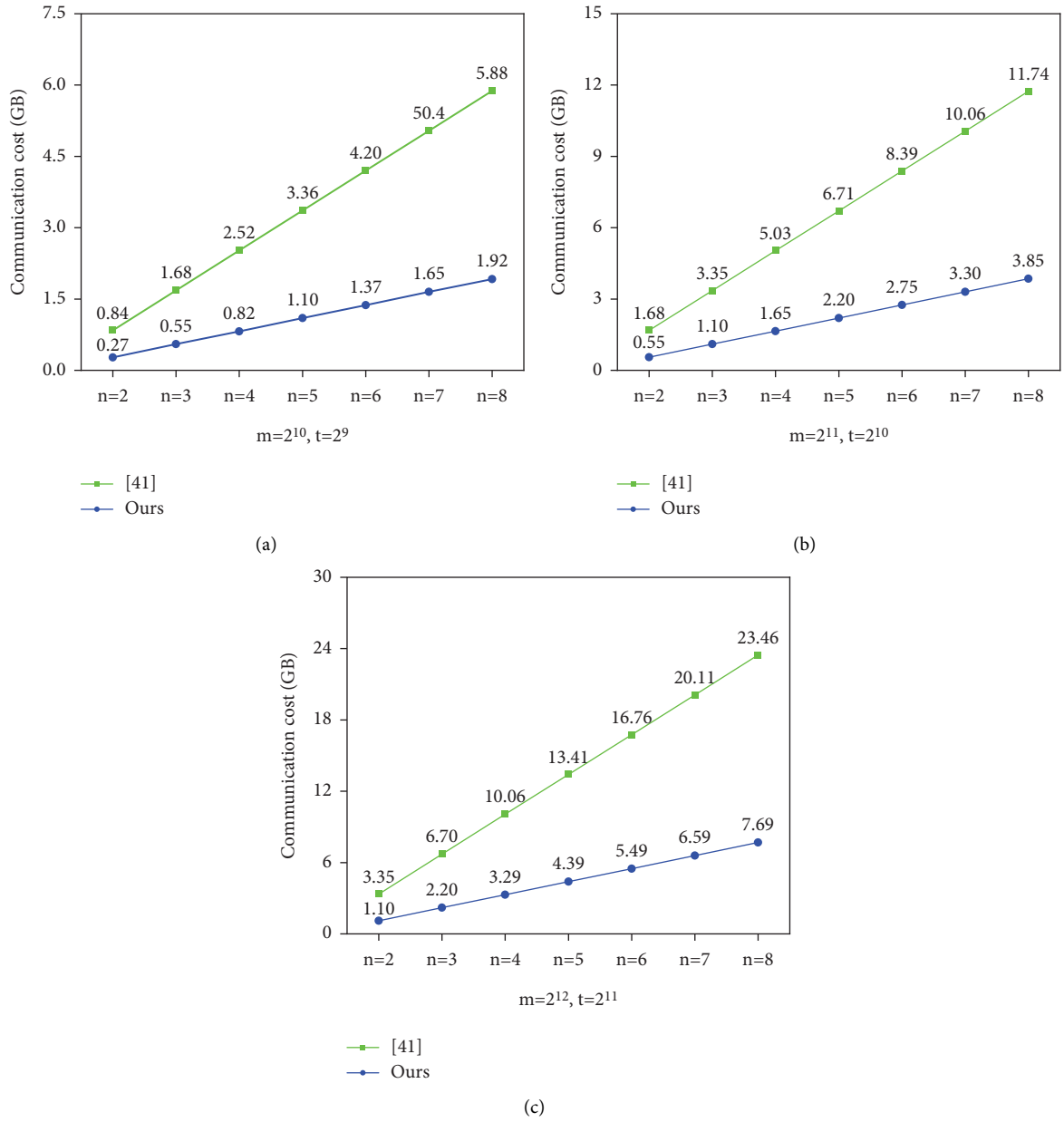


Figure 5: Comparison of communication cost.

has the input data set A_i and random value r_i of $\mathcal{A}_i$. The simulation strategy of $\mathcal{S}$ is described as follows.

Initialization. $\mathcal{S}$ represents each honest party P_i running the distributed setup TFHE.DisSet algorithm just like in the real world. $\mathcal{S}$ also knows the secret key share $\{sk_i\}_{\mathcal{A}_i \in \mathcal{A}^*}$ of all corrupt parties $\mathcal{A}^*$.

MP-TPSI Cardinality Testing. $\mathcal{S}$ does the following:

In Step 1, $\mathcal{S}$ encodes the intersection set $I = \{a_1, a_2, \cdots, a_I\}$ as a rational polynomial $a_I(x) = \prod_{a_i \in I}(x - a_i)$, chooses randomly a rational polynomial $u(x)$ of degree t, and computes a rational polynomial $f(x) = a_I(x) \cdot u(x)$.

In Steps 2–4, whenever each honest party P_i sends any encrypted value, $\mathcal{S}$ computes the ciphertext $0 = \text{TFHE.Enc}(0)$ employing fresh random value on behalf of P_i just like in the real world.

In Steps 5–6, instead of computing the value b_i by executing the partial decryption algorithm $\text{TFHE.PartDec}(sk_i, b)$ on behalf of every honest party P_i just like in the real world, $\mathcal{S}$ calculates the value b_i by executing the simulator algorithm $\{b_i\}_{P_i \in \mathcal{P}} = \text{TFHE.}\mathcal{S}(\mathcal{C}, b, b, \{sk_i\}_{\mathcal{A}_i \in \mathcal{A}^*})$, where $\mathcal{C}$ represents the computation circuit performed by P_1 to calculate the value b just like in the real world, this corresponds to the ideal world, $\mathcal{P}$ denotes the set of the honest parties. If P_1 is honest, $\mathcal{S}$ sends the evaluation value b just like in the real world.

MPSI Computing. $\mathcal{S}$ does the following:

In steps 1, instead of computing the value $f(k)_i$ by executing the partial decryption algorithm TFHE.PartDec $(sk_i, f(k))$ on behalf of every honest party P_i just like in the real world, $\mathcal{S}$ calculates the value $f(k)_i$ by executing the simulator algorithm $\{f(k)_i\}_{P_i \in \mathcal{P}} = \text{TFHE}.\mathcal{S}(\mathcal{C}, f(k), f(k)_i, \{sk_i\}_{\mathcal{A}_i \in \mathcal{A}^*})$, where $\mathcal{C}$ represents the computation circuit performed by P_1 to calculate the value $f(k)$ just like in the real world, this corresponds to the ideal world. If P_1 is honest, $\mathcal{S}$ sends the evaluation value $f(k)$ just like in the real world.

In steps 2, $\mathcal{S}$ outputs the interpolation polynomial $y_i(x)$ and set intersection I on behalf of every honest party P_i just like in the real world.

Next, suppose a simulator $\mathcal{S}_h$, we show that the proposed MP-TPSI protocol is secure against the environment $\mathcal{Z}$ in the semi-honest setting through a set of computationally indistinguishable consecutive hybrids.

Hybrid$_0$: $\mathcal{S}_h$ simulates all operations of honest parties just like in the real world.

Hybrid$_1$: $\mathcal{S}_h$ simulates a ideal functionality $\mathcal{F}_{\text{MP–TPSI–CT}}$. If $|A_i \backslash I| \le t$, $\mathcal{S}_h$ returns true, otherwise returns false.

Hybrid$_2$: $\mathcal{S}_h$ simulates the partial decryption performed by the honest parties just like in the ideal world. For each $k \in [2t+1]$, $\mathcal{S}_h$ computes the partial decryption as $\{f(k)_i\}_{P_i \in \mathcal{P}} = \text{TFHE}.\mathcal{S}(\mathcal{C}, f(k), f(k)_i, \{sk_i\}_{\mathcal{A}_i \in \mathcal{A}^*})$. The rational polynomial $f(k)$ is still calculated as in the real world.

Hybrid$_3$: Instead of calculating the rational polynomial $f(k)$ just like in the real world, $\mathcal{S}_h$ selects randomly a rational polynomial $u(x)$ of degree t, and computes a rational polynomial $f(x) = a_I(x) \cdot u(x)$.

Hybrid$_4$: $\mathcal{S}_h$ simulates the ciphertexts computed by any honest parties as encryption of 0, just like $\mathcal{S}$ does in the ideal world.

Theorem 1. *Assuming that the TFHE scheme is secure, the proposed MP-TPSI protocol $\Pi_{MP-TPSI}$ securely realizes $\mathcal{F}_{MP-TPSI-CT}$ and $\mathcal{F}_{MP-TPSI-C}$ in a star network topology, and resists a semi-honest adversary who has the ability to corrupt up to $(n-1)$ parties. It can be proved by Lemma 1–4 in Appendix.*

7. Conclusion

In this study, using sparse polynomial interpolation and TFHE, we introduce a MP-TPSI protocol with low communication complexity, in which the communication complexity only depends on the threshold t and the number of parties n, not on the size of data set m. Compared with the existing MP-TPSI protocols, the proposed MP-TPSI protocol utilizes the same form of evaluation polynomial in the cardinality testing and intersection computing phases, which enables the parties to transmit and compute only a small number of evaluation values, and hence reduces the communication and computational cost. Performance evaluation demonstrates that our MP-TPSI protocol requires 92.0% and 67.2% less computational and communication costs respectively than the competitive MP-TPSI protocol. Moreover, the proposed MP-TPSI protocol can achieve the correctness of the intersection result, and ensure the security of the data of the parties, that is, the semi-honest adversary cannot learn additional information beyond the intersection. In the future, we will explore the MP-TPSI protocol in the broadcast communication setting, optimize the rounds of MP-TPSI, and design a more efficient MP-TPSI protocol with malicious security.

Appendix

Lemma 1. *Hybrid$_0$ and Hybrid$_1$ is computationally indistinguishable due to the correctness of the MP-TPSI protocol $\Pi_{MP-TPSI}$.*

Proof. The difference between Hybrid$_0$ and Hybrid$_1$ is that in Hybrid$_0$, $\mathcal{S}_h$ calls $\mathcal{F}_{\text{MP–TPSI–CT}}$ honestly, while in Hybrid$_1$, $\mathcal{S}_h$ simulates the ideal functionality $\mathcal{F}_{\text{MP–TPSI–CT}}$ that returns *true* if $|A_i \backslash I| \le t$ and false otherwise. In Hybrid$_0$, the output result of $\mathcal{F}_{\text{MP–TPSI–CT}}$ is correct due to the correctness of our protocol $\Pi_{\text{MP–TPSI}}$. In Hybrid$_1$, the output result of $\mathcal{F}_{\text{MP–TPSI–CT}}$ is always correct. Therefore, Hybrid$_0$ and Hybrid$_1$ are computationally indistinguishable.

Lemma 2. *Hybrid$_1$ and Hybrid$_2$ is computationally indistinguishable due to the simulation-based security of TFHE [42].*

Proof. The difference between Hybrid$_1$ and Hybrid$_2$ is that in Hybrid$_1$, $\mathcal{S}_h$ computes the partial decryption of TFHE of all honest parties just like in the real world, while in Hybrid$_2$, $\mathcal{S}_h$ simulates the partial decryption by running TFHE.$\mathcal{S}$. If there is an $\mathcal{Z}$ that is able to distinguish Hybrid$_1$ and Hybrid$_2$ with a non-negligible probability ϵ, we are able to build a reduction algorithm $\mathcal{B}$ that has the ability to break TFHE's simulation-based security with a non-negligible probability ϵ'. $\mathcal{B}$ interacts with a challenger $\mathcal{C}$ in TFHE's simulation-based security game, and interacts with $\mathcal{Z}$ in the game of Hybrid$_1$ and Hybrid$_2$. The corrupt parties in the game of $\mathcal{B}$ and $\mathcal{Z}$ are the same as the corrupt parties in the game of $\mathcal{B}$ and $\mathcal{C}$. $\mathcal{B}$ sends the public key share pk_i and secret key share sk_i of the corrupt party that it receives from $\mathcal{Z}$ to $\mathcal{C}$, and sends the public key share pk_i of the honest party that it receives from $\mathcal{C}$ to $\mathcal{Z}$. $\mathcal{B}$ sends the corrupt party's input data set A_i and random value R_i that it receives from $\mathcal{Z}$ to $\mathcal{C}$. $\mathcal{B}$ sends the honest party's ciphertext that it receives from $\mathcal{C}$ to $\mathcal{Z}$. $\mathcal{B}$ sends the evaluation circuit of rational polynomial $f(x)$ to $\mathcal{C}$. $\mathcal{C}$ returns the honest party's partial decryption to $\mathcal{B}$. $\mathcal{B}$ continues to interact with $\mathcal{Z}$ for the rest progress just like in Hybrid$_1$. In the interaction process, if $\mathcal{C}$ sends honestly computed partial decryption, then the interaction process between $\mathcal{B}$ and $\mathcal{Z}$ is associated with Hybrid$_1$, if the partial decryption is simulated by TFHE.$\mathcal{S}$, the interaction process between $\mathcal{B}$ and $\mathcal{Z}$ is associated with Hybrid$_2$.

From above, if there is an $\mathscr{Z}$ that is able to distinguish Hybrid_1 and Hybrid_2 with a non-negligible probability ϵ, $\mathscr{B}$ has the ability to break TFHE's simulation-based security with a non-negligible probability ϵ', this contradicts with TFHE's simulation-based security [42]. Therefore, Hybrid_1 is computationally indistinguishable from Hybrid_2.

Lemma 3. *Hybrid_2 is statistically close to Hybrid_3.*

Proof. The difference between Hybrid_2 and Hybrid_3 is how the rational polynomial $f(x)$ is calculated. In Hybrid_2, $\mathcal{S}_h$ computes

$$\begin{aligned} f(x) &= \sum_{\mathrm{P}_i \in \mathscr{P}} \left(r_i \cdot \prod_{a_{i,j} \in A_i} \left(x - a_{i,j} \right) \right) = a_I(x) \cdot \sum_{i \in [n]} \left(r_i \cdot \prod_{a_{i,j} \in A_i} \left(x - a_{i,j} \right) \right) \\ &= a_I(x) \cdot \sum_{\mathrm{P}_i \in \mathscr{A}} \left(r_i \cdot \prod_{a_{i,j} \in A_i} \left(x - a_{i,j} \right) \right) + a_I(x) \cdot \sum_{\mathrm{P}_i \in \mathscr{P}} \left(r_i \cdot \prod_{a_{i,j} \in A_i} \left(x - a_{i,j} \right) \right) \\ &= a_I(x) \cdot v_1(x) + a_I(x) \cdot v_2(x) \\ &= a_I(x) \cdot \left(v_1(x) + v_2(x) \right). \end{aligned} \tag{A.1}$$

For each $i \in [n]$, $\text{Deg}(r_i \cdot a_{A_i \setminus I}(x)) = t$. Thus, $\text{Deg}(v_1(x)) = \text{Deg}(v_2(x)) = t$. Since $v_2(x)$ is statistically close to a uniform random polynomial of degree t, we can obtain $f(x) = a_I(x) \cdot (v_1(x) + v_2(x)) = a_I(x) \cdot u(x)$, where $u(x)$ is uniform random polynomials of degree t. In Hybrid_3, $\mathcal{S}_h$ computes $f(x) = a_I(x) \cdot u(x)$. Therefore, the distribution of $f(x)$ in Hybrid_2 is statistically close to the distribution of $f(x)$ in Hybrid_3.

Lemma 4. *Hybrid_3 and Hybrid_4 is computationally indistinguishable due to the semantic security of TFHE [42].*

Proof. The difference between Hybrid_3 and Hybrid_4 is that in Hybrid_3, $\mathcal{S}_h$ computes the encryption of TFHE of all honest parties just like in the real world, while in Hybrid_4, $\mathcal{S}_h$ computes the encryption of 0.

If there is an $\mathscr{Z}$ that is able to distinguish Hybrid_3 and Hybrid_4 with a non-negligible probability ϵ, we are able to build a reduction algorithm $\mathscr{B}$ that has the ability to break TFHE's semantic security with a non-negligible probability ϵ'. $\mathscr{B}$ interacts with a challenger $\mathscr{C}$ in TFHE's semantic security game, and interacts with $\mathscr{Z}$ in the game of Hybrid_3 and Hybrid_4. The corrupt parties in the game of $\mathscr{B}$ and $\mathscr{Z}$ are the same as the corrupt parties in the game of $\mathscr{B}$ and $\mathscr{C}$. $\mathscr{B}$ sends the public key share pk_i and secret key share sk_i of the corrupt party that it receives from $\mathscr{Z}$ to $\mathscr{C}$, and sends the public key share pk_i of the honest party that it receives from $\mathscr{C}$ to $\mathscr{Z}$. $\mathscr{B}$ sends the honestly generated plaintext and 0 to $\mathscr{C}$. $\mathscr{C}$ returns their ciphertexts to $\mathscr{B}$. $\mathscr{B}$ uses the ciphertext it receives from $\mathscr{C}$ to interact with $\mathscr{Z}$. $\mathscr{B}$ continues to interact with $\mathscr{Z}$ for the rest progress just like in Hybrid_3. In the interaction process, if $\mathscr{C}$ sends honestly computed ciphertext, then the interaction process between $\mathscr{B}$ and $\mathscr{Z}$ is associated with Hybrid_3, if the ciphertext is computed as 0's encryption, the interaction between $\mathscr{B}$ and $\mathscr{Z}$ is associated with Hybrid_4.

From above, if there is an $\mathscr{Z}$ that is able to distinguish Hybrid_3 and Hybrid_4 with a non-negligible probability ϵ, $\mathscr{B}$ has the ability to break TFHE's simulation-based security with a non-negligible probability ϵ', this contradicts with TFHE's semantic security [42]. Therefore, Hybrid_3 is computationally indistinguishable from Hybrid_4.

Data Availability

No data were used to support this study.

Conflicts of Interest

The authors declare no conflicts of interest.

Acknowledgments

This work was supported by the National Natural Science Foundation of China (Grant no. U19B2021) and the National Natural Science Foundation of China (Grant no. 62172427).

References

[1] C. Meadows, "A more efficient cryptographic matchmaking protocol for use in the absence of a continuously available third party," in *Proceedings of the IEEE Symposium on Security & Privacy*, pp. 134–137, Oakland, CA, USA, April 1986.

[2] J. R. Troncoso-Pastoriza, S. Katzenbeisser, and M. Celik, "Privacy preserving error resilient DNA searching through oblivious automata," in *Proceedings of the ACM Conference on Computer & Communications Security*, pp. 519–528, Alexandria, VA, USA, October 2007.

[3] S. Nagaraja, P. Mittal, C. Y. Hong, M. Caesar, and N. Borisov, "BotGrep: finding P2P bots with structured graph analysis," in *Proceedings of the 19th USENIX Security Symposium*, pp. 95–110, Washington, DC, USA, August 11-13, 2010.

[4] D. Demmler, P. Rindal, M. Rosulek, and N. Trieu, "PIR-PSI: scaling private contact discovery," *Proceedings on Privacy Enhancing Technologies*, vol. 2018, no. 4, pp. 159–178, 2018.

[5] D. Mutchler, "Matching secrets in the absence of a continuously available trusted authority," *IEEE Transactions on Software Engineering*, vol. SE-13, no. 2, pp. 289–292, 1987.

[6] D. Dachman-Soled, T. Malkin, M. Raykova, and M. Yung, "Efficient robust private set intersection," in *Proceedings of the*

International Conference on Applied Cryptography and Network Security, pp. 125–142, Paris-Rocquencourt, France, June 2009.

[7] E. D. Cristofaro, J. Kim, and G. Tsudik, "Linear-complexity private set intersection protocols secure in malicious model," in *Proceedings of the Advances in Cryptology - ASIACRYPT 2010 - 16th International Conference on the Theory and Application of Cryptology and Information Security*, pp. 213–231, Singapore, December 2010.

[8] E. D. Cristofaro and G. Tsudik, "Practical private set intersection protocols with linear complexity," in *Proceedings of the 14th International Conference on Financial Cryptography & Data Security*, pp. 143–159, Tenerife, Canary Islands, January 2010.

[9] Y. Huang, D. Evans, and J. Katz, "Private set intersection: are garbled circuits better than custom protocols?" in *Proceedings of the 19th Network and Distributed Security Symposium*, pp. 1–15, San Diego, CA, USA, February 2012.

[10] C. Hazay and K. Nissim, "Efficient set operations in the presence of malicious adversaries," *Journal of Cryptology*, vol. 25, no. 3, pp. 383–433, 2012.

[11] C. Hazay, "Oblivious polynomial evaluation and secure set-intersection from algebraic PRFs," in *Proceedings of the 20th Annual TCC Worldwide Online Conference*, pp. 90–120, 2012.

[12] C. Dong, L. Chen, and Z. Wen, "When private set intersection meets big data: an efficient and scalable protocol," in *Proceedings of the 20th ACM SIGSAC Conference on Computer & communications security*, pp. 789–800, Berlin, Germany, November 2013.

[13] B. Pinkas, T. Schneider, and M. Zohner, "Faster private set intersection based on OT extension," *ACM Transactions on Privacy & Security*, vol. 21, no. 2, pp. 797–812, 2014.

[14] B. Pinkas, T. Schneider, and G. Segev, "Phasing: private set intersection using permutation-based hashing," in *Proceedings of the 24th USENIX Security Symposium*, pp. 515–530, Washington, DC, USA, August 2015.

[15] V. Kolesnikov, R. Kumaresan, M. Rosulek, and N. Trieu, "Efficient batched oblivious PRF with applications to private set intersection," in *Proceedings of the 23rd ACM SIGSAC Conference on Computer & Communications Security*, pp. 818–829, Vienna, Austria, October 2016.

[16] M. J. Freedman, C. Hazay, K. Nissim, and B. Pinkas, "Efficient set intersection with simulation-based security," *Journal of Cryptology*, vol. 29, no. 1, pp. 115–155, 2016.

[17] M. Orru, E. Orsini, and P. Scholl, "Actively secure 1-out-of-N OT extension with application to private set intersection," in *Proceedings of the Cryptographers' Track at the RSA Conference - CTRSA 2017*, pp. 381–396, San Francisco, CA, USA, February 2018.

[18] P. Rindal and M. Rosulek, "Improved private set intersection against malicious adversaries," in *Proceedings of the Advances in Cryptology - EUROCRYPT 2017 - 36th Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 235–259, Paris, France, May 2017.

[19] P. Rindal and M. Rosulek, "Malicious-secure private set intersection via dual execution," in *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, pp. 1229–1242, Dallas, TX, USA, October 2017.

[20] B. Pinkas, T. Schneider, and M. Zohner, "Scalable private set intersection based on OT extension," *ACM Transactions on Privacy and Security*, vol. 21, no. 2, pp. 1–35, 2018.

[21] B. Pinkas, T. Schneider, C. Weinert, and U. Wieder, "Efficient circuit-based PSI via cuckoo hashing," in *Proceedings of the Advances in Cryptology - EUROCRYPT 2018 - 37th Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 125–157, Tel Aviv, Israel, May 2018.

[22] B. Pinkas, M. Rosulek, N. Trieu, and A. Yanai, "SpOT-Light: lightweight private set intersection from sparse OT extension," in *Proceedings of the Advances in Cryptology - CRYPTO 2019 - 39th Annual International Cryptology Conference*, pp. 401–431, Santa Barbara, CA, USA, August 2019.

[23] B. Pinkas, M. Rosulek, N. Trieu, and A. Yanai, "PSI from paxos: fast, malicious private set intersection," in *Proceedings of the Advances in Cryptology - EUROCRYPT 2020 - 39th Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 739–767, Zagreb, Croatia, May 2020.

[24] A. C. Yao, "Protocols for secure computations," in *Proceedings of the 23rd Annual IEEE Symposium on Foundations of Computer Science*, pp. 1–5, Chicago, IL, USA, November 1982.

[25] S. Even, O. Goldreich, and A. Lempel, "A randomized protocol for signing contracts," *Communications of the ACM*, vol. 28, no. 6, pp. 637–647, 1985.

[26] R. L. Rivest, L. M. Adleman, and M. L. Dertouzos, "On data banks and privacy homomorphisms," *Foundations of Secure Computation*, vol. 76, no. 4, pp. 169–179, 1978.

[27] M. J. Freedman, Y. Ishai, B. Pinkas, and O. Reingold, "Keyword search and oblivious pseudorandom functions," in *Proceedings of the Theory of Cryptography Conference - TCC 2005*, pp. 303–324, Cambridge, MA, USA, February 2005.

[28] L. Kissner and D. Song, "Privacy-preserving set operations," in *Proceedings of the Advances in Cryptology - CRYPTO 2005 - 25th Annual International Cryptology Conference*, pp. 241–257, Santa Barbara, CA, USA, August 2005.

[29] A. Miyaji and S. Nishida, "A scalable multiparty private set intersection," in *Proceedings of the International Conference on Network and System Security*, pp. 376–385, New York, NY, USA, November 2015.

[30] C. Hazay and M. Venkitasubramaniam, "Scalable multi-party private set-intersection," in *Proceedings of the Public-Key Cryptography - PKC 2017 - 20th IACR International Conference on Practice and Theory in Public-Key Cryptography*, pp. 175–203, Amsterdam, Netherlands, May 2017.

[31] V. Kolesnikov, N. Matania, B. Pinkas, M. Rosulek, and N. Trieu, "Practical multi-party private set intersection from symmetric-key techniques," in *Proceedings of the ACM SIGSAC Conference on Computer & Communications Security*, pp. 1257–1272, Dallas, TX, USA, November 2017.

[32] R. Inbar, E. Omri, and B. Pinkas, "Efficient scalable multiparty private set-intersection via garbled bloom filters," in *Proceedings of the 11th International Conference on Security and Cryptography for Networks, Lecture Notes in Computer Science*, vol. 7, pp. 235–252, Amalfi, Italy, September 2018.

[33] S. Ghosh and T. Nilges, "An algebraic approach to maliciously secure private set intersection," in *Proceedings of the Advances in Cryptology - EUROCRYPT 2019 - 38th Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 154–185, Darmstadt, Germany, May 2019.

[34] L. Lu and N. Ding, "Multi-party private set intersection in vertical federated learning," in *Proceedings of the 19th International Conference on Trust, Security and Privacy in Computing and Communications*, pp. 707–714, Guangzhou, China, January 2020.

[35] A. Kavousi, J. Mohajeri, and M. Salmasizadeh, "Efficient scalable multi-party private set intersection using oblivious PRF," in *Proceedings of the 17th International Workshop on*

Security and Trust Management, pp. 81–99, Darmstadt, Germany, October 2021.

[36] A. Bay, Z. Erkin, J. H. Hoepman, S. Samardjiska, and J. Vos, "Practical multi-party private set intersection protocols," *IEEE Transactions on Information Forensics and Security*, vol. 17, pp. 1–15, 2022.

[37] Q. Yang, Y. Liu, T. Chen, and Y. Tong, "Federated machine learning," *ACM Transactions on Intelligent Systems and Technology*, vol. 10, no. 2, pp. 1–19, 2019.

[38] S. Ghosh and M. Simkin, "The communication complexity of threshold private set intersection," in *Proceedings of the Advances in Cryptology - CRYPTO 2019 - 39th Annual International Cryptology Conference*, pp. 3–29, Santa Barbara, CA, USA, August 2019.

[39] R. A. Mahdavi, T. Humphries, B. Kacsmar et al., "Practical over-threshold multi-party private set intersection," in *Proceedings of theAnnual Computer Security Applications Conference*, pp. 772–783, Austin, USA, December 2020.

[40] P. Branco, N. Dttling, and S. Pu, "Multiparty cardinality testing for threshold private intersection," in *Proceedings of the Public-Key Cryptography - PKC 2021 - 24th IACR International Conference on Practice and Theory of Public Key Cryptography*, pp. 32–60, Virtual Event, May 2021.

[41] S. Badrinarayanan, P. Miao, S. Raghuraman, and P. Rindal, "Multi-party threshold private set intersection with sublinear communication," in *Proceedings of the Public-Key Cryptography - PKC 2021 - 24th IACR International Conference on Practice and Theory of Public Key Cryptography*, pp. 349–379, Virtual Event, May 2021.

[42] D. Boneh, R. Gennaro, S. Goldfeder, A. Jain, and A. Sahai, "Threshold cryptosystems from threshold fully homomorphic encryption," in *Proceedings of the Advances in Cryptology - CRYPTO 2018 - 38th Annual International Cryptology Conference*, pp. 565–596, Santa Barbara, CA, USA, August 2018.

[43] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," in *Proceedings of the Advances in Cryptology - EUROCRYPT 1999 - International Conference on the Theory and Application of Cryptographic Techniques*, pp. 223–238, Prague, Czech Republic, May 1999.

[44] B. H. Bloom, "Space/time trade-offs in hash coding with allowable errors," *Communications of the ACM*, vol. 13, no. 7, pp. 422–426, 1970.

[45] R. Cramer, R. Gennaro, and B. Schoenmakers, "A secure and optimally efficient multi-authority election scheme," in *Proceedings of the Advances in Cryptology - EUROCRYPT 1997 - International Conference on the Theory and Application of Cryptographic Techniques*, pp. 103–118, Konstanz, Germany, May 1997.

[46] M. J. Freedman, K. Nissim, and B. Pinkas, "Efficient private matching and set intersection," in *Proceedings of the Advances in Cryptology - EUROCRYPT 2004 - International Conference on the Theory and Application of Cryptographic Techniques*, pp. 19–38, Interlaken, Switzerland, May 2004.

[47] A. Abadi, S. J. Murdoch, and T. Zacharias, "Polynomial representation is tricky: maliciously secure private set intersection revisited," in *Proceedings of the 26th European Symposium on Research in Computer Security*, pp. 721–742, Virtual Event, October 2021.

[48] T. Elgamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," *IEEE Transactions on Information Theory*, vol. 31, no. 4, pp. 469–472, 1985.

[49] R. Canetti, "Universally composable security: a new paradigm for cryptographic protocols," in *Proceedings of the 42nd Annual Symposium on Foundations of Computer Science*, pp. 136–145, Las Vegas, NV, USA, October 2001.

[50] Lattigo, "Tunesight," 2022, https://github.com/tuneinsight/lattigo.

[51] S. Halevi, Y. Polyakov, and V. Shoup, "An improved RNS variant of the BFV homomorphic encryption scheme," in *Proceedings of the Topics in Cryptology - CT-RSA 2019 - the Cryptographers' Track at the RSA Conference*, pp. 83–105, San Francisco, CA, USA, March 2019.

Hindawi
Security and Communication Networks
Volume 2024, Article ID 9864701, 1 page
https://doi.org/10.1155/2024/9864701

Retraction

Retracted: Jamming Meets Antijamming: A Survey of GPS Communication Networks

Security and Communication Networks

Received 8 January 2024; Accepted 8 January 2024; Published 9 January 2024

This article has been retracted by Hindawi following an investigation undertaken by the publisher [1]. This investigation has uncovered evidence of one or more of the following indicators of systematic manipulation of the publication process:

(1) Discrepancies in scope

(2) Discrepancies in the description of the research reported

(3) Discrepancies between the availability of data and the research described

(4) Inappropriate citations

(5) Incoherent, meaningless and/or irrelevant content included in the article

(6) Manipulated or compromised peer review

The presence of these indicators undermines our confidence in the integrity of the article's content and we cannot, therefore, vouch for its reliability. Please note that this notice is intended solely to alert readers that the content of this article is unreliable. We have not investigated whether authors were aware of or involved in the systematic manipulation of the publication process.

Wiley and Hindawi regrets that the usual quality checks did not identify these issues before publication and have since put additional measures in place to safeguard research integrity.

We wish to credit our own Research Integrity and Research Publishing teams and anonymous and named external researchers and research integrity experts for contributing to this investigation.

The corresponding author, as the representative of all authors, has been given the opportunity to register their agreement or disagreement to this retraction. We have kept a record of any response received.

References

[1] Y. Yang, "Jamming Meets Antijamming: A Survey of GPS Communication Networks," *Security and Communication Networks*, vol. 2022, Article ID 9438027, 7 pages, 2022.

Hindawi
Security and Communication Networks
Volume 2022, Article ID 9438027, 7 pages
https://doi.org/10.1155/2022/9438027

Review Article

Jamming Meets Antijamming: A Survey of GPS Communication Networks

Yifan Yang

School of Cybersecurity, Northwestern Polytechnical University, Xi'an 710072, China

Correspondence should be addressed to Yifan Yang; yyf20010525@mail.nwpu.edu.cn

Received 9 May 2022; Revised 20 June 2022; Accepted 4 July 2022; Published 25 September 2022

Academic Editor: Zhiping Cai

GPS signal is fragile. With the development of GPS interference and anti-jamming technology, this paper tends to briefly describe the current classification of related interference technology and antijamming technology, analyze and summarize the current status of classical interference technology and antijamming technology, compare and analyze all kinds of current interference and antijamming technology, and prospect the future development of interference and antijamming technology.

1. Introduction

Global positioning system (GPS), which is a high-precision radio navigation system based on an artificial Earth satellite, provides real-time information such as three-dimensional position and three-dimensional velocity all over the world [1]. The GPS navigation system has been widely used in various disciplines, engineering practice, scientific research, and military fields, from engineering survey, and geodesy, to dynamics and other disciplines. As an important means of the modern positioning system, GPS has become an integral part of today's society, but at the same time, while enjoying the convenience brought by GPS, people have expressed higher requirements in security management, antifraud, and anti-interference. As an important means of the modern positioning system, GPS has the disadvantage of getting weak of its signal in the process of transmission. Simultaneously, due to signal disclosure and other reasons, it cannot completely suppress external interference [2]. Therefore, the accuracy and security of navigation have been unprecedentedly challenged when faced with the series of problems mentioned above. It is very easy to be deceived and interfered by people with ulterior motives, which causes losses to production and life. With the development of the society, what merits caution is that the GPS technology has presented many issues on security, confidentiality, and anti-interference. Meanwhile, the society also puts forward higher requirements for GPS security management, anti-fraud and anti-interference technology.

At present, GPS jamming technology is mainly divided into suppression jamming and spoofing jamming [3]. Suppression jamming refers to the generation of broadband or narrowband active noise signals in the tuning frequency band, the formation of a suppression jamming environment in space radiation [4], and the artificial transmission of noise to the receiver to increase the noise level at its input and reduce its signal-to-noise ratio, so as to interfere with the normal work, and thus the purpose of jamming is achieved [5]. Spoofing jamming is to make the target generate wrong positioning information by transmitting false signals with the same parameters as the original positioning signal and jamming the receiving end. In essence, it destroys the code synchronization circuit of the GPS receiver, making it to capture false signals. Compared with suppression jamming, spoofing jamming can realize the interference to the receiving end with less power, although it has higher technical requirements.

According to the technical characteristics of GPS, anti-interference technology is mainly divided into three aspects: interference source, receiver adjustment, and technical adjustment. As to interference sources, now there are two methods to achieve anti-interference. One of them is to cut

off the interference source to achieve the purpose of anti-interference [6], while the second method is to adjust the technology of emission control and improve the overall safety of the control system. As for the receiver, the purpose of anti-interference is usually achieved by improving the function of the receiver [7]. Currently, several technologies are applied, such as radio frequency interference technology [8], code ring and carrier tracking technology, narrowband interference technology, antenna enhancement technology, and antimultipath technology [9]. These technologies mainly utilized the characteristics of com-mon interference signals, such as amplitude, frequency [10], time, space, and polarization, to suppress and reduce interference [11].

Over the past two years, research studies on GPS related interference and anti-interference technologies have been continuously carried out by research institutions at home and abroad, including the University of Texas, Seoul National University, Northwest Pacific National Laboratory, West Virginia University, Korea Advanced Institute of science and technology, Gdansk University of Science and technology, and other relevant foreign universities and enterprises. Domestic participants are Tsinghua University, Shanghai Jiaotong University, National University of Defense Electronic Science and Technology, Nanjing University of Science and Technology, and other relevant universities and enterprises. Relevant papers at academic conferences all around the world are also gradually increasing. This paper aims to introduce and analyze the current GPS interference and anti-interference related technologies.

2. GPS Related Jamming Technology at Present

2.1. Suppression Jamming

2.1.1. Principle of Suppression Jamming. GPS signal adopts two kinds of pseudocode modulation, namely, coarse acquisition code (C/A code) and fine code (P (Y) code). C/A code is only modulated in L1 (1575.42 MHz) frequency band, while P (Y) code is modulated in L1 and L2 (1227.6 MHz) frequency bands at the same time [12]. Because the GPS signal is transmitted by the satellite 20,200 km away from the ground, the signal strength becomes very weak when it reaches the ground [7]. The power of C/A code in Ll band when it reaches the ground is 159.6 dBW, which enables the application of the suppression jamming.

Suppression jamming blocks the GPS signal frequency band by transmitting high-power noise signals with the same frequency through the GPS jammer, so as to reduce or completely deprive the working ability of the enemy's GPS receiver [7]. Suppression jamming contains many modes, including continuous wave jamming [13], noise band limited jamming, and correlation jamming. Different jamming modes lead to different jamming effects. According to the classification of signal spectrum width, suppressive interference can be divided into aiming interference and blocking interference [14]. The commonly used suppression jamming mainly includes the following types: aiming jamming [15], broadband noise jamming, broadband spectrum interference, and synchronous pseudocode spread spectrum interference.

2.1.2. Aiming Jamming. Based on suppression jamming, aiming jamming is a technology mainly used in direct sequence spread spectrum communication system [16]. It is to accurately aim the jamming signal, which is concentrated within the GPS spectrum, to the GPS downlink signal [17].

Specifically, as is demonstrated in Figure 1, for aiming jamming, the data code data is transmitted through C/A code spread spectrum and BPSK modulation, and therefore becomes a GPS signal [18, 19]. GPS signals and jamming signals are received by the receiver at the same time, and the data code DATA is obtained through demodulation and dispreading. DATA of the receiving end contains both noise signals and data [20], by which the GPS receiving system is disturbed.

Generally speaking, there are two key technologies to realize aiming jamming: firstly, the jamming signal bandwidth should be consistent with the GPS signal bandwidth of 2 MHz; secondly, the jamming signal carrier frequency should be consistent with the GPS signal carrier frequency of 1575.42 MHz.

2.1.3. Broadband Noise Interference. Broadband noise interference refers to the transfer of the Gaussian noise with limited bandwidth (the spread spectrum that is usually expected to be interfered has the same bandwidth [20], and the bandwidth of C/A code is 2 MHz) to the carrier frequency of the desired interference signal [21, 21], so as to increase the Gaussian noise input to the receiver, artificially increase the measurement error [22], and finally achieve the effect of interference by reducing the signal-to-noise power ratio of GPS receiver C/N0 below the threshold value.

Due to the increasing benefits of the spread spectrum, the GPS receiver can expand the interference power while "amplifying" the signal power [23], which is actually equivalent to reducing the interference power. The spread spectrum gain of the GPS system is very large [24, 25], and it works with strong interference power. Compared with aiming jamming, broadband noise interference requires more power to achieve the same jamming effect because the carrier frequency information of the signal is not used.

2.1.4. Broadband Spectrum Interference. Broad Band Spectrum Interference adopts the interference technology combining sawtooth wave wideband frequency modulation and noise narrowband frequency modulation to ensure that the blocking interference can produce a wideband uniform interference spectrum (comb and continuous), which presents an equal amplitude envelope in the time domain [26]. Therefore, broad band spectrum interference is the best technology to implement total blocking interference [27]. In this system, most of the interference signals can pass through the receiver narrowband filter without being filtered out, so it can produce an ideal interference effect.

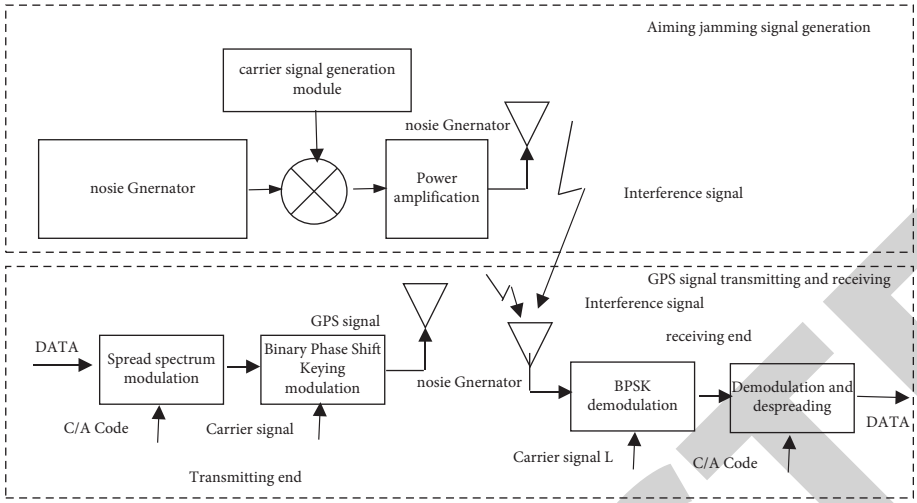


Figure 1: Aiming jamming and GPS transceiver system.

In practical application, the generation of the required broadband uniform spectrum signals needs to reasonably set the relevant signal bandwidth and power parameters. The adjustable parameters in the generation process of interference signal include: amplitude A of FM interference signal [28], FM mutual conductance K_{f1} of sawtooth FM signal, period T_s of sawtooth wave, slope A_s of sawtooth wave, FM mutual conductance K_{f2} of narrowband noise FM signal and mean square root of narrowband noise signal σ_N et al. [29, 30].

2.1.5. Synchronous Pseudocode Spread Spectrum Interference. This interference means that the interference signal and the GPS signals entering the receiver have the exact same code type [31], synchronize completely on the chip interval, and have the same carrier frequency. Set the interference signal as follows:

$$j(t\sqrt{2}) = m(t)p(t)\cos(\omega t). \quad (1)$$

Within, $m(£)$ modulates the baseband signal for interference. After the operation of dispreading, demodulating, and integrating, the processing gain of the dispreading system to the interference signal is invalid, so it is the best way to interfere. To synchronize pseudocode spread spectrum interference, it is necessary to know the carrier frequency and code type structure of GPS signal so as to synchronize the jamming pseudocode with its signal pseudocode as much as possible. As the synchronization difference increases, the interference effect decreases, and if it is out of sync, it degenerates to aiming interference.

2.2. Spoofing Jamming

2.2.1. The Principle of Spoofing Jamming. Spoofing jamming means that the signal structure of a deceptive signal is the same as that of a real GPS signal [32], but the navigation message is different. Because of the strong similarity between a deceptive signal and a real GPS signal, the receiver cannot judge the authenticity of the received signal. This jamming is

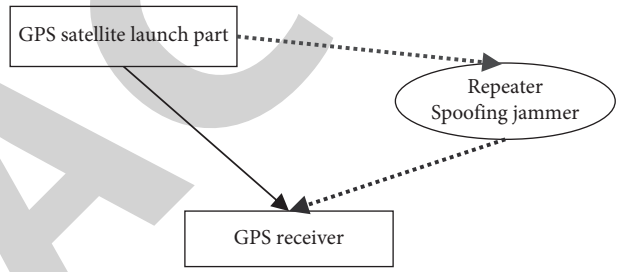


Figure 2: Basic principle of repeater spoofing jamming.

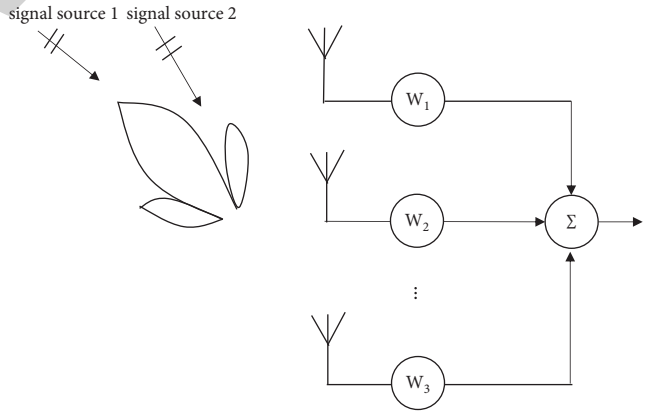


Figure 3: Space detection characteristics of beamforming technology.

of great confusion, which makes the receiver mistake it for receiving the correct information and produces wrong positioning [33, 34].

Spoofing jamming is mainly divided into Repeater Spoofing Jamming and Generating Spoofing Jamming [35]. The former one is to add a certain delay to the received GPS signal and retransmit it after power adjustment [36]. This method is simple to operate and does not need to know its code structure. The only thing needed is to calculate the delay, yet Repeater Spoofing Jamming is easily treated as a

Table 1: Jamming technology form.

Name	Category	Technical principle	Technical features
Aiming-jamming	Suppression jamming	The purpose of interference is achieved by aiming the jamming signal accurately at the GPS downlink signal and concentrating it within the GPS spectrum	Low carrier noise ratio and good interference performance
Broadband noise interference	Suppression jamming	The purpose of interference is achieved by reducing the signal-to-noise power ratio C/N0 of the GPS receiver below the threshold through artificially increasing the measurement error	Good interference performance at less wastage of the jammer
Broad band spectrum interference	Suppression jamming	The purpose of interference is achieved by combining the use of sawtooth wave broadband frequency modulation and the use of noise narrowband frequency modulation	Good interference effect with most of the interference signals passing through the narrowband filter of the receiver without being filtered
Synchronous pseudo code spread spectrum interference	Suppression jamming	The purpose of interference is achieved by using the jamming signal in the same code of the GPS signal at equal chip intervals and the same carrier frequency and then conducting despreading, demodulation, and integration operations to deactivate the despreading system's processing gain of the jamming signal	The requirement of highly matching the carrier frequency with code structure of the GPS signal
Asynchronous pseudo-code spread spectrum interference	Suppression jamming	The purpose of interference is achieved by keeping the interference carrier frequency the same as the signal carrier frequency and two pseudo code sequences with the same code element width	Small correlation between interference pseudo code and signal number
Repeater jamming	Spoofing jamming	The satellite signal is amplified and transmitted through the repeater jamming system, so that the pseudorange of the corresponding satellite measured by the target receiver deviates, and then the positioning result deviates from the real position	As the signal propagation delay increases, the observed pseudo range deviates, which makes it necessary to extract and amplify the signal from a very low signal-to-noise ratio to ensure no or less distortion of the signal and improve the output signal-to-noise ratio
Generating spoofing jamming	Spoofing jamming	The purpose of interference is achieved by generating the pseudorandom code with the greatest phase according to the code structure detected by the reconnaissance and then modulating the false navigation message identical with the format of the navigation message	Highly simulated the real satellite signal has the advantages of the signal power that is much lower than the noise, better concealment, and higher efficiency

multipath signal by the receiver, which leads to the failure of deception, and it inevitably has some limitations. Generative Spoofing Jamming generates a wireless signal with the same structure as the real GPS signal. It is highly flexible and can adjust various parameters in accordance with its own needs [37].

2.2.2. Repeater Spoofing Jamming. The Repeater Spoofing Jamming makes use of the natural delay of the signal, so it is relatively easy to realize the jamming on technology. For the receiver without special measures, it is easy to be deceived by this deception signal.

As is demonstrated in Figure 2, the repeater jammer receives the local GPS satellite carrier signal and then radiates it into the air through the antenna transmitted by the jammer after delay and power amplification, so that other GPS users in a certain area can receive the signal transmitted by the jammer. Repeater jamming needs to extract and amplify the signal from a very low signal-to-noise ratio to ensure that the signal is not or less distorted and improve the output signal-to-noise ratio. Since the jammer increases the propagation delay after forwarding [38], the pseudorange measured by the GPS receiver changes, resulting in its failure to work normally and navigation, so as to achieve the purpose of deception.

2.2.3. Generating Spoofing Jamming. The generating jamming is mainly realized by independently generating satellite navigation signals carrying false navigation information. According to whether the generated deception signal is synchronized with the real satellite signal, the generated deception jamming can be divided into asynchronous generation jamming and synchronous generation jamming.

At present, the asynchronous generation deception jamming technology is relatively mature and can be realized by satellite navigation RF signal simulator, but it also has some limitations [39]. The asynchronous generation jamming generally needs to track the relevant real satellite

Table 2: Anti-interference technology form.

Name	Technical principle	Technical features
Adaptive nulling technology	The reception of useful signals is ensured by forming the optimal beam, which adaptively responds to the spatially varying interference environment, and an adaptive null which effectively filters the interference	The spatial resolution of distinguishing signal and interference is limited. When the number of interference signals is larger than the array degree of freedom, the ability of the system to suppress interference signals decreases rapidly and the system cannot lock and suppress the interference when the interference is unstable
Adaptive nulling based on beamforming technology	The reception of effective signals and the formation of the null notch in the interference direction to suppress interference is ensured by adaptively adjusting the weighted vector of each array element in the antenna array according to the position, attitude, interference direction, and intensity of the carrier and the same time using the array synthesis direction map to point to the incoming signal direction	Effective suppression of interference is achieved by ensuring normal reception of the satellite signal and at the same time forming a depth of negative gain in interference
Time-frequency domain filtering technology	The different mapping characteristics of navigation signal and narrowband interference in the frequency domain are used to eliminate interference	It improves the degree of freedom of the antenna and effectively suppresses the interference signal without increasing the number of antennas by selecting the antenna array according to the optimal criterion. However, it has high requirements for the processor and demands a large amount of calculation

signals with the help of the suppression jammer, and the effective deception jamming can be carried out only after ensuring that the target receiver enters the search and acquisition state.

Synchronous deception jamming is to guide the target receiver when receiving the real satellite signal so that the attack object gradually deviates from the real signal and attacks the target receiver. Therefore, the same is more difficult to be found, and the synchronous deception jamming attack is more hidden [15].

3. Anti-Interference Technology

With the development of GPS jamming technology, anti-jamming technology also keeps pace with the times. At present, the main anti-jamming technical measures mainly include Adaptive Nulling Technique, Onboard Adaptive Nulling Based on Beamforming Technology, and Time-Frequency Domain Filtering Technology.

3.1. Adaptive Nulling Technology. The essence of Adaptive Nulling technology is optimal beamforming, which can adaptively respond to the spatially changing interference environment and forms adaptive zeros in the interference direction to effectively filter the interference so that useful signals can be received. Statistical optimal beamforming is an analytical tool, which provides a theoretical basis for the implementation of adaptive beamforming.

There are two types of satellite antennas to realize multibeam formation: phased array antenna and multibeam antenna. The former one is extremely flexible to achieve beam scanning or fast hopping by controlling the feed phase of the antenna unit and can obtain good spatial (zeroing) resolution characteristics. However, when the phased array antenna is used as a satellite antenna, its beam coverage performance is often difficult to meet the requirements. In contrast, multibeam antennas use the same antenna aperture to form multiple independent and overlapping narrow beams, although the zeroing resolution is not as good as that of phased array antennas, they can achieve the best airspace coverage of the beam and easily form a zero point with broadband characteristic s in the direction of the interference source [40].

The Adaptive Nulling Technology also has disadvantages of not considering the direction of the satellite signal. It does not consider the direction of the satellite signal. When the interference is close to the direction of the satellite signal, the interference is eliminated and at the same time, the signal is weakened. Moreover, the Adaptive Nulling Technology can not point to the signal [41]. For the signal, the signal-to-noise ratio is the same as that received by a single antenna, so it cannot make full use of the advantages of the antenna array.

3.2. Adaptive Nulling Based on Beamforming Technology. Adaptive Nulling Based on Beamforming Technology is a new antenna beamforming technology since the 1980s. As is demonstrated in Figure 3, it is widely used in radar, communication, and other fields because of its high data rate, multibeam formation at the same time, and adaptive zero control. Adaptive Nulling Based on Beamforming Technology uses multiple receiving antennas to receive signals respectively, and then send them to the back-end processing [42]. By adjusting the weighting coefficient of each channel, the signals in a specific direction can pass through and the signals in other directions will be filtered out, so as to achieve the purpose of spatial filtering.

Adaptive Nulling Based on Beamforming technology can align the antenna beam with the satellite to be tracked, improving the satellite signal gain, and form zero in the direction of interference, so the application of Adaptive

Nulling Based on Beamforming Technology in GPS anti-interference can obtain better antiinterference ability [43].

3.3. Time-Frequency Domain Filtering Technology. Time-Frequency Domain Filtering technology includes time-domain filtering and frequency-domain filtering. Time domain filtering mainly uses the digital signal processing (DSP) method to eliminate or suppress narrowband, continuous wave, and other interference in the time domain [44]. Generally, it is realized by an adaptive FIR/IIR filter. This technology is only effective for narrowband interference or continuous wave interference and can not effectively suppress wideband interference [45]. The typical product is the ATF filter chip of the Mayflower communication company, and its improvement of narrowband anti-interference is about 30 dB.

Frequency domain filtering uses the different mapping characteristics of navigation signal and narrowband interference in the frequency domain to eliminate interference [46]. The mapping characteristics of navigation signal in the transform domain are relatively flat and the intensity is relatively small (lower than noise), while the mapping characteristics of narrowband interference are relatively prominent and the intensity is relatively large [47]. Therefore, it is easy to distinguish between noise signal and narrowband interference in the transform domain, so as to suppress-interference through corresponding transform domain processing algorithms. The typical product is the frequency domain removal chip developed by mitre company, and its anti-interference improvement is about 35 dB.

4. Research Directions and Challenges

At present, some GPS interference methods and anti-interference methods have solved some related difficulties but still have their own advantages and disadvantages. The comparison of various interference technologies and anti-interference technologies is shown in Tables 1 and 2.

5. Concluding Remarks

Based on the current situation of the GPS system, this paper discusses and summarizes the relevant technologies and measures of interference and anti-interference of the GPS system, which provides a certain reference for GPS related interference and anti-interference measures.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

[1] H. Hu and Na Wei, "A study of GPS jamming and anti-jamming," in *Proceedings of the 2009 2nd International Conference on Power Electronics and Intelligent Transportation System*, pp. 388–391, PEITS), Shenzhen, December 2009.

[2] E. Union, *European GNSS Open Service Signal In Space Interface Control Document*, Europian Union, Brussels, Belgium, 2010.

[3] S. S. Ozdemir and E. Aksoy, "GPS jamming mitigation through Taguchi's optimization method," in *Proceedings of the 2017 25th Telecommunication Forum (TELFOR)*, pp. 1–4, Belgrade, Serbia, November 2017.

[4] B. Iyidir and Y. Ozkazanc, "Jamming of GPS receivers," in *Proceedings of the IEEE 12th Signal Processing and Communications Applications Conference, 2004*, pp. 747–750, Kusadasi, Turkey, April 2004.

[5] M. K. Bek, E. M. Shaheen, and S. A. Elgamel, "Mathematical analyses of matched spectrum interference signal on post-correlation C/N0 for the GPS receivers," in *Proceedings of the 2014 9th International Conference on Computer Engineering & Systems*, pp. 119–124, ICCES), Cairo, Egypt, December 2014.

[6] M. Ahmad, M. A. Farid, S. Ahmed, K. Saeed, M. Asharf, and U. Akhtar, "Impact and detection of GPS spoofing and countermeasures against spoofing," in *Proceedings of the 2019 2nd International Conference on Computing, Mathematics and Engineering Technologies*, pp. 1–8, iCoMET), Sukkur, Pakistan, January 2019.

[7] P. Bethi, S. Pathipati, and P. Aparna, "Stealthy GPS spoofing: spoofer systems, spoofing techniques and strategies," in *Proceedings of the 2020 IEEE 17th India Council International Conference (INDICON)*, pp. 1–7, New Delhi, India, December 2020.

[8] X. Xie, M. Lu, and D. Zeng, "Research on GNSS generating spoofing jamming technology," in *Proceedings of the IET International Radar Conference 2015*, pp. 1–5, Hangzhou, October 2015.

[9] R. Musselman, S. Killpack, B. Killion, E. Herbort, P. Kim, and R. Todd, "Adaptive null-steered interference-rejection for a mobile satellite receiver," in *Proceedings of the 2010 IEEE International Symposium on Phased Array Systems and Technology*, pp. 969–973, Waltham, MA, USA, October 2010.

[10] A. Pal, A. Mehta, A. Skippins, P. Spicer, and D. Mirshekar-Syahkal, "Novel interference suppression null steering antenna system for high precision positioning," *IEEE Access*, vol. 8, Article ID 77779, 2020.

[11] Q. Yan, B. Lin, and K. Wang, "Research on adaptive digital beam forming technology," in *Proceedings of the 2018 IEEE 3rd International Conference on Cloud Computing and Big Data Analysis*, pp. 446–450, ICCCBDA), Chengdu, China, April 2018.

[12] S. Jeong, T. Kim, and J. Kim, "Spoofing detection test of GPS signal interference mitigation equipment," in *Proceedings of the 2014 International Conference on Information and Communication Technology Convergence*, pp. 651-652, ICTC), Busan, Republic of Korea, October 2014.

[13] W. Pan, Z. Yang, and J. Zheng, "GPS pseudocode targeting-based jamming and hardware implementation," *Modern Defense Technology*, vol. 4, 2017.

[14] Y. Sun, C. Cao, J. Lai, and T. Yu, "An anti-GPS spoofing approach for UAVs based on LSTM-KF model," *Journal of Network and Information Security*, vol. 6, no. 5, pp. 80–88, 2020.

[15] P. Jiang, S. Bian, and N. Zhan, "Research on GPS suppression jamming technology based on navigation warfare," *Ship Electronics Engineering*, vol. 8, 2010.

[16] Y. Liu and Y. Kou, "Research and design of synchronous GPS spoofing interference signal generation technology," *Journal of Beijing University of Aeronautics and Astronautics*, vol. 46, no. 4, pp. 814–821, 2020.

Hindawi
Security and Communication Networks
Volume 2024, Article ID 9807516, 1 page
https://doi.org/10.1155/2024/9807516

Retraction

Retracted: A Table Tennis Motion Correction System Based on Human Motion Feature Recognition

Security and Communication Networks

Received 8 January 2024; Accepted 8 January 2024; Published 9 January 2024

This article has been retracted by Hindawi following an investigation undertaken by the publisher [1]. This investigation has uncovered evidence of one or more of the following indicators of systematic manipulation of the publication process:

(1) Discrepancies in scope

(2) Discrepancies in the description of the research reported

(3) Discrepancies between the availability of data and the research described

(4) Inappropriate citations

(5) Incoherent, meaningless and/or irrelevant content included in the article

(6) Manipulated or compromised peer review

The presence of these indicators undermines our confidence in the integrity of the article's content and we cannot, therefore, vouch for its reliability. Please note that this notice is intended solely to alert readers that the content of this article is unreliable. We have not investigated whether authors were aware of or involved in the systematic manipulation of the publication process.

Wiley and Hindawi regrets that the usual quality checks did not identify these issues before publication and have since put additional measures in place to safeguard research integrity.

We wish to credit our own Research Integrity and Research Publishing teams and anonymous and named external researchers and research integrity experts for contributing to this investigation.

The corresponding author, as the representative of all authors, has been given the opportunity to register their agreement or disagreement to this retraction. We have kept a record of any response received.

References

[1] L. Han, "A Table Tennis Motion Correction System Based on Human Motion Feature Recognition," *Security and Communication Networks*, vol. 2022, Article ID 7049429, 8 pages, 2022.

Hindawi
Security and Communication Networks
Volume 2022, Article ID 7049429, 8 pages
https://doi.org/10.1155/2022/7049429

Research Article

A Table Tennis Motion Correction System Based on Human Motion Feature Recognition

Liangzi Han

Sports Department, Shenyang Aerospace University, Shenyang, Liaoning 110000, China

Correspondence should be addressed to Liangzi Han; hanlz@sau.edu.cn

Received 18 July 2022; Revised 10 August 2022; Accepted 23 August 2022; Published 13 September 2022

Academic Editor: Fang Liu

Computer-aided sports systems are an important area of current research. To be specific, it can combine computer vision, computer graphics, and motion capture technologies with the characteristics of sports, and design and develop assisted systems according to user needs. As a result, it is of great practical importance and application to improve the entertainment and science of sports learning, to stimulate public participation in sports, and to learn sports skills. Table tennis has a very great popular base in China and has a wide range of audiences. However, for beginners or amateurs of table tennis, it is difficult to learn table tennis skills by relying on books, videos, etc., due to the lack of professional technical guidance, which makes it relatively difficult for them to continuously improve their skills. Sometimes they tend to form wrong technical habits, which are not easy to detect and correct in time, and can lead to sports injuries over time. Therefore, the lack of professional instruction has hindered the development of table tennis in public fitness to a certain extent. On the other hand, in a table tennis course, the learning of table tennis techniques is mostly dependent on the teacher's explanation. Students are bored with the repetitive and boring teaching because they need to repeat the exercises several times. The formation of correct table tennis movements requires repeated instruction from the instructor to address problems with the student's movements. However, due to limited teaching resources, it is difficult for teachers to accommodate different students during the teaching process. In addition, with a limited team of instructors, the level of proficiency varies, making it difficult for them to make an objective assessment. As a result, with the rapid development and application of modern science and technology in the field of sports, there is an urgent need to explore intelligent sports technology instructional support systems to improve the shortcomings of the traditional teaching model. Motion recognition technology, as an essential branch of multimodal interaction technology, has been developing rapidly in recent years. This research focus on designing and implementing a system for recognizing human motion based on skeletal point pose information by combining inertial sensors. This system can collect data from sensors located at the main skeletal points of the human body and transmits them to the host computer through multi-Bluetooth pairing transmission. After that, support vector machines are applied to classify human movements and to recognize general human movements. This system has significant advantages for human movement recognition and classification due to the distinctive technical characteristics of table tennis. The recognition and classification of both players in the video can play an important role in the technical analysis and tactical arrangement of the players. As a result, the table tennis motion correction system based on human motion feature recognition has crucial research significance and application value.

1. Introduction

In recent years, with the continuous development of computer technologies such as mathematical modeling [1, 2], deep learning [3, 4], and machine learning [5, 6], society as a whole has entered a new phase of rapid development. The impact of these technologies has spread to all walks of life. The social changes brought by these technologies are everywhere, and the intelligent society has come. At the same time, people's living standards are also improving. In many advanced devices for people, it is essential to collect data about people, and human movement data are particularly important [7]. Numerous research institutions and laboratories are studying how to capture human motion data,

and analyze and restore it. These sets of motion capture systems have begun to move from laboratory research to the consumer market, and are beginning to open up in conjunction with virtual reality technology [8]. The main motion capture technologies on the market today are optical image-based technologies based on image processing and light point positioning. In addition, motion capture technologies such as inertial navigation, electromagnetic sensing, and mechanical feedback are also at the forefront of scientific research [9]. The optical capture system uses image processing to obtain the human motion model and corrects the fit by comparison to obtain the human kinematic parameters [10]. The inertial navigation capture system uses inertial sensor units bound to the skeleton. By obtaining the acceleration and angular velocity of the sensor nodes, the posture of the human skeleton can be restored, and the corresponding displacement information can be calculated [11]. Inertial sensors are widely adopted in the development of motion posture machines and scientific experiments because of their ability to collect data in a timely manner, their relatively low cost, their independence from light field environments, as well as their ease of installation.

Mechanical motion capture solutions have been around for a long time and are actually humanoid structures that can perform specific movements in place of the user [12]. By design, a mechanical capture solution consists of multiple linkage structures and joints that rely on mechanical stresses between the linkages. When the user wears the device, the active movement of the body causes the mechanical structure to change its angle and strain [13]. The motion is then captured and analyzed based on the angle change measured by the angle sensor and the length of the linkage. Figure 1 shows a classic mechanical motion capture system. Electromagnetic motion capture solutions generally consist of a transmitter source, a receiver point, and a data processing unit. The transmission method is an electromagnetic wave, and the process is to build a uniform low-frequency magnetic field environment in the test environment [14]. The test subject wears an electromagnetic receiver. When the test subject moves, the magnetic field changes and the motion data can be captured, and the position and direction of the receiver can be obtained after decoding. The optical motion capture solution works by capturing the spatial position of the light-emitting point to determine the motion trajectory of the subject [15]. Depending on the capture method, there are two options. Passive solutions are those in which reflective devices are placed on the subject's joints and the motion capture camera marks the subject with a reflected light source [16]. The active solution is that the subject wears a light-emitting device and the camera captures the location of the light point directly.

Human motion recognition has been researched in the past mainly based on visual aspects. With the development of sensors, sensor-based human motion recognition has only been noticed [17]. The existing human motion recognition methods are mainly these two. The vision-based human motion recognition method is to install the filming equipment in a fixed space and determine the human motion state

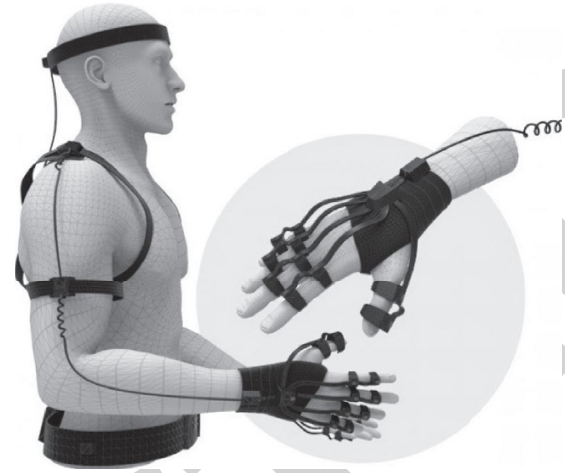


Figure 1: A classic mechanical motion capture system.

by analyzing the human motion state in the filmed pictures and the comparison of the before and after pictures [18]. Its technology started earlier and its theoretical research is more mature. From the existing research, the complexity of the algorithm and the accuracy of the recognition rate of the system are able to meet the daily needs. However, one of the major shortcomings of the system is that it has strict requirements for the environment in which the images are acquired [19]. The acquisition of human motion images requires a spacious environment, sufficient light, and no obstruction of the subject. The sensor-based human motion recognition system is a new direction in pattern recognition. Its basic principle is to collect the motion data information from one or more miniature sensors carried by the user [20]. After that, the motion of the human body is recognized and judged accordingly according to the data. Table 1 compares the characteristics of two different human motion recognition systems, vision based and sensor based.

From the comparison results in the table, it is clear that the sensor-based human motion recognition system has unique advantages. First of all, it allows free access to data information about different human movements. The sensor-based human motion recognition system is minimally dependent on the environment and is not affected by the equipment used to capture the images [21]. As a result, it can be acquired at any time and at any place. When capturing human motion data, the human body can move freely, thus making the data collected more realistic. In addition, there is no need for other peripherals to interfere with the acquisition of the user's data. As long as the user is moving, the data can be obtained without violating the user's privacy [22]. What is more, the sensor-based human motion recognition system is small, light, and inexpensive. Thus, it can be placed on any part of a person's body, and the corresponding motion data information can be collected anywhere.

In recent years, as wireless body area networks are used more and more in various fields, researchers can design specific identifiers according to their system requirements

Table 1: Characteristics of two different human motion recognition systems.

Feature	Vision-based system	Sensor-based system
Collected data	Image	Discrete data from sensors
Portability	Low	High
Affected by the environment	High	Low
Affected by space	Fixed regions	Any regions
Signal processing complexity	High	Low

using different methods to collect different kinds of human motion data information. In the existing research, the sensor modules used to collect human motion data mainly include acceleration sensors [23], gyroscope sensors [24], magnetometer sensors [25], and so on. In previous studies, researchers have used individual acceleration sensors to collect the corresponding acceleration signals and then used different recognition methods to identify human motion. These methods are generally only related to a specific human motion and have a single signal and function [26]. As a result, the application value and the accuracy of the recognition are limited. In order to avoid these issues, this study proposes a human motion recognition system based on humans' skeletal points. To be specific, it is mainly based on low-cost pose sensors, and the motion data collected are parsed and classified by machine learning classification algorithms. In terms of hardware, it can overcome the spatial limitations of optical motion detection methods and wired acquisition methods [27]. In terms of motion recognition, the classification algorithm can be used to classify and train the motion in a statistical way, thus effectively improving the accuracy of table tennis motion recognition [28]. In summary, the skeleton point-based human motion recognition system designed in this research can be applied in the field as shown in Figure 2.

This system is designed and developed to meet the demand of table tennis enthusiasts to learn table tennis skills on their own, as there is a lack of professional table tennis instruction for beginners or amateurs in the public fitness field. By matching the user's table tennis technical movement data features with the extracted technical movement features of the best athletes, the similarity of the movements and the detailed evaluation results are fed back to the user, which can help guide the beginners or amateurs to correct their technical movements [29]. It is of practical significance and application value to meet the basic needs of table tennis enthusiasts in mass fitness to learn sports skills. On the other hand, by combining computer vision and motion capture technologies, the system can analyze and guide the user's technical movements in a real-time, efficient, and objective manner [30]. To be specific, it can balance the deviations of the gesture guidance evaluation caused by human subjective judgment, which is important for the realization of a digital and scientific auxiliary evaluation system. This research method can be further developed for the characteristics of other sports, which is conducive to the cross-fertilization of sports and computer theory technology and other interdisciplinary disciplines to promote the development of sports.

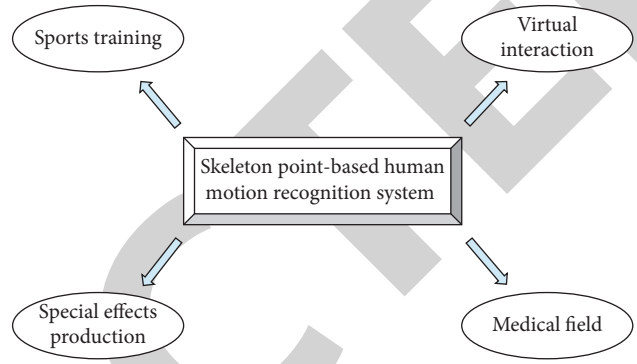


Figure 2: Application field of skeleton point-based human motion recognition.

2. Research on Human Motion Feature Recognition

2.1. Framework of Motion Recognition. The existing multisensor-based human motion recognition system mainly consists of a portable sensor terminal, a wireless sensor network, and a remote monitoring center, and the basic framework is shown in Figure 3. To be specific, the unknown human motion data are first collected by the sensor terminal and then transmitted to the monitoring device through the wireless sensor network.

2.2. Data Acquisition Module. The sensor module is mainly responsible for collecting effective data information of human body movement. In recent years, with the rapid development of sensor technology, data signal processing technology, and hardware circuit technology, many parameters of the human body can be represented by collecting some sensor data. For example, the temperature of the human body can be represented by temperature sensor data information, and the pulse rate of the human body can be represented by pulse sensors. The motion of the human body can be represented by the acceleration sensor, gyroscope sensor data information, etc.

The main sensors used to collect human motion data are pressure sensors, acceleration sensors, and gyroscopic sensors. Different researchers have placed sensor nodes in different locations to collect data on different human movements. There is no unified database and no specific hardware technology standard in the existing recognition systems. Therefore, researchers generally have to design and select sensor modules that meet their system performance according to their research requirements and experimental goals.

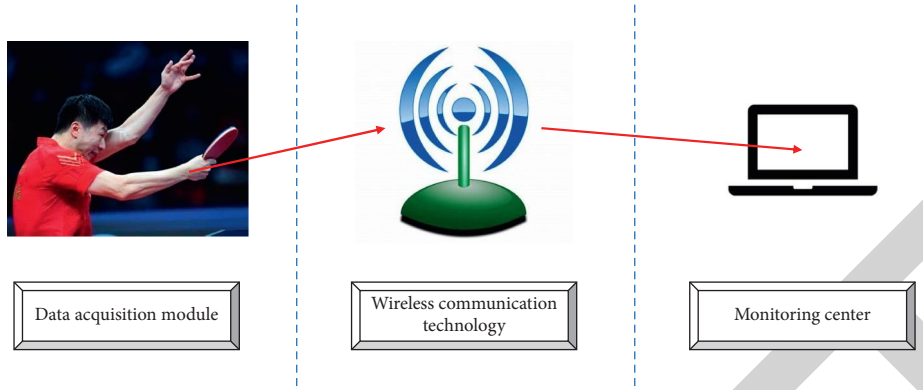


Figure 3: Framework of motion recognition.

2.3. Wireless Communication Technology. Wireless communication technology mainly refers to short-range and low-power communication around the human body. In recent years, with the rapid development of wearable devices and mobile IoT products, short-range wireless communication technology is also developing rapidly. Among the many short-range communication technologies, Bluetooth is one of the most widely used and popular technologies. Bluetooth communication with low-power consumption has the characteristics of low price, fast connection, and strong anti-interference. Therefore, it is widely used in the field of medical and health care for individual users. Radio frequency recognition technology, also called electronic label or wireless video radio frequency recognition, is a kind of widely used short-distance wireless communication technology. The video recognition uses the wireless signal to recognize the specific target and read–write the related data without establishing mechanical or optical contact. Therefore, this technology has a low cost, the use convenient characteristic. However, its main disadvantage is the slow transmission speed. As a result, it is widely applied in access control and automatic charging occasions.

2.4. Human Motion Recognition Mode. The essence of sensor-based human motion pattern recognition is to first collect a large amount of sensor data information. Then, the recognizer is trained to meet the system recognition system based on the collected data, and finally the trained recognizer is used to recognize some unknown human motion data information. The main steps include data acquisition, data preprocessing, feature extraction and selection, recognizer selection, etc. This process is illustrated in Figure 4.

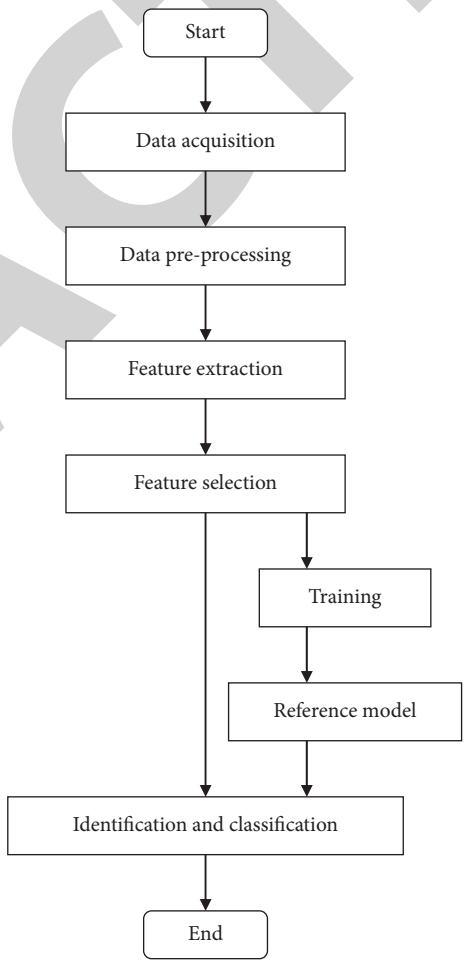


Figure 4: Process of human motion mode.

The accelerometer and gyroscope sensors are used to capture the signals generated by human motion. Due to human jitter, environmental factors, and device measurement biases, the measured data include not only human motion information but also unavoidable noise. In order to reduce the impact of noise on the system, effective preprocessing is required before data feature extraction. The existing preprocessing methods include filtering and normalization for noise removal and windowing for signal length reduction. In sensor-based human motion recognition systems, data denoising and data smoothing are generally used. The jitter of the human body and the jitter of the equipment when collecting sensor data information will bring the noise to the system. In addition, the measurement noise of the system is included in the collected sensor data information. As a result, the effectiveness and reliability of the system will be improved by removing the interference noise.

Normalization is also a technique frequently used in preprocessing. The main function of the normalization method is to adjust the motion data of different intensities

according to the specificity of the signal. In human motion recognition systems, the differences in height, weight, age, etc. can lead to differences in the magnitude of the motion data for different people doing the same motion. Therefore, some researchers have used normalization to reduce the impact of signal amplitude differences on the system.

Since the input data for human motion recognition are usually collected from the user's motion data signals over a period of time, the length of the input data is usually very long, which is not suitable for direct feature extraction and classification. As a result, windowing is usually applied to the collected sensor data before feature extraction. The function of windowing is to split the long sensor data signal into many windows with the same or different lengths. In the existing research, there are two main windowing methods commonly used in human motion recognition systems. The first one is sliding window segmentation as shown in Figure 5. Sliding window segmentation means that the motion signal collected by the sensor is divided into windows of the same length, and the adjacent windows may or may not have overlapping places. Adding windows to the sensor data not only shortens the length of the acquired data but also fixes the length of the sensor data signals between different people. This is essential for later data feature extraction, selection, and pattern recognition. When adopting fixed window lengths, no additional processing of the data is required, and it is often used in systems with high real-time requirements. However, this window segmentation technique also has some shortcomings. To be specific, when two motion signals are present in a window, it is difficult to recognize the transitions between the different motions.

In addition, as shown in Figure 6, the motion window-based segmentation technique refers to the processing and preliminary judgment of the data to determine the start and end times of the motion, and to segment the sensor data into windows of different lengths according to the time of the motion. Each of these windows represents a complete motion. Although this windowing technique can accurately identify each motion, the data needs to be processed and analyzed upfront. As a result, this method has a significant impact on the complexity of the algorithm and the energy consumption of the system.

Some of the existing human motion recognition algorithms require the use of sensor data from the three directional components of the sensor. Therefore, some researchers have taken advantage of the fact that the direction of acceleration of the human body at rest is always vertical to correct the tilt problem of the sensor. The principle of tilt correction is to calculate the tilt angle of sensor placement by using the feature that the direction of gravitational acceleration is always downward.

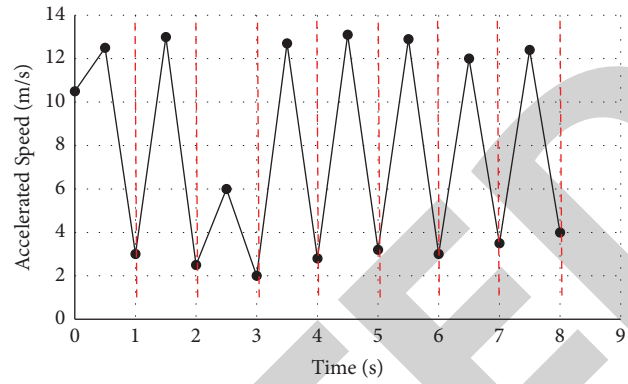


Figure 5: Example of sliding window segmentation.

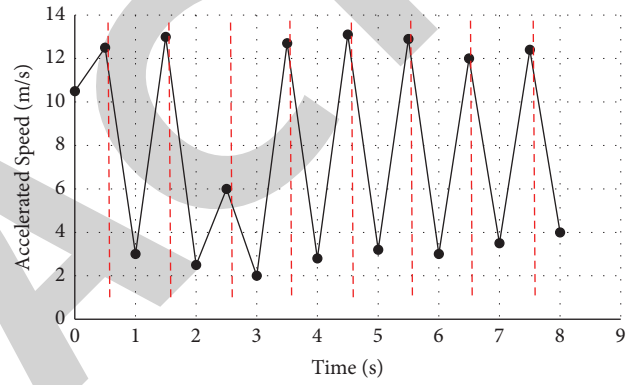


Figure 6: Example of motion window-based segmentation.

3. Design of Table Tennis Motion Correction System

3.1. User Requirements Analysis. The learning of technical movements is one of the key aspects of table tennis practice that is difficult for practitioners to master. The rationality of the technical movements has a great impact on the quality of the stroke, the continuity of the movement, and the learning of the combination technique. Currently, most table tennis courses rely on the traditional teaching model of demonstration and explanation by teachers or coaches. It is difficult for students to identify problems with their own technical movements during practice and to perceive and evaluate incorrect technical movements. As a result, it often took a long learning period to fix the technical movements. Second, due to the limited teaching resources, teachers or coaches have different skill levels. In addition, there are differences in the subjective judgments of teachers and coaches regarding the technical movements of table tennis, which have an impact on the formation of standard technical movements of beginners. As a result, there is a need for a table tennis movement correction that can replace or assist the teacher in making a scientific, objective evaluation and analysis that can be recorded. The table tennis movement correction system is aimed at the average table tennis hobbyist. The system will help them to understand the problems of their own technical movements through independent learning, thus providing a scientific basis for improving their skills. On the other hand, the system should meet the functional requirements of table tennis courses. By recording the results of the analysis of the testers' technical movements, it can assist teachers or coaches in the comprehensive evaluation of teaching effectiveness and student learning.

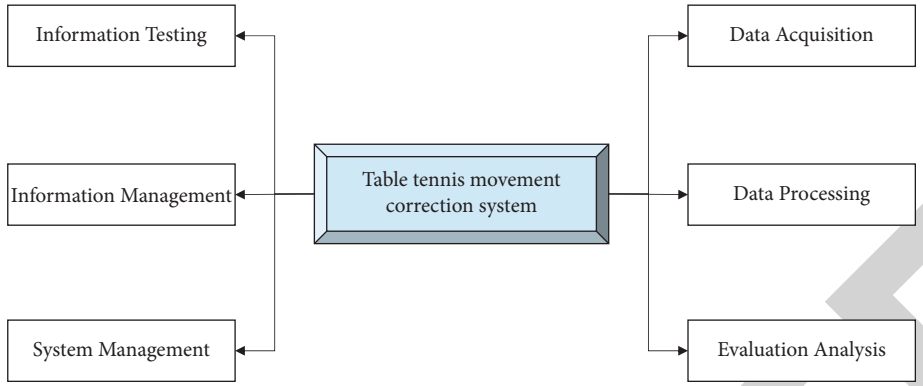


Figure 7: Functional requirements of the table tennis motion correction system.

3.2. Functional Requirements Analysis. The table tennis movement correction system designed and developed in this study should mainly implement the functions of testing and evaluating the user's table tennis technical movements and providing models of each technical movement of excellent players. In addition, the system should ensure the scientific accuracy and reliability of the test and evaluation results. Therefore, the design should include data collection and data processing modules. Due to the different fields of use, the test evaluation system should have a user test information storage and management function. Therefore, the functional requirements of the table tennis motion correction system are shown in Figure 7.

The application of motion capture technology in sports is particularly concerned with whether the system equipment will affect the data collection of the athlete's complete movements. Due to the physical constraints of wearing the device, the athlete may be limited in the use of the device and the accuracy of the test results. This system is designed for the masses of table tennis enthusiasts and therefore requires simple and easy-to-use equipment. Therefore, the system uses Kinect 2.0 motion capture technology, which allows for the acquisition of technical movement data without wearing sensors. In addition, in order to improve the data accuracy, the data processing module designed in this study can effectively reduce the system internal error of the device and thus improve the data accuracy. Therefore, this system can ensure the user experience and provide professional and accurate guidance on technical movements.

The core function of this system is to evaluate and analyze the technical movements of table tennis. This system establishes a database of movement characteristics by collecting the technical movement information of several outstanding athletes and provides evaluation and analysis criteria to assist in the evaluation of table tennis technical movements. The collection and filtering of data from several outstanding athletes ensure the reliability of this system. As a result, this system allows the user's sports information data to be compared with the database of movement characteristics of the best athletes, and the evaluation and analysis functions can be realized through the scoring algorithm, thus improving the learning efficiency of the user's table tennis technical movements. This system then enables users to identify and correct problems in their own technical movements and improve their skills.

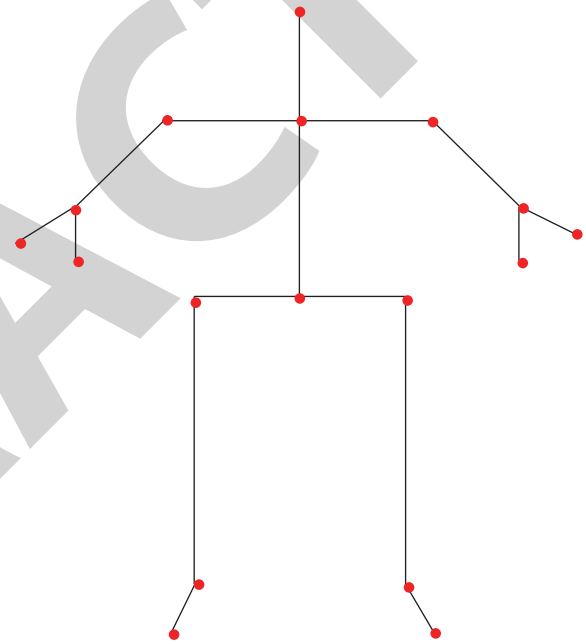


Figure 8: Schematic diagram of human stick model.

3.3. Human Motion Modeling Analysis. The structure of the human body is complex. In scientific research, complex problems need to be modeled in a rational way to achieve the research objectives. In the case of human motion posture acquisition, it is impossible to build a completely accurate model. As a result, it is extremely important to construct a reasonable and simple model. In medical research, virtual modeling, etc., the human body is often simplified into a stick model, as shown in Figure 8, considering the actual way of human motion. According to the knowledge of human decompression, a typical adult has 198 different bones. The bones are generally connected to each other by joints and ligaments, which are extremely complex. This study is to

classify the overall motion of the human body and does not focus on the small and dense joints such as the palms of the hands and feet. Therefore, it is not necessary to collect data from every skeletal point in this study. In addition, considering the actual size of the sensors, the limitations of the gesture sensing technology, and the cost control, only a few key human nodes need to be collected in this study.

The goal of this system is to design a simple, environment-independent hardware solution for motion pose acquisition. Therefore, the recognition of human motion can be achieved by collecting a large number of human motion data to form a human motion dataset, which can be trained by classification algorithms. Factors such as the location of the posture sensors and the number of sensors have an impact on the overall system. Therefore, if some data factors are controlled at the data collection stage, it can have a beneficial impact on the human motion analysis based on skeletal points.

4. Conclusion

Human motion recognition is a hot research topic in the field of computer vision, and technical motion detection in human sports videos is an important application in the field of computer vision in sports. In many sports, the technical movements of table tennis players are more obvious and the motion background is more fixed. Therefore, it is more advantageous to classify and recognize the technical movements of table tennis players intelligently. The recognition and classification of both players' movements in sports videos are important for the technical analysis and tactical arrangement of players. The skeleton point-based human motion recognition system can capture human motion information and also classify the data from the inertial measurement unit directly through algorithms to obtain the human motion status. This system is useful for the research and development of human-computer interaction. In addition, the system can be used to enhance human–computer interaction through posture recognition, combined with the Internet of Things technology, and open up a wide market. In this research, a skeleton point-based human motion recognition system is designed by combining inertial sensor technology and human motion posture. To be specific, the table tennis motion correction system can collect the posture information of human skeleton points to form a dataset in order to analyze and recognize the human motion posture with high accuracy.

The table tennis motion correction system designed in this study can provide feedback to the user in the form of graphs and other evaluation and analysis results, as well as personal information management and test information management, but it still does not provide an intuitive description of the user's motion. As a result, this system should also include 3D reconstruction technology. To be specific, the 3D reconstruction technology can restore the user's technical action and the standard technical action in 3D animation and reproduce the technical action process, so that the users can understand and find out the problems of their own technical actions.

Data Availability

The labeled dataset used to support the findings of this study can be obtained from the author upon request.

Conflicts of Interest

The author declares that there are no conflicts of interest.

References

[1] Y. Peng, Y. Lin, C. Fan et al., "Passenger overall comfort in high-speed railway environments based on EEG: assessment and degradation mechanism," *Building and Environment*, vol. 210, no. 2022, Article ID 108711, 2022.

[2] B. Cheng, J. Huang, J. Li, S. Chen, and H. Chen, "Improving contractors' participation of resource utilization in construction and demolition waste through government incentives and punishments," *Environmental Management*, vol. 70, no. 4, pp. 666–680, 2022.

[3] C. Fan, Y. Peng, S. Peng, H. Zhang, Y. Wu, and S. Kwong, "Detection of train driver fatigue and distraction based on forehead EEG: a time-series ensemble learning method," *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 8, pp. 13559–13569, 2022.

[4] P. Wang, W. Li, P. Ogunbona, J. Wan, and S. Escalera, "RGB-D-based human motion recognition with deep learning: a survey," *Computer Vision and Image Understanding*, vol. 171, pp. 118–139, 2018.

[5] B. Cheng, C. Fan, H. Fu, J. Huang, H. Chen, and X. Luo, "Measuring and computing cognitive statuses of construction workers based on electroencephalogram: a critical review," *IEEE Transactions on Computational Social Systems*, pp. 1–16, 2022.

[6] Y. Qian, S. Chen, J. Li et al., "A Decision-Making Model Using Machine Learning for Improving Dispatching Efficiency in Chengdu Shuangliu Airport," *Complexity*, vol. 2020, 2020.

[7] D. J. Peart, C. Balsalobre-Fernández, and M. P. Shaw, "Use of mobile applications to collect data in sport, health, and exercise science: a narrative review," *The Journal of Strength & Conditioning Research*, vol. 33, no. 4, pp. 1167–1177, 2019.

[8] A. Drapeaux and K. Carlson, "A comparison of inertial motion capture systems: DorsaVi and Xsens," *International Journal of Kinesiology & Sports Science*, vol. 8, no. 3, pp. 24–27, 2020.

[9] H. Fu, J. Niu, Z. Wu et al., "Influencing factors of stereotypes on wastewater treatment plants- case study of 9 wastewater treatment plants in xi'an, China," *Environmental Management*, vol. 70, no. 3, pp. 526–535, 2022.

[10] E. Protopapadakis, A. Voulodimos, A. Doulamis, S. Camarinopoulos, N. Doulamis, and G. Miaoulis, "Dance pose identification from motion capture data: a comparison of classifiers," *Technologies*, vol. 6, no. 1, p. 31, 2018.

[11] N. A. Mohd Jelani, A. N. Zulkifli, S. Ismail, and M. F. Yusoff, "A Review of virtual reality and motion capture in martial arts training," *International Journal on Interactive Design and Manufacturing*, vol. 5, no. 1, pp. 22–25, 2019.

[12] M. Menolotto, D. S. Komaris, S. Tedesco, B. O'Flynn, and M. Walsh, "Motion capture technology in industrial applications: a systematic review," *Sensors*, vol. 20, no. 19, p. 5687, 2020.

[13] M. Topley and J. G. Richards, "A comparison of currently available optoelectronic motion capture systems," *Journal of Biomechanics*, vol. 106, Article ID 109820, 2020.

Hindawi
Security and Communication Networks
Volume 2024, Article ID 9827176, 1 page
https://doi.org/10.1155/2024/9827176

Retraction

Retracted: Software Security Testing through Coverage in Deep Neural Networks

Security and Communication Networks

Received 8 January 2024; Accepted 8 January 2024; Published 9 January 2024

This article has been retracted by Hindawi following an investigation undertaken by the publisher [1]. This investigation has uncovered evidence of one or more of the following indicators of systematic manipulation of the publication process:

(1) Discrepancies in scope

(2) Discrepancies in the description of the research reported

(3) Discrepancies between the availability of data and the research described

(4) Inappropriate citations

(5) Incoherent, meaningless and/or irrelevant content included in the article

(6) Manipulated or compromised peer review

The presence of these indicators undermines our confidence in the integrity of the article's content and we cannot, therefore, vouch for its reliability. Please note that this notice is intended solely to alert readers that the content of this article is unreliable. We have not investigated whether authors were aware of or involved in the systematic manipulation of the publication process.

Wiley and Hindawi regrets that the usual quality checks did not identify these issues before publication and have since put additional measures in place to safeguard research integrity.

We wish to credit our own Research Integrity and Research Publishing teams and anonymous and named external researchers and research integrity experts for contributing to this investigation.

The corresponding author, as the representative of all authors, has been given the opportunity to register their agreement or disagreement to this retraction. We have kept a record of any response received.

References

[1] W. Fu and L. Wang, "Software Security Testing through Coverage in Deep Neural Networks," *Security and Communication Networks*, vol. 2022, Article ID 2834982, 7 pages, 2022.

Hindawi
Security and Communication Networks
Volume 2022, Article ID 2834982, 7 pages
https://doi.org/10.1155/2022/2834982

Research Article

Software Security Testing through Coverage in Deep Neural Networks

Weiyu Fu [1,2] **and Lixia Wang** [3,4]

[1]*School of Computer Science and Technology, China University of Mining and Technology, Xuzhou, Jiangsu 221116, China*
[2]*Jiangsu Vocational College of Finance and Economics, Huai'an, Jiangsu 223003, China*
[3]*School of Management, China University of Mining and Technology, Xuzhou, Jiangsu 221116, China*
[4]*School of Business Administration, Henan Polytechnic University, Jiaozuo, Henan 454003, China*

Correspondence should be addressed to Weiyu Fu; 19800341@jscj.edu.cn and Lixia Wang; wanglx@hpu.edu.cn

Received 6 July 2022; Revised 7 August 2022; Accepted 13 August 2022; Published 31 August 2022

Academic Editor: Zhiping Cai

With the continuous progress of society, computer technology and information technology are also experiencing rapid development. Especially in recent years, the application of computer technology has rapidly entered into people's daily life. As people's lives become richer, these applications have become particularly complex. For some large software, tens of thousands of function points or millions of lines of source code may be triggered to support it when performing related tasks. As a result, the security of such a complicated and excellent software becomes quite essential. The most effective way to ensure software security is to test the security of software products during the development process. A precise and effective security testing process is the basis for ensuring that software is tested for security. Without a detailed scientific software security testing model to guide software development for security testing, software security testing will become very difficult. This not only wastes more time and money but also does not guarantee the security of the software. A great security testing methodology should be able to find security problems that may be hidden deep within the software. In addition, a scientific process management can greatly facilitate the implementation of software security testing. As a result, it is relatively meaningful to establish a complete software security testing process model, generate excellent security test cases, and develop security process management tools for software security testing. At the same time, in recent years, deep learning has gradually entered more and more people's lives. However, the widespread application of deep learning systems can bring convenience to human life but also bring some hidden dangers. Hence, deep neural networks must be adequately tested to eliminate as many security risks as possible in some safety-critical software that involves personal and property safety. As the foundation of deep learning systems, deep neural networks should be adequately tested for security. However, deep learning systems are fundamentally different from traditional software testing, so traditional software testing techniques cannot be directly applied to deep neural network testing. In recent years, many scholars in related fields have proposed coverage guidelines based on deep learning testing, but the usefulness of these guidelines is still debatable. Based on the complexity of the large software development process and the fact that the interrelationship between nodes often constitutes a complex network of collaborative relationships, this study applies coverage-based testing in deep neural networks to test the security of software. To be specific, this research applies metrics such as peak coverage, speed to peak, and computational speed to evaluate coverage criteria and to investigate the feasibility of using coverage to guide test case selection to select solutions for security testing.

1. Introduction

With the rapid development of information technology, the third technological revolution has led mankind into the information age. In this context, the pervasive information technology has changed the traditional production, life, and communication methods of human beings [1]. However, the rapid development and unprecedented prosperity of the information industry have also brought negative effects [2]. Software security incidents have occurred more frequently

in recent years, bringing not only a lot of inconvenience to the country and people's lives but also a lot of damage. What is worse, the rate of such incidents is also increasing [3]. Nowadays, the security of software is more important than ever, so it is necessary to ensure and use secure software. How to ensure the security of software products has become an important issue that people must address [4]. Software testing is a key technology to ensure the software security and an important method to ensure software quality and reliability. To be specific, software testing is the process of manually or automatically analyzing software to check whether it meets design requirements [5]. As the complexity of software increases and the scale of software expands, the importance of software testing grows. Software security testing is a crucial way to ensure the quality and safety of software and to reduce its own instability [6]. It can prevent security incidents from occurring or minimize damage in the event of an incident. For technical and cost reasons, the focus has been solely on the usability of computers and networks, with no consideration given to security from design to implementation [7]. This has proven to create a variety of security risks for information infrastructures. After all, software is the soul of the information infrastructure [8]. Due to the historical lack of security and the reality of increasingly complex functional requirements, software designs often fail and malfunction, causing huge losses to society and users. Software testing is the process of manually or automatically analyzing software to check whether it meets design requirements [9]. Static source code analysis and dynamic target code runs are used to determine whether the software has the expected functions and properties. Security is a nonfunctional attribute of software, and software testing can identify, locate, and then eliminate software security risks [10]. As a result, software testing is a key technology to ensure the software security and is a necessary security tool in software development and maintenance.

Currently, software security testing is treated the same as regular software testing [11]. Most of the software security testing is done in the context of general software testing. As a result, there is a lack of a specific software security testing process model to guide the security testing process [12]. In addition, there is a lack of tools to manage the security testing process. This is obviously unfair and unscientific for both software security testing and software security quality assurance [13]. As security testing cannot be standardized scientific guidance, then the software security testing cannot be fully carried out, and the quality of software security cannot be strongly guaranteed. A precise security testing process is the basis for ensuring that software is tested for security [14]. Specifically, it not only ensures that software security testing is performed efficiently, saving time and costs but also further improves the security quality of the software. A great security test case can find the security problems that may be hidden in the software, it is the most basic guarantee and basis for security testing [15]. The analysis and design of the security test cases are based on the hazard analysis of the entire software requirements, which is fundamental to the quality of the security test cases. Excellent use cases can be used several times, which can also improve the efficiency and quality of testing [16]. A scientific process management can bring great convenience to the software security testing work and can also improve the efficiency of software security testing, saving manpower and material resources.

In terms of computer system framework, information security includes four levels: physical security [17], operational security [18], data security [19], and content security [20], as shown in Figure 1. Physical security refers to hardware security, which is mainly ensured by the security of the power supply system, hardware reliability, electromagnetic shielding, and personnel management [21]. Operational security refers to software security such as operating systems and application software. To be specific, this includes intrusion detection, vulnerability scanning, virus prevention and control, and emergency response [22]. Data security refers to the security of information in processing, storage, transmission, and use. This process can take authentication, cryptographic encryption, integrity verification, digital signature, and other algorithms and protocols for security reinforcement. Content security refers to the concealment and discovery of the true content of information to ensure its security [23]. This can be achieved through information identification, data mining, information filtering, and information hiding.

With the rapid development of computer technology, more and more software and applications are taking a significant place in human life [24]. These applications not only bring a lot of convenience and efficiency in doing various things but also bring a lot of possibilities to people. In recent years, deep learning and machine learning systems have gained great popularity in various applications, such as speech processing [25], building construction [26, 27, 28], image processing [29, 30], and human traffic detection [31]. Deep neural networks as a deep learning system are the key driver behind the recent success. However, while software systems based on deep neural networks bring convenience to humans, they also bring many serious problems. For example, a few years ago, there was a car accident involving a Google self-driving car in which people lost their lives, and several cases in which self-driving vehicles were unable to handle accidents and corner situations with varying degrees of consequences. All were misbehaviors exhibited by deep neural network software that led to serious consequences. In security-critical and other critical domains, deep neural networks exhibit misbehavior that can lead to irreversible and serious consequences. Therefore, it is necessary to adequately test deep neural networks to avoid misbehavior as much as possible.

At this stage, traditional software testing techniques have gradually matured. However, because of the fundamental difference between traditional software and neural networks, traditional software testing techniques cannot be directly applied to deep neural network testing [32]. In traditional software, each statement in a program performs certain operations that either transform the output from the previous statement to the next statement or change the state of the program. For traditional software, scholars have defined

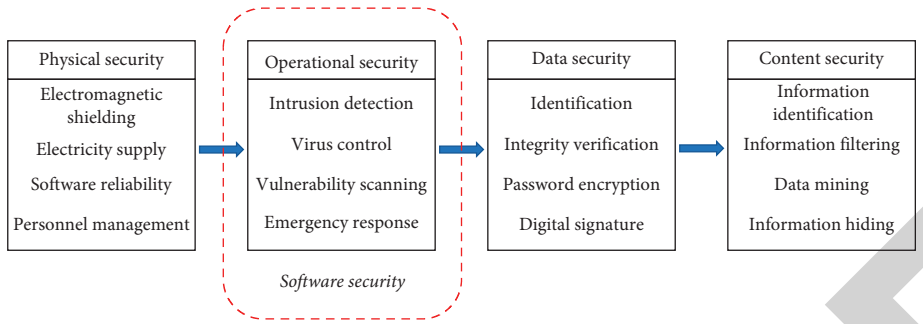


Figure 1: Computer system framework.

many coverage criteria at different levels in order to analyze the runtime behavior of the software from different perspectives. At the code level, there are now statement coverage, branch coverage, data flow coverage, and mutation testing [33]. Among them, statement coverage measures whether the target has executed every instruction. Branch coverage puts the target to test whether each branch of the control structure is covered. Both of these tests are based on control flow statements. Data flow coverage counts whether the definition of each variable is covered and thus detects data flow anomalies. At the model level, there are state coverage and transformation-based coverage. The model-based coverage criterion aims to cover more program behavior through abstract models. The many and varied coverage criteria above can be adapted to different testing methods and granularity.

The objective of testing deep neural networks is to identify potential errors, i.e., erroneous behaviors exhibited at runtime, and correct them in time [34]. In the test experiments, some counter samples are usually artificially added. In other words, samples that cause the model to give incorrect outputs with high confidence should be added to the data set by deliberately adding subtle disturbances. If these adversarial samples are well picked out by the experiment, it can be of great help to the deep neural network testing technique. In order to improve the efficiency of software testing as soon as possible, it is necessary to execute important test cases as early as possible so that defects in the system to be tested can be detected as soon as possible [35]. There are many criteria to measure the importance of a test case, including coverage, runtime, and how well the test case meets the requirements. If the coverage rate of a coverage criterion is used as the measure for test case selection, and more adversarial samples can be found in the selected test cases than in the random selection, then the coverage test can well guide the selection of adversarial samples to better find faults and defects.

As a result, it is of great theoretical and practical significance to establish a scientific and detailed software security testing process model to guide the software security testing in the development process. In the development-oriented process, it can improve the quality of software security testing and ensure that software security testing is carried out smoothly and efficiently, thus further improving the security quality of software. At the same time, based on the established software security testing process model, we design and implement software security testing process management tools, which have important engineering significance. In these contexts, this study investigates coverage testing in deep neural networks. First, some recently proposed coverage criteria will be evaluated, followed by a series of experiments to assess the efficiency of using coverage to guide the selection of test cases for testing the security of software development.

2. Deep Neural Network

Deep learning is a new field in machine learning research, which is motivated by the creation of neural networks that simulate the human brain for analytical learning. The "depth" of deep learning refers to the properties of the flow graph. In a deep neural network, data are input from the input layer and output from the output layer after passing through the hidden layer of the neural network. As a result, the computation involved in the data can be represented by the flow direction, and the property of this flow graph is the depth. Neural networks are the basis of deep learning, which is a technology that simulates the neural network of the human brain in order to achieve machine learning for artificial intelligence.

2.1. Framework of Deep Neural Network. A deep neural network consists of many neurons in several layers. That is, a deep neural network can connect multiple neurons to form a network. Figure 2 shows the most common model of a fully connected neural network. In Figure 2, there is one neuron in the input layer, one neuron in the output layer, and six neurons in the hidden layer. The hidden layer has two layers, each containing three neurons. In general, the number of neurons in the input and output layers is fixed and is determined by the input data and the format of the output. In contrast, the number of hidden layers and the number of neurons in each hidden layer are variable and can be defined by the training programmer. The neuronal interconnections represent the interactions of the neurons, and each connection corresponds to a weight. Therefore, a layer in which all neurons in the graph are connected to all neurons in the neighboring layers is called a fully connected layer.

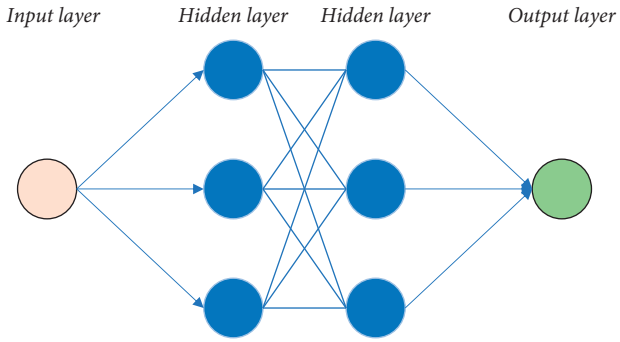


Figure 2: Fully connected neural network.

2.2. Calculation Process of Deep Neural Network. Neural network technology is a simulation of the human brain's nervous system, which consists mainly of neurons and a large number of synapses. As a result, a neuron can be understood as a function containing weights. The neuron in the upper layer passes the data to the neuron, which then performs the computation and passes the result to the neuron in the next layer. After multiple layers of computation, the result is abstracted to a higher level and finally, a computational result is an output based on the processing of multiple layers of neurons. Therefore, the calculation process of a deep neural network can be seen in Figure 3.

2.3. Adversarial Sample. Adversarial samples are mainly used for deep neural network testing. In fact, an adversarial sample is an input sample composed by intentionally adding a very small amount of interference to the data set. Although this sample is only slightly different from the original input sample, the model gives a completely wrong output with a high confidence level. In practice, the error rate of the test set can be reduced by adversarial training. That is, neural network training can be performed on the training set samples of the adversarial perturbation.

For example, in Figure 4, both the left and right images appear to be cats to the human eye, and humans cannot tell the difference between them. However, the right image is actually a sample image obtained by artificially changing a few pixels in the left image. For the model, the left image gives a 43.6% confidence level that it is a cat, while the right image gives an 89.6% confidence level that it is a dog. This is a completely different confidence result. The main reason for the formation of the adversarial sample is the excessive linearity of the model. Neural networks are mainly constructed from linear blocks. In some experiments, the overall function they implement is highly linear. If a linear function has many inputs, then its value can change very quickly. In deep neural networks, if a particular input is changed, even though the change is very small, it can have a huge impact on the result after a multidimensional computation.

2.4. Coverage in Deep Neural Network. In recent years, many deep neural network-based coverage criteria have been proposed by scholars in related fields. These criteria are

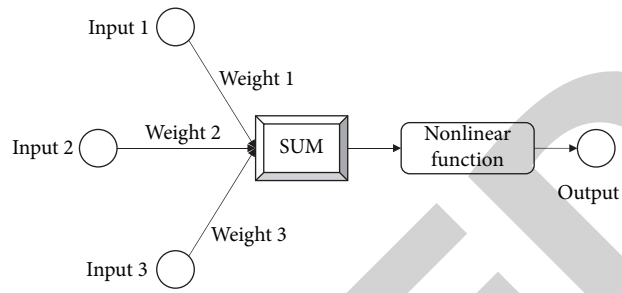


Figure 3: Calculation process of deep neural network.

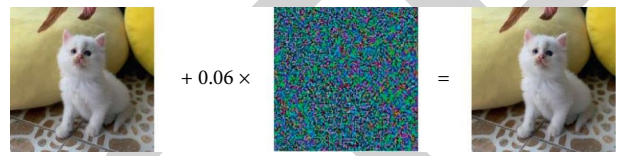


Figure 4: Example of adversarial sample.

either for the activation state of a single neuron or for the state of a combination of neurons in the same layer.

This research assumes that the set of neurons in the neural network is $M = \{m_1, m_2, , \ldots\}$, defines the set of test inputs as $K = \{k_1, k_2, \ldots\}$. The value of neuron m at the input k is recorded as $w(m, k)$. The threshold of activation is set to 0.

A neuron m is an active neuron if it is active under one of the test case inputs. The neuron coverage is the percentage of activated neurons to the total neurons. Therefore, the neuron coverage can be defined as follows:

$$MCov(S, k) = \frac{|\{m|\exists k \in S: w(m, k) > 0\}|}{|M|}. \quad (1)$$

When training the model, each neuron m can calculate its upper bound value based on the analysis of the training set data. As a result, the strong activation neuron coverage criterion can be defined as follows:

$$SMACov(S, k) = \frac{|\{m|\exists k \in S: w(m, k) \in (high, \infty\}|}{|M|}. \quad (2)$$

With the widespread use of deep learning, adversarial samples are an increasing threat to deep learning systems. By continuously feeding new types of adversarial samples and performing adversarial training, the robustness of the network can be continuously improved. This method is called brute force adversarial training because of the large amount of training data required. In addition, input gradient regularization can improve the robustness of adversarial attacks. The combination of this method and brute force adversarial training has good results, but there is still the problem of high computational complexity.

3. Software Security Testing

Software security is an engineering approach that enables software to continue to function correctly in the face of malicious attacks. In other words, software security is a

systematic, quantitative, and disciplined approach to guiding the construction of secure software. Software security is a key issue in information security. Due to the complexity of software functions and the inherent characteristics of programming languages, software flaws and vulnerabilities are inevitable. With the worldwide availability of the Internet, there have been numerous incidents of hackers exploiting software vulnerabilities to compromise systems via the network. As a result, there are high-risk security vulnerabilities in application and system software. By exploiting these vulnerabilities, attackers are often able to perform a range of unauthorized actions such as system access without local access to the computer. The knowledge architecture of software security is shown in Figure 5.

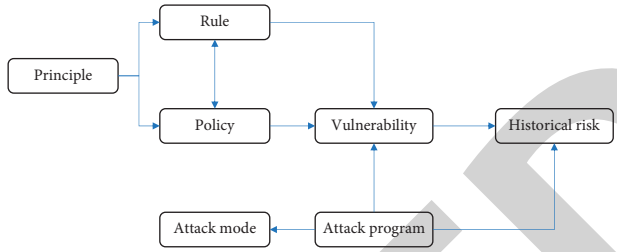


Figure 5: Knowledge architecture of software security.

3.1. Principle of Software Security Testing. Software testing is a complicated system engineering. During software testing, the tester must be well aware of the basic principles of software testing. Inadequate testing is a foolish act, while excessive testing of software is a sin. In general, the basic principles of software security testing are as follows.

Firstly, the most serious mistake made during software development is the failure of a software system to meet user requirements. Problems identified during system development can occur at some point in the early stages of development, so correcting errors must be done retroactively. In addition, software testing should be implemented early, preferably in the requirements phase. After all, the most unacceptable error is the failure of a system to meet user requirements. Figure 6 represents the general pattern of software vulnerabilities.

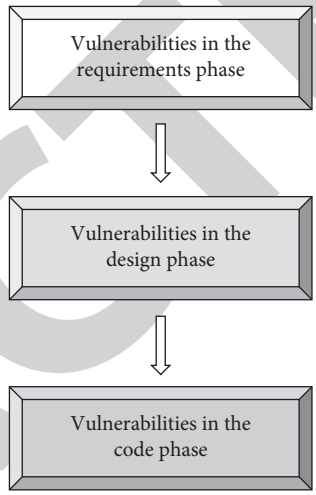


Figure 6: General pattern of software vulnerabilities.

Therefore, if problems are identified in a timely manner, the smaller the cost of solving the problem, which is the golden rule of software development.

3.2. Requirement of Software Security Testing. Software security testing is a specific process for solving problems that has been developed and tested over a long period of time in software development practice. It can guide the software development process from a macro perspective, control the risks in the software development process, shorten the software development cycle, and improve the quality of software. It is with the software security testing model that the cost of software can be predicted scientifically and the quality of software can be controlled reasonably. As a result, the software security testing should have the requirements as shown in Figure 7.

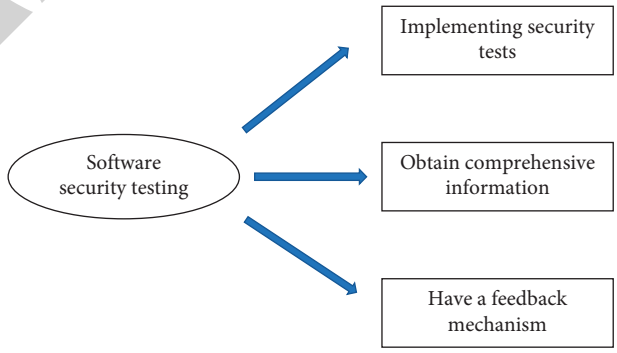


Figure 7: Requirements of software security testing.

3.3. Trajectory Model Design. The design of the software security testing process model aims to improve the confusion and confusion of software security testing in the software development process, and thus improve the efficiency of software security testing in the software development process. Based on the idea of the software development process and common testing model, as well as the analysis of software security and security testing content, a scientific security testing process model needs to be designed. The model starts from the perspective of software engineering and system security and links the software development process to the system security testing process. Then, the development process is analyzed and prepared accordingly, and security testing is performed for each of its process hazards.

In each subprocess of the software development process, its security is first analyzed. Once the security analysis is complete and ready, security testing is performed on it. This is a good way to deal with the security testing lag that can occur in software security testing. Each subprocess of the security testing process consists of several small cycles of testing activities, which can well solve the problem of frequent alternation and iteration of security testing.

Software security testing activities exist throughout the life cycle of software product development and are conducted simultaneously with the development process. The model is characterized by its ability to show not only the software development process but also to support the independence of the software development process from the software security testing process. Thus, the software development process and the software security testing process can be performed independently of each other. The development activity is an iterative process, and the security testing activity is an iterative security testing process that follows the development activity.

4. Conclusion

With the rapid development of computer technology, deep learning and deep neural networks are becoming more and more important in people's daily life. As deep learning systems are used in critical areas where security is important, it is even more necessary to test their security. Obviously, if the system behaves completely wrongly due to some errors in the neural network in critical areas such as autonomous driving, automatic medical diagnosis, and face recognition systems, the results would be unthinkable. Although the testing of traditional software has become increasingly sophisticated, there are fundamental differences between deep neural networks and traditional software. As a result, traditional software testing techniques cannot be directly applied to deep neural network testing. In this context, how to test deep neural networks and how to judge the adequacy of a test has become a recent challenge. In this context, this paper introduces the basic concepts of neural networks from the structure, computational process, and adversarial samples. Then, this research introduces the testing of artificial neural networks, focusing on the testing framework of deep learning systems.

Although some theoretical and technical progress has been made in this study, there are still many problems that need to be further investigated. The following work needs to be further developed and studied in depth. For the dynamic knowledge base, the number of samples in the database should be expanded to improve the accuracy of behavior determination. The attack tree model is further refined to be closer to the realistic attack situation in terms of weight setting. Also, in addition to finding adversarial samples, efforts can also be focused on generating adversarial samples. Knowing which samples make the system make wrong judgments and thus improve the system is also a possible direction to improve the robustness of deep neural networks.

Data Availability

The labeled dataset used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that there are no conflicts of interest.

References

[1] M. Salahshour Rad, M. Nilashi, and H. Mohamed Dahlan, "Information technology adoption: a review of the literature and classification," *Universal Access in the Information Society*, vol. 17, no. 2, pp. 361–390, 2018.

[2] T. Alam, "Cloud computing and its role in the information technology," *IAIC Transactions on Sustainable Digital Innovation*, vol. 1, no. 2, pp. 108–115, 2020.

[3] H. Mumtaz, M. Alshayeb, S. Mahmood, and M. Niazi, "An empirical study to improve software security through the application of code refactoring," *Information and Software Technology*, vol. 96, pp. 112–125, 2018.

[4] L. Ben Othmane, G. Chehrazi, E. Bodden, P. Tsalovski, and A. D. Brucker, "Time for addressing software security issues: prediction models and impacting factors," *Data Science and Engineering*, vol. 2, no. 2, pp. 107–124, 2017.

[5] O. Bin Tauqeer, S. Jan, A. Omar Khadidos, A. Omar Khadidos, F. Qudus Khan, and S. Khattak, "Analysis of security testing techniques," *Intelligent Automation & Soft Computing*, vol. 29, no. 1, pp. 291–306, 2021.

[6] B. Aloraini, M. Nagappan, D. M. German, S. Hayashi, and Y. Higo, "An empirical study of security warnings from static application security testing tools," *Journal of Systems and Software*, vol. 158, Article ID 110427, 2019.

[7] P. Zech, M. Felderer, and R. Breu, "Knowledge-based security testing of web applications by logic programming," *International Journal on Software Tools for Technology Transfer*, vol. 21, no. 2, pp. 221–246, 2019.

[8] D. He, Q. Qiao, J. Gao, S. Chan, K. Zheng, and N. Guizani, "Simulation design for security testing of integrated electronic systems," *IEEE Network*, vol. 34, no. 1, pp. 159–165, 2020.

[9] P. Ping, Z. Xuan, and M. Xinyue, "Research on security test for application software based on spn," *Procedia Engineering*, vol. 174, pp. 1140–1147, 2017.

[10] L. Ma, H. Yang, J. Xu, Z. Yang, Q. Lao, and D. Yuan, "Code analysis with static application security testing for Python program," *Journal of Signal Processing Systems*, pp. 1–14, 2022.

[11] L. M. Alrawais, M. Alenezi, and M. Akour, "Security testing framework for web applications," *International Journal of Software Innovation*, vol. 6, no. 3, pp. 93–117, 2018.

[12] M. Peroli, F. De Meo, L. Viganò, and D. Guardini, "MobSTer: a model-based security testing framework for web applications," *Software Testing, Verification and Reliability*, vol. 28, no. 8, p. e1685, 2018.

[13] O. M. Pisareva, V. A. Alexeev, D. N. Mednikov, A. V. Starikovsky, and V. B. Kurguzov, "Creating a national certification system for unmanned vehicles: tasks of information security testing," *St. Petersburg State Polytechnical University Journal. Economics*, vol. 14, no. 2, pp. 63–80, 2021.

[14] N. M. Mohammed, M. Niazi, M. Alshayeb, and S. Mahmood, "Exploring software security approaches in software development lifecycle: a systematic mapping study," *Computer Standards & Interfaces*, vol. 50, pp. 107–115, 2017.

[15] M. Alenezi and S. Almuairfi, "Security risks in the software development lifecycle," *International Journal of Recent Technology and Engineering*, vol. 8, no. 3, pp. 7048–7055, 2019.

[16] M. Cheah, S. A. Shaikh, J. Bryans, and P. Wooderson, "Building an automotive security assurance case using systematic security evaluations," *Computers & Security*, vol. 77, pp. 360–379, 2018.

[17] B. Ali and A. I. Awad, "Cyber and physical security vulnerability assessment for IoT-based smart homes," *Sensors*, vol. 18, no. 3, p. 817, 2018.

Hindawi
Security and Communication Networks
Volume 2024, Article ID 9852152, 1 page
https://doi.org/10.1155/2024/9852152

Retraction

Retracted: Research on Securities Portfolio Model Based on Genetic Optimization Neural Network

Security and Communication Networks

Received 8 January 2024; Accepted 8 January 2024; Published 9 January 2024

This article has been retracted by Hindawi following an investigation undertaken by the publisher [1]. This investigation has uncovered evidence of one or more of the following indicators of systematic manipulation of the publication process:

(1) Discrepancies in scope

(2) Discrepancies in the description of the research reported

(3) Discrepancies between the availability of data and the research described

(4) Inappropriate citations

(5) Incoherent, meaningless and/or irrelevant content included in the article

(6) Manipulated or compromised peer review

The presence of these indicators undermines our confidence in the integrity of the article's content and we cannot, therefore, vouch for its reliability. Please note that this notice is intended solely to alert readers that the content of this article is unreliable. We have not investigated whether authors were aware of or involved in the systematic manipulation of the publication process.

Wiley and Hindawi regrets that the usual quality checks did not identify these issues before publication and have since put additional measures in place to safeguard research integrity.

We wish to credit our own Research Integrity and Research Publishing teams and anonymous and named external researchers and research integrity experts for contributing to this investigation.

The corresponding author, as the representative of all authors, has been given the opportunity to register their agreement or disagreement to this retraction. We have kept a record of any response received.

References

[1] P. Zhang, "Research on Securities Portfolio Model Based on Genetic Optimization Neural Network," *Security and Communication Networks*, vol. 2022, Article ID 6476168, 10 pages, 2022.

Hindawi
Security and Communication Networks
Volume 2022, Article ID 6476168, 10 pages
https://doi.org/10.1155/2022/6476168

Research Article

Research on Securities Portfolio Model Based on Genetic Optimization Neural Network

Puming Zhang

Department of Economics and Management, Weinan Normal University, Weinan 714099, Shaanxi, China

Correspondence should be addressed to Puming Zhang; zhangpuming@wnu.edu.cn

Received 27 May 2022; Revised 11 July 2022; Accepted 22 July 2022; Published 29 August 2022

Academic Editor: Zhiping Cai

Portfolio is an investment management concept different from individual asset management. This consideration leads to an interesting result, that is, investors should buy a variety of securities at the same time instead of one kind of securities for diversified investment. Aiming at the limitations of BPNN (BP neural network) in traditional artificial neural network and its shortcomings such as many iterations, low convergence accuracy, and poor generalization, a portfolio method based on GA_BPNN (Genetic Optimization Neural Network) was proposed. The setting of GA (genetic algorithm) parameters and BPNN parameters are discussed in detail, and the implementation steps of genetic BP algorithm are described. The results show that the evaluation indexes of GA_BPNN prediction model are obviously better than those of the comparison prediction model, with the coincidence rate of 77.96% and the average absolute error of 12.451. The combination of GA and BPNN can effectively solve this problem. The simulation results of optimizing securities portfolio show that its optimization scheme is better than quadratic programming method, and this method is more correct, efficient, and practical.

1. Introduction

Investors always hope to get as high a return as possible and take as little risk as possible during the period of holding securities, and with the increase of return, the risk of securities also increases. How to make the securities investors get as high a return as possible at a certain level of risk or make the risk of securities investment as small as possible at a certain level of return? The most sensible way is to diversify the funds into a number of securities to form a portfolio. Due to the inherent speculative and high-risk characteristics of the securities market, in the trading of the securities market, the holders of the securities share a certain investment income but also conditionally bear the investment risks caused by the production risks. Using intelligent algorithms to solve portfolio problems has attracted more and more attention of academic researchers. The advantages of intelligent algorithm in solving portfolio optimization problems are becoming more and more obvious. The research of modern portfolio theory has proved that GA (genetic algorithm) can effectively solve portfolio optimization problems.

Optimization technology is based on mathematics and widely used in industry, agriculture, economy, medicine, and other fields to solve various engineering problems. BPNN (BP neural network) in artificial neural network is based on the optimization technology. It has the characteristics of simple structure, intelligence, strong self-adaptive ability, and strong self-learning ability and has been widely used in signal prediction and combination optimization [1]. However, the traditional BPNN adopts gradient descent method to solve the optimal problem, which is easy to fall into local extremum, and its network convergence speed is slow [2]. Todea and Pleșoianu summarized and studied the overconfidence theory in detail and established a behavioral financial model of overconfidence [3]. Wu et al. established a capital asset pricing model to accurately describe the return and risk of assets and studied the relationship between the expected return of assets and risky assets in the securities market, as well as the formation of equilibrium prices [4]. Hanafizadeh et al. effectively solved the time adaptability problem of portfolio optimization model by establishing genetic network programming model [5]. Moeen used

cultural gene algorithm to improve the utility of portfolio in static and dynamic trading environment and solved the problem of time adaptability of portfolio [6].

Generally, investors analyze the price of securities through two analysis techniques, namely basic analysis and technical analysis. Because their assumptions are often far from reality, they have only theoretical significance, and the effect of practical application is poor [7, 8]. With the gradual establishment of chaos and fractal theory in the securities market, people began to use neural network to predict the changes of the securities market. The learning of BPNN has the weakness of weak global searchability and easy to fall into local minima, while GA does not require the continuity of the objective function, so it has good global searchability. On the basis of obtaining the effective solution, this paper provides a method to obtain the optimal solution. By using this method, we can obtain the optimal portfolio of securities that satisfies investors with specific preferences. The validity of the model is verified by the actual historical data of the securities market, and a good conclusion is obtained.

2. Related Work

2.1. Research on the Portfolio Model. The investment theory has developed with the development of the securities market. The purpose of investment portfolio is to allocate assets in unrelated multi-markets and to reduce and avoid the risks caused by market uncertainty by diversifying investment. With the establishment and improvement of China's socialist market economic system and the continuous development of the financial market, the research on securities portfolio has become more and more extensive.

Lee et al. explained the Black-Litterman model step by step by combining the insights from some articles related to the model and made an empirical analysis of the model with eight types of assets such as US Treasury bonds [9]. The author also puts forward a new method to restrain the excessive bias caused by investors' views and increase the usability of the model. Goddard and Marcum introduced liquidity risk measurement constraints on the basis of Black-Litterman model, put forward a new model and method for optimizing asset allocation, and improved the portfolio selection model based solely on historical returns and historical volatility [10]. Delong proposed to use Bayesian moving average method to simulate and predict investors' subjective returns, and substituted it into Black-Litterman model to get the asset allocation weight [11].

Clouse proposed a particle swarm optimization algorithm with symbiotic multipopulation to solve the portfolio optimization problem. A portfolio model of energy adaptability under new assets is proposed [12]. Tsai et al. put forward a new risk function based on semiabsolute deviation risk function and minimax principle-minimax semiabsolute deviation risk function [13]. Zhang introduced the application strategies of neural networks in financial fields such as investment, portfolio decision-making, and stock forecasting [14]. However, due to the noisy and unstable characteristics of the stock market, these predictions still have not achieved satisfactory results.

2.2. Neural Network-Related Research. Neural network is a mathematical model that aims to simulate the processing mechanism of the brain nervous system to the outside complex information. It has shown good intelligent characteristics in the fields of pattern recognition, intelligent robots, and automatic control. Neural network composed of many adaptive elements connected by parallel computing, which can process information in the same way as biological neural network.

Neural network can be used for large-scale parallel processing and distributed information storage. It has good self-learning, self-adaptation, self-organization, strong associative memory, and fault-tolerance functions and can fully approximate any complex nonlinear relationship. Bhutto et al. showed that the neural network method is helpful to improve the prediction accuracy by comparing the neural network method with the traditional statistical prediction method [15]; Wang and Chuang used BPNN to predict and analyze the fluctuation law of public utility index and achieved ideal prediction results [16]. Alimoradi et al. modeled and predicted the stock price based on sparse Bayesian extreme learning machine [17]. Chan et al. put forward a stock price prediction model based on BPNN and grey model [18] in view of the shortcomings of the existing algorithms such as low prediction accuracy and large lag. Zhang et al. used normalization and principal component analysis methods to preprocess the historical data of a listed company's stock trading, designed a BP learning algorithm training parameter with multilayer network structure based on driving quantity term, and used the activation function ReLU (Rectified Linear Units) and the weight initialization method to modify the deeply sparse neural network model [19].

GA is the product of the intersection and penetration of life science and engineering science. There are five elements involved in GA: parameter coding, setting of initial population, design of fitness function, design of genetic operation, and setting of control parameters. Patra et al. proposed that each gene value should be represented by an N-based floating-point number, then divided into an integer part and a decimal part, and the new GA based on N-based partial coding operator was re-coded to make it have strong global searchability in the early stage and avoid falling into local extremum [20]. Sulkow et al. proposed a variable population size GA based on generation gap information [21]. Using the difference information of the optimal solution between adjacent generations of population, the population size was changed according to the logistic model when the premature phenomenon occurred in GA, and the diversity of the population was maintained. Balamurugan et al. proposed a crossover operator based on evolutionary algebra and individual fitness, which adaptively adjusted the crossover operation according to the fitness of each generation of individuals and the change of evolutionary algebra, so that the crossover was carried out in a direction conducive to the convergence of the algorithm [22].

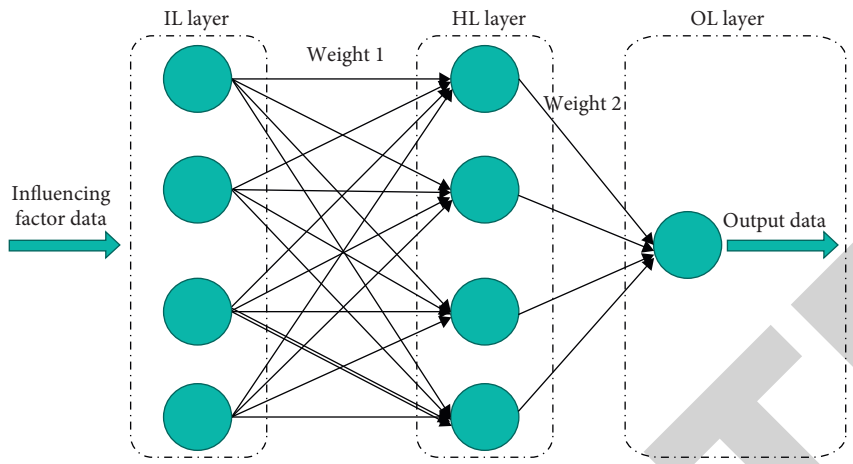


Figure 1: BPNN structure model.

3. Research Method

3.1. GA BPNN Thought. The topology of BPNN model includes IL (input layer), HL (hidden layer), and OL (output layer). Figure 1 shows the structure model of BPNN.

The relationship between the input and output of each HL is as follows:

$$\begin{aligned} n^k &= W^k V^{k-1} + b^k, \quad k = 1, 2, \ldots, M-1, \\ V^k &= f^k\left(W^k V^{k-1} + b^k\right), \quad k = 1, 2, \ldots, M-1. \end{aligned} \tag{1}$$

The input and output of the network are

$$Y = f^M\left(W^M V^{M-1} + b^M\right), \quad k = 1, 2, \ldots, M-1. \tag{2}$$

The learning process of BPNN can be divided into two parts: forward propagation of working signal and backward propagation of error signal:

(1) From IL to OL through HL, the weight of the network is constant in the process of signal forward transmission, and the state of each layer of neurons only affects the state of the next layer of neurons, which is called working signal forward propagation [18]; if the OL cannot get the desired output, the error signal will be transmitted back.

(2) The difference between the actual output and the expected output of the neural network is called error signal [19].

At present, in the practical application of artificial neural network, most neural network models adopt neural networks and their variations. It is also the core part of feedforward network, which embodies the essence of artificial neural network. BPNN has the ability to optimize calculation. However, there are local minimum problems in its optimization calculation, which must be improved.

At present, investors' expectations for investment decisions are constantly changing, and the same portfolio may not be universally applicable to different investors. It is also important to establish a corresponding portfolio optimization model for specific investors' preferences. According to the actual situation of the securities market, when the market share price index goes up, the prices of most stocks also go up; conversely, when the market share price index goes down, the prices of most stocks go down. That is, the

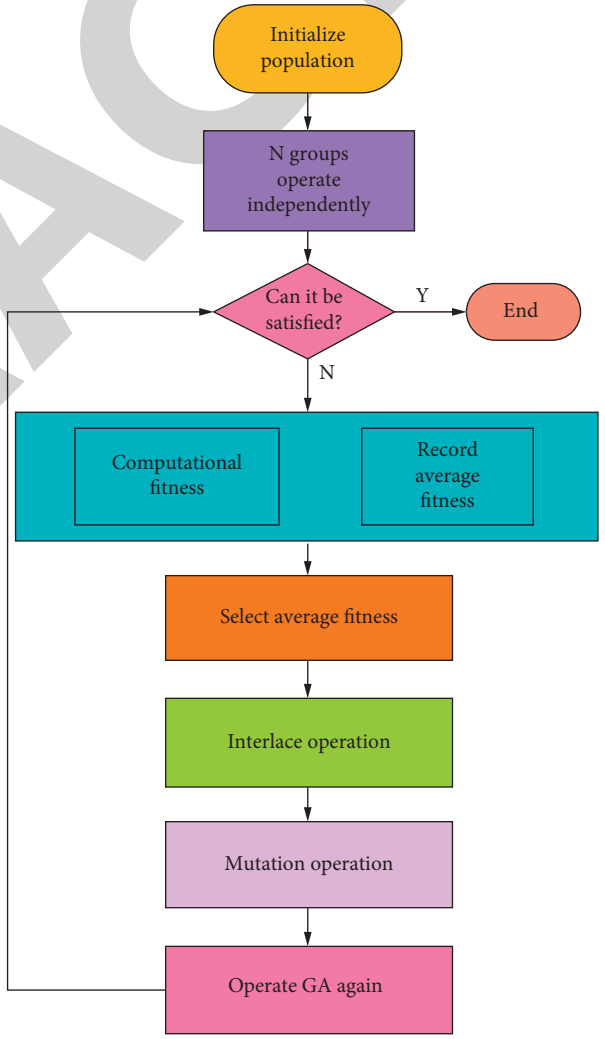


Figure 2: GA thought.

factors that can affect the stock price index of the securities market; microfactors refer to the specific internal environment of the company, such as the introduction of new products, major personnel changes, and other factors that affect the company's operations.

No matter in application, algorithm design, or basic theory, GA has made great progress and has become a hot research field concerned by many disciplines such as information science, computer science, operational research, and applied mathematics.

The structure of GA is open and has nothing to do with the problem, so it is easy to improve the execution strategy. The improvement of GA execution strategy includes hybrid GA, parallel GA, cooperative evolutionary algorithm, and chaotic GA. Figure 2 shows GA thoughts.

The stopping conditions in GA are generally determined in different ways according to different problems. For example, one of the following criteria can be used as a judgment condition: the maximum fitness of individuals in a population exceeds a preset value; the average fitness of individuals in the population exceeds the preset value; the generation number exceeds the preset value.

GA is a robust search algorithm that can be used for complex system optimization. Compared with the traditional optimization algorithm, it has the following characteristics:

(1) Some coding forms of GA dealing with decision variables enable us to learn from the concepts of chromosomes and genes in biology, imitate the genetic and evolutionary mechanism of natural organisms, and also enable us to conveniently apply genetic operators.

(2) The genetic manipulation of this population produces a new generation of population, which includes a lot of population information.

(3) GA increases the flexibility of its search process.

(4) GA filtering process is a parallel filtering mechanism.

3.2. Portfolio Model Design

3.2.1. Application of BPNN in Security Investment Portfolio. To make a portfolio investment, you must first select the securities for investment. When choosing the securities to invest in, we must first go through careful analysis. At present, there are two main types of analysis methods used in securities investment analysis: basic analysis and technical analysis. Basic analysis is a method to analyze the basic factors that determine the price of securities according to the basic principles of economics, finance, financial management, and investment. Technical analysis is to explore some typical laws and predict the future trend of the securities market by applying mathematical and logical methods to the past and present behavior of the market.

The single index model only considers a single factor that can affect the yield of securities, which is not in line with the actual securities market environment. Therefore, it is more reasonable to use the multi-index model to explain the factors that affect the yield of securities. The structure is divided into stock market, bond market, fund market and derivatives market according to the types of securities, and the submarkets are interrelated. The object of bond market transactions is bonds. Because of the fixed coupon rate and maturity, the market price of bonds is stable relative to the stock price. Therefore, it represents the ownership or creditor's right of a certain amount of property and the related right of income. In fact, the securities market is the place where property rights are directly exchanged.

BPNN securities portfolio allows individual samples in learning samples to have large errors or even complete errors. This is because every time the weights and thresholds of BPNN are corrected according to the characteristics of the whole learning sample, and the errors of individual samples will not affect the training process of BPNN. In the process of error signal back propagation, the weights of the network are adjusted by error feedback, and the actual output of the network is closer to the expected output through constant correction of the weights.

In the process of securities investment, investors and investment institutions all hope that they can invest the same amount of money in the securities market to obtain the maximum return while taking the minimum investment risk. However, according to the investment theory [2], it is impossible to have a portfolio that requires the minimum risk and the maximum investment return in theory or in practice.

To forecast the stock price is to use historical data to predict the future, but the securities system is a nonlinear and complex system, and some traditional forecasting methods, such as statistical methods, have poor results. GA is used to optimize the initial weights and thresholds of BPNN, and then the securities portfolio is carried out [12]. The research shows that genetic optimization can improve the efficiency and accuracy of BPNN's portfolio.

3.2.2. Implementation of Genetic Neural Network Optimization. To establish a portfolio model based on GA_BPNN, we must first analyze the invested assets, analyze the risk factors of assets, extract the indicators through factor analysis, screen the indicators by cluster analysis, establish the risk index system of stock assets, establish the weight set of indicators, objectively analyze the influence degree of each indicator on the risk of assets, establish the membership matrix, and judge the category of assets by the value of membership degree.

The main idea is to construct the so-called evaluation function with the help of the intuitive background in geometry or application, so as to transform the multiobjective optimization problem into a single-objective optimization problem.

In the process of GA execution, coding will directly affect genetic operations such as selection, crossover, and mutation. According to the above analysis, the objective function of this paper can be expressed as

$$\begin{cases} \min T = (1-\mu)\left(\sum_{x_i}\beta_i\right)\delta_m^2 - \mu\sum_{x_i}A_i \\ \text{s.t.}\sum_{x_i}=1 \end{cases}, \quad (3)$$

x_i represents the weight of the i th asset; $x_i \geq 0$ means that short selling of securities is not allowed in China.

In GA_BPNN algorithm, each chromosome is decomposed into connecting gene and parameter gene, and the two parts are coded by different coding methods. The code string consists of binary "0" and "1." Each binary number in the code string represents an HL neuron, "1" means that the neuron exists, and "0" means that it does not exist. Therefore, there are as many binary numbers of 0 or 1 as there are HL neurons, that is, the length of the binary code is equal to the number of HL nodes.

In GA, the fitness function value is used to measure the excellence degree of each individual in the group that can reach or approach or help to find the optimal solution in the optimization calculation. The fitness function of GA_BPNN algorithm is based on the total error of neural network, that is, the fitness function of each chromosome is taken as follows:

$$f = \frac{1}{1+E}, \quad (4)$$

where E is the total error in the neural network.

The selection operator of GA used to optimize BPNN usually chooses the fitness ratio selection method, and the probability of individual being selected in a population is directly proportional to its fitness value.

For the population whose fitness function is f, the probability of individual being selected is

$$P_{si} = \frac{f_i}{\sum_{i=1}^{n} f_i}. \quad (5)$$

In the above formula, P_{si} represents the probability that the ith individual is selected, n represents the number of training samples, and f_i represents the fitness value of the ith individual.

The arithmetic crossover operator is used to crossover the temporary population. Assuming that arithmetic crossover is performed between two individuals X_A^t, X_B^t, the two new individuals generated after the crossover operation are

$$\begin{aligned} X_A^{t+1} &= P_c X_B^{t+1} + (1-P_c)X_A^t, \\ X_B^{t+1} &= P_c X_A^t + (1-P_c)X_B^t, \end{aligned} \quad (6)$$

where P_c is a parameter, which can usually be set as a constant or a variable determined by evolutionary algebra. In order to improve the diversity of the population and ensure that there is no premature phenomenon in the later stage of the algorithm, P_c is an adaptive cross parameter.

Generally speaking, in GA, mutation operation acts on a single chromosome to generate a new chromosome. Specifically, in the kth iteration, the algorithm will generate another random number $\gamma_k \in (-1, 1)$. Let x_k be the chromosome selected from fea$X$ or infe$X$ set, and the algorithm uses the following rules to generate a new chromosome m_k:

$$m_k = x_k + \gamma_k. \quad (7)$$

In the mutation operation, all chromosomes selected with probability p_k will participate in the operation. After that, the algorithm will check the feasibility of these new chromosomes m_k and put them into fea$X$ and infe$X$ sets accordingly for the next iteration.

After optimization, the learning samples are trained and fitted. The optimized BPNN makes GA and BPNN give full play to their respective advantages, and their strengths and weaknesses are avoided. Compared with the traditional BPNN, the nonlinear fitting ability is greatly improved. The flow of BP algorithm is shown in Figure 3:

GA_BPNN algorithm steps:

(1) Initialize algorithm parameters. Generate a random initial population (i.e. the initial weight thresholds of N groups of neural networks).

(2) The weights and thresholds are given to BPNN in turn, and the global error of each chromosome is calculated for the given input set and output set. Calculate the population fitness.

(3) Evaluate fitness. The probability of individual selection is allocated, and individuals are selected by roulette wheel selection method.

(4) The arithmetic crossover operator is used to crossover the temporary population.

(5) The temporary population is mutated by mutation operator. The author adopts the adaptive uniform mutation operation, that is, the original gene value in the individual coding string is replaced by the adaptive probability.

(6) Global optimal convergence. Calculate the global error of the new individual.

(7) Output the individual with the best fitness value in the population. The optimized network connection weight coefficient and threshold can be obtained by decoding the optimal individual.

4. Result Analysis

In stock trading, the benefits and risks coexist. Maximizing the benefits and minimizing the risks are the goals pursued by all stock investors. The stock price fully reflects all relevant information, and the price changes are subject to random walk, while the prediction of the stock price is meaningless. However, the biggest controversy in classical literature focuses on the predictability of stock returns. The market efficiency itself cannot be tested, and the test of whether the price properly reflects the information must be carried out in an asset pricing model. Even if an abnormal case of earnings behavior is found, it may be due to the inefficiency of the market or the problem of the adopted equilibrium model.

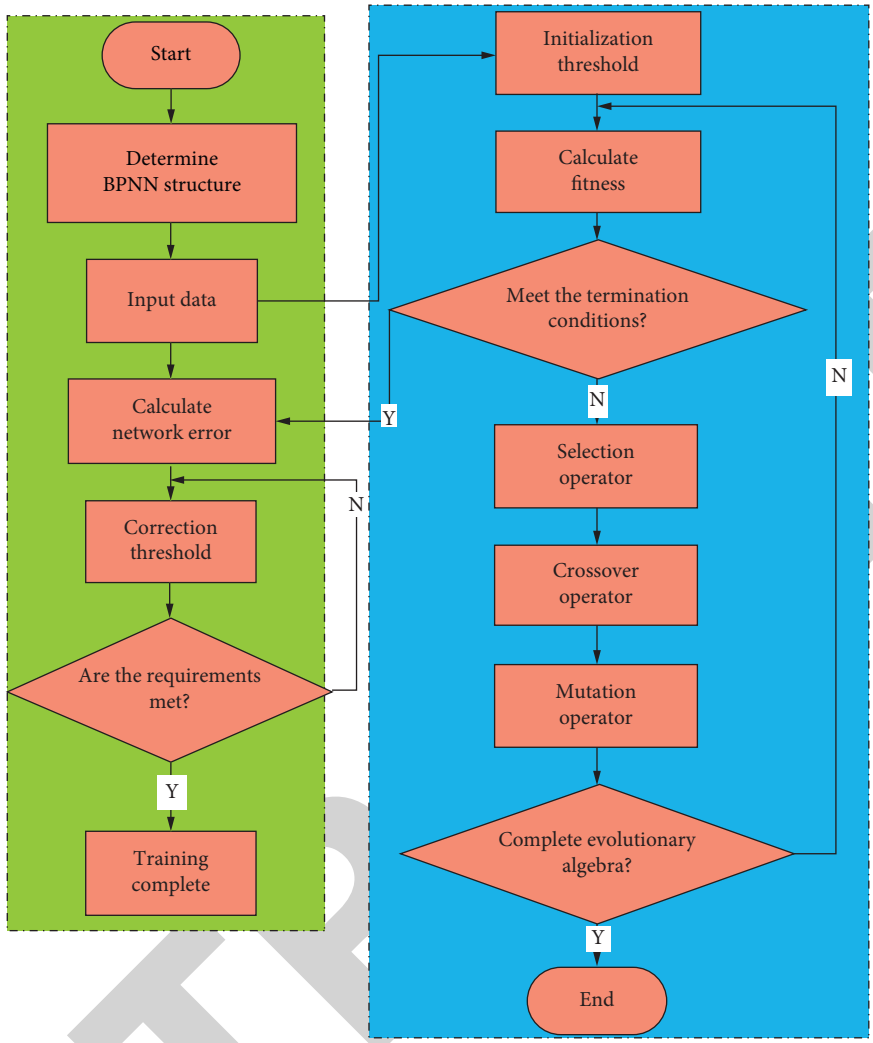


Figure 3: GA_BPNN algorithm flow.

This paper takes Markowitz's securities investment theory as the basic framework and capital asset pricing theory as the theoretical basis of securities portfolio, so as to simplify the model parameters and reduce the calculation workload [16]. Using MATLAB simulation software to analyze the data, the relationship between the ratio of securities investment, the rate of return and the risk loss rate are obtained (see Table 1 and Figure 4).

The rate of return increases with the increase of risk loss rate and will remain unchanged when the rate of return increases to a certain level. Therefore, the rate of return does not increase indefinitely with the risk loss rate. Through the above experimental analysis, it can be seen that a reasonable investment scheme can be selected according to investors' preferences by positioning a suitable expected value and risk loss value [18].

The selection of parameters in the model directly affects the solution effect and efficiency. For example, if the mutation probability is too small, the search space will be reduced, while if it is too large, it will degenerate into random search, which will reduce the stability of the population. If the evolution algebra is too large, the solution efficiency will be affected. In the mutation operation, the individuals to be mutated are randomly selected according to the mutation probability, then the mutated bits are randomly selected, and the weights of the two basic points are exchanged.

Although the solution obtained by this algorithm is only the suboptimal solution, it can be used as the optimal solution to some extent, because the optimization process characteristics of this solution are in line with the changing characteristics of the securities market and have certain fuzzy optimization characteristics, so it can be used as a portfolio allocation scheme.

Through the error comparison of many experiments, it is found that the GA-optimized BPNN has better initial weights and thresholds than the general BPNN. The former's initial weights and thresholds are close to the optimal solution, and it has a faster convergence speed and can reduce the occurrence of network oscillation, non-convergence, too long training time, and falling into local minima caused by improper initial connection weight thresholds. In this paper, 15 groups of test data are predicted by the trained network using test samples, and the results are shown in Figure 5:

Table 1: Average securities yield and investment ratio.

Securities name number	Coefficient 1	Coefficient 2	Average yield
1	0.036	0.56	−0.053
2	−0.021	0.13	0.013
3	−0.026	0.44	−0.021
4	−0.022	0.19	−0.011
5	−0.027	0.31	−0.086

Figure 4: Average return rate of securities and investment ratio chart.

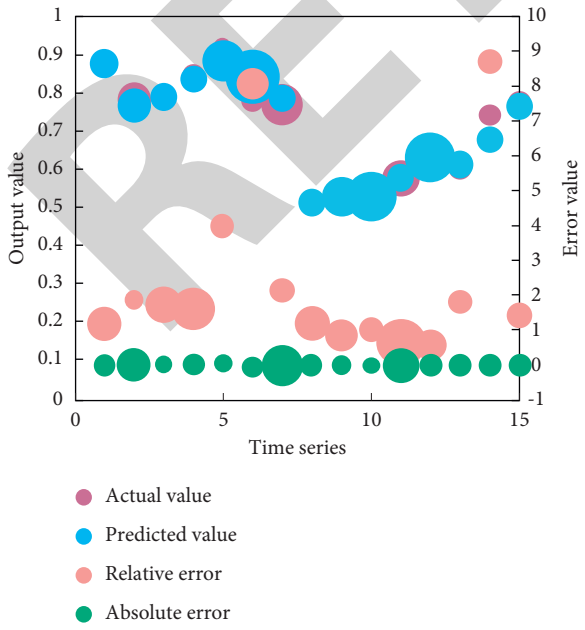


Figure 5: Prediction result.

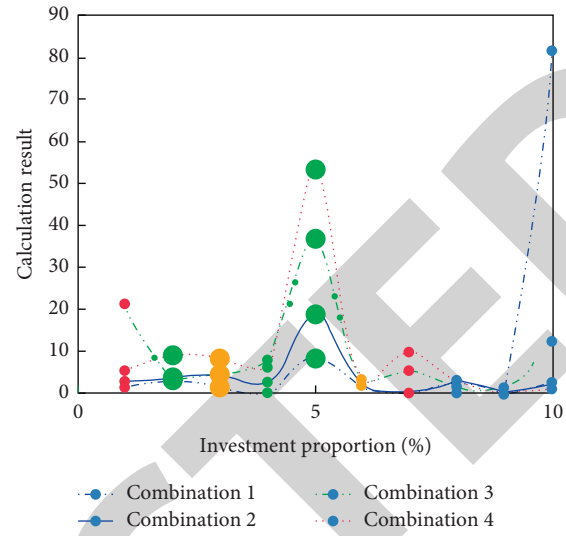


Figure 6: GA calculation results.

GA can effectively solve the nonlinear multiobjective optimization problem and avoid falling into local optimum. After each operator of GA is determined and the corresponding operation method is selected, GA is executed to search. In the developed market economy environment, the securities market is an important part of the complete market system. The securities market can reflect and adjust the movement of monetary funds and affect the development and operation of the whole economy. Securities market mainly includes participants, instruments, and places of securities market.

Because it has been transformed into a quadratic programming problem, there are many realized methods to obtain its optimal solution. In this research, we design and implement a model called parametric dual neural network to obtain its optimal solution. Therefore, the GA uses the objective function of the upper-level problem as the fitness function. It also provides guidance and suggestions on how to choose good initialization parameters when using this algorithm to solve other quadratic bilevel programming problems.

The stock market is a dynamic system that is constantly changing. As time goes by, the network system must be retrained in combination with the new data generated by the stock market to adapt to the changing situation, so as to get a better effect.

Now the problem is transformed into solving the indifference curve. It is assumed that investors' preferences are consistent, that is, regardless of the number of securities included in the portfolio, the determined indifference curve is the same. When the portfolio has the same risk, the more conservative the investor, the higher the return, otherwise he would rather give up his investment. Therefore, the calculation of the indifference curve is also subjective, and it is difficult for investors to determine the indifference curve that is really suitable for them, so they consider another way to obtain the best advantage.

Table 2: Yield error.

	Combination 1	Combination 2	Combination 3	Combination 4
$E(R)$ (%)	2.3016	2.6687	3.3427	3.9655
Error (%)	0.22	0.02	0.001	0.03

In this case, the problem to be considered changes from the relationship between R and σ to the relationship between S, a.

Different investors will take different S, a values. On the one hand, the value of S should be as large as possible, and on the other hand, the probability that the rate of return is lower than S should be controlled, and the result is shown in Figure 6:

Among them, combination l–4 is the concrete combination of the four best advantages in the case of risk-free assets obtained above. Because the effective boundary is generated by fitting numerous discrete points by the method of fitting the effective solution set, it will also lead to a certain error between the best point obtained by tangency between the indifference curve and the effective boundary curve and the best point calculated by GA, but as long as this error is within a certain range, it will be considered reasonable and can be ignored.

When the capital invested in a certain security is less than the specified value, it means that there is an error in the calculation of this item, and it needs to be corrected, whereas the opposite is not required, so it only needs to be reduced by 0. Therefore, no difference in yield is shown in Table 2:

From the above table, we can know that after ignoring the transaction cost in GA calculation, there may be errors in the obtained income, that is, the obtained optimal combination is not always exactly what investors need but may be less than the income generated by the combination required by investors. However, after analysis, the error is small, so this error is ignored here, that is, it is considered that this portfolio is the optimal portfolio required by investors.

This section compares and analyzes the expected return, variance, and Sharpe ratio of the two models according to the experimental results. The comparison of the expected return, variance, and Sharpe ratio of the two models is shown in Figure 7.

It can be seen that the return of this model is higher than that of ref [15] model when the risk level is basically the same, and it can be seen from the Sharpe ratio that this portfolio optimization model is obviously better than ref [15] model. Considering the transaction costs in the actual securities market, under the same conditions of risk and return, the fewer the assets in the portfolio, the less the transaction costs. Therefore, the portfolio optimization model in this paper is effective.

In order to compare the GA_BPNN prediction model with other neural network models, this paper selects the two most commonly used static neural networks, namely BPNN model and RBF (Radial Basis Function) neural network model. Comparison of prediction results is shown in Figure 8:

The evaluation indexes of GA_BPNN prediction model are obviously superior to RBF prediction model, which

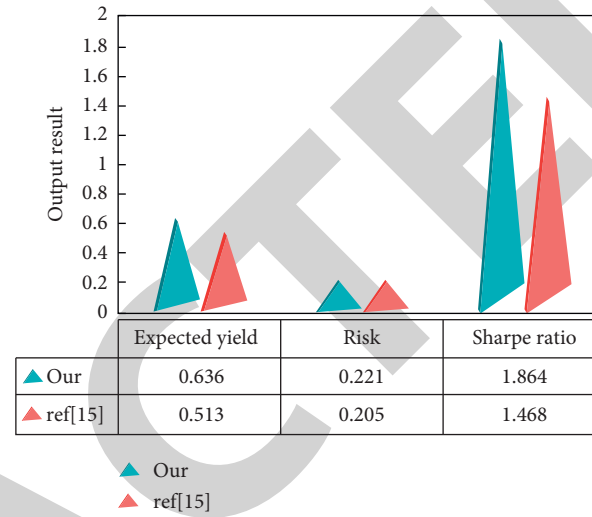


Figure 7: Model comparison diagram.

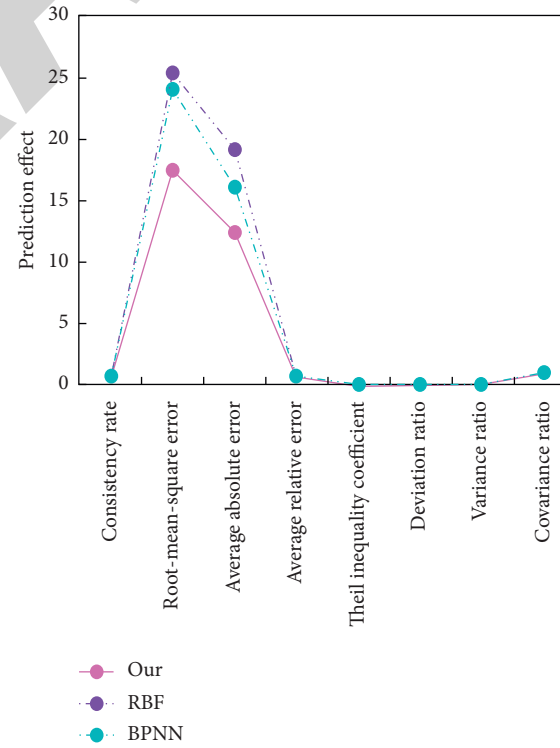


Figure 8: Comparison of prediction effects of three prediction models.

shows that the convergence speed of GA_BPNN prediction model system is fast, and the accuracy is higher. The coincidence rate is 77.96%, and the average absolute error is 12.451. This is because the initial weight of GA_BPNN is

composed of randomly generated uniform real numbers between -1 and 1, and it has the ability of "memory."

The factors that affect the stock price are complex and changeable. How to select the appropriate quantity from these complicated data factors directly affects the effective optimization and simplification of the network structure of the final forecast result. It is also the key of forecasting, which can not only improve the forecasting accuracy but also increase the operation speed.

The fluctuation of stock price is not completely random, it seems random and messy, but behind its complex surface, there is a deterministic mechanism, so there is a predictable component. The reason why an investor wants to sell his stock is because he thinks that the current price has reached its peak and will soon fall, or even if it rises, the increase will be limited and will not bring great profits. If there is no big change in the stock price as before after a certain news is published, it means that the news is not a factor affecting the stock market. If one day we see that the price jumps up a lot and the volume of transactions increases sharply, there must be one or several bullish news. What news is it, there is absolutely no need to ask, because it has already been reflected in the market behavior, and vice versa.

Many factors that affect the stock market include not only some quantitative data such as historical data, technical indicators, macro variables but also some qualitative data. If these factors are effectively quantified into the forecasting model and comprehensively analyzed, the forecasting accuracy will definitely be improved and more credible guidance will be provided for investors. The amount of sample data selected is mostly determined by experience, and it lacks theoretical guidance to predict the stock. How to select training samples as completely as possible to include the change pattern of the stock and provide the most effective data for online training is also a subject worth studying.

5. Conclusion

Since the portfolio theory was put forward, more and more scholars have devoted themselves to the research of portfolio model, especially the Black-Litterman model. The optimal portfolio can guide the company to choose the right investment object and its proportion when entering the capital market, so as to minimize the investment risk at a certain rate of return. According to the current situation of China's securities investment market, this paper puts forward the objective model of securities portfolio optimization based on GA_BPNN. Using the method of combining GA with neural network to solve complex optimization calculation problems can overcome the individual premature phenomenon caused by GA alone and the shortcomings of BPNN that are easy to converge locally. The optimal combination meeting the investment requirements of investors with specific preferences is obtained, which achieves a certain balance between maximizing the expected return and minimizing the uncertainty of the return rate. Therefore, the training samples of the network should be constantly adjusted with time. The research proves that it is an effective method to apply this model to the stock market forecast.

Data Availability

The labeled dataset used to support the findings of this study are available from the author upon request.

Conflicts of Interest

The author declares that there are no conflicts of interest.

Acknowledgments

This research was supported by Shaanxi Educational Science Planning Project + Research on The Teaching Mode Optimization of Securities Investment Curriculum + SGH20Y1272.

References

[1] R. A. Cohn, W. G. Lewellen, R. C. Lease, and G. G. Schlarbaum, "Individual investor risk aversion and investment portfolio composition," *The Journal of Finance*, vol. 30, no. 2, pp. 605–620, 2012.

[2] B. D. K. N. Ameha, "Oil prices, stock markets and portfolio investment: evidence from sector analysis in Europe over the last decade," *Energy Policy*, vol. 38, no. 8, pp. 4528–4539, 2010.

[3] A. Todea and A. Pleşoianu, "The influence of foreign portfolio investment on informational efficiency: empirical evidence from Central and Eastern European stock markets," *Economic Modelling*, vol. 33, no. 2, pp. 34–41, 2013.

[4] J. Wu, S. Li, and D. D. Selover, "Foreign direct investment vs. Foreign portfolio investment," *Management International Review*, vol. 52, no. 5, pp. 643–670, 2012.

[5] P. Hanafizadeh, A. Kazazi, and A. Jalili Bolhasani, "Portfolio design for investment companies through scenario planning," *Management Decision*, vol. 49, no. 4, pp. 513–532, 2011.

[6] M. Moeen, "Entry into nascent industries: disentangling a firm's capability portfolio at the time of investment versus market entry," *Strategic Management Journal*, vol. 38, no. 10, pp. 1986–2004, 2017.

[7] B. M. Ordu-Akkaya and U. Soytas, "Does foreign portfolio investment strengthen stock-commodity markets connection?" *Resources Policy*, vol. 65, Article ID 101536, 2020.

[8] R. Feinberg, "Cuba: portfolio of opportunities for foreign investment, 2016-17," *Foreign Affairs*, vol. 96, no. 2, 180 pages, 2017.

[9] S. K. Lee and S. S. Jang, "A portfolio approach in lodging firms' investment behavior: examining investment-disinvestment interdependency," *Cornell Hospitality Quarterly*, vol. 54, no. 3, pp. 318–326, 2013.

[10] G. J. Goddard and B. Marcum, "Real estate investment," *Journal of Portfolio Management*, vol. 31, no. 5, pp. 46–54, 2012.

[11] L. Delong, "Applications of time-delayed backward stochastic differential equations to pricing, hedging and portfolio management," *Quantitative Finance*, vol. 20, no. 3, pp. 333–418, 2012.

[12] T. Clouse, "Regulators boost foreign portfolio investment limits," *AIChE Journal*, vol. 59, no. 6, pp. 1934–1951, 2012.

[13] C. L. Tsai, H. Wang, and N. Zhu, "Does a bayesian approach generate robust forecasts? Evidence from applications in portfolio investment decisions," *Annals of the Institute of Statistical Mathematics*, vol. 62, no. 1, pp. 109–116, 2010.

Hindawi
Security and Communication Networks
Volume 2024, Article ID 9792589, 1 page
https://doi.org/10.1155/2024/9792589

Retraction

Retracted: Analysis of Risk Assessment of Overseas Infrastructure Projects Integrating BP-ANN Algorithm

Security and Communication Networks

Received 8 January 2024; Accepted 8 January 2024; Published 9 January 2024

This article has been retracted by Hindawi following an investigation undertaken by the publisher [1]. This investigation has uncovered evidence of one or more of the following indicators of systematic manipulation of the publication process:

(1) Discrepancies in scope

(2) Discrepancies in the description of the research reported

(3) Discrepancies between the availability of data and the research described

(4) Inappropriate citations

(5) Incoherent, meaningless and/or irrelevant content included in the article

(6) Manipulated or compromised peer review

The presence of these indicators undermines our confidence in the integrity of the article's content and we cannot, therefore, vouch for its reliability. Please note that this notice is intended solely to alert readers that the content of this article is unreliable. We have not investigated whether authors were aware of or involved in the systematic manipulation of the publication process.

Wiley and Hindawi regrets that the usual quality checks did not identify these issues before publication and have since put additional measures in place to safeguard research integrity.

We wish to credit our own Research Integrity and Research Publishing teams and anonymous and named external researchers and research integrity experts for contributing to this investigation.

The corresponding author, as the representative of all authors, has been given the opportunity to register their agreement or disagreement to this retraction. We have kept a record of any response received.

References

[1] C. Li and J. Zhou, "Analysis of Risk Assessment of Overseas Infrastructure Projects Integrating BP-ANN Algorithm," *Security and Communication Networks*, vol. 2022, Article ID 7864665, 13 pages, 2022.

Hindawi
Security and Communication Networks
Volume 2022, Article ID 7864665, 13 pages
https://doi.org/10.1155/2022/7864665

Research Article

Analysis of Risk Assessment of Overseas Infrastructure Projects Integrating BP-ANN Algorithm

Chengni Li[1] **and Jian Zhou**[2]

[1]*Auhui Audit College, Hefei 230601, China*
[2]*Anhui Fuhuang Architectural Design and Research Co., Ltd, Hefei 230601, China*

Correspondence should be addressed to Chengni Li; 2012010@ahsjxy.edu.cn

Received 11 April 2022; Revised 30 May 2022; Accepted 16 July 2022; Published 8 August 2022

Academic Editor: Fang Liu

In order to improve the risk assessment effect of infrastructure projects, this paper combines the BP-ANN algorithm to conduct risk assessment and analysis of overseas infrastructure projects to avoid the problem of slow learning and speed up network learning. Moreover, this paper normalizes the input value, and redefines the concept of risk on the basis of previous research. In addition, this paper sets up to record the basic information and risk-related information of the project. In order to verify the effectiveness of the algorithm, this paper predicts the training data, test data, and verification data, respectively, to verify the effectiveness of the algorithm, and collects existing overseas infrastructure project cases as samples to perform the simulation experiments. The experimental study shows that the risk assessment model of overseas infrastructure projects that integrates the BP-ANN algorithm proposed in this paper has a good risk analysis effect.

1. Introduction

At present, in the context of the slow recovery of the global economy, the pure pursuit of export growth in international trade can easily cause many frictions and contradictions. The "going out" foreign investment method is relatively easy to accept, and the "soft landing" investment method to deal with external demand is obviously a better path than simply exporting. Moreover, by implementing the "going out" investment method, large infrastructure companies can effectively drive the output of China's higher value-added products, such as the investment and construction of transportation infrastructure and subsequent management and operation. In addition, it is also in line with the direction of the country's supply-side reforms and the ultimate goal of industrial upgrading.

The environment faced by overseas infrastructure projects is very complex and uncontrollable. For example, the payback period of investment in overseas infrastructure projects is long, and long-term investment contract relationships must be planned, and long-term investment contracts are quite difficult to implement. Secondly, the planning of public facilities has a profound impact on the public, as well as a great impact on national security, economic development, and the environment. In addition, the object of the transaction is the government, because the government can use public opinion as a reason for changing policies, and use its power to change relevant legal provisions and influence court decisions. Therefore, it is not easy for private organizations to find a dynamic balance between environment, capability, and strategy when formulating strategies and goals [1].

Risk identification and assessment rely too much on experience, and mainly rely on the experience of experts, which is more subjective. Another method is to analyze the data accumulated over the years. However, the various countries outside the country are very different, and the accumulation of relevant data is seldom and has not reached a sufficient scale to support the judgment and management of project risks [2]. The risk sharing mechanism is not reasonable enough. Over the years, many domestic and foreign experts have conducted research on overseas

infrastructure models, but they still lack a large number of specific case experience support in terms of actual operation. The overseas infrastructure model structure is complex, and risk management is, to a large extent, the key to the success of overseas infrastructure projects. However, in practice, the private sector often enters the market after the project plan is determined, and the public sector has allocated the main risks of overseas infrastructure projects, resulting in an unreasonable share of the public-private partnership [3].

The risk management system is not sound. The risks of overseas infrastructure projects come from various risks such as international politics, economy, law, and projects. The demands of different stakeholders are very different. The construction of their risk management system is very important because the risks of each project are different. All the same, there is also a lack of a widely applicable risk management system. The management capabilities of private institutions need to be improved. The comprehensive capabilities and social responsibilities of private organizations need to be improved. For example, there is insufficient research on investment business policies in different overseas countries, and the effectiveness of related management such as its own investment strategy formulation, system construction, investment risk monitoring, and evaluation is not high. The government's role is insufficient. Under the overseas infrastructure model, the responsibility of government departments is to adopt good policy advantages to create a good investment and construction environment for the operation of overseas infrastructure projects, and to obtain certain benefits to ensure the quality of public facilities or services. However, the governments of some foreign countries are not perfect in policy formulation and supervision, and they have not played the role of the government well.

The topic selection of this paper is innovative. Through literature research, it is found that most of the PPP project research focuses on the transportation and municipal project industries, and rarely involves the cultural industry. In this paper, through the combination of qualitative and quantitative analysis, the BP-ANN algorithm is used to identify the risk factors of overseas projects, and then the analytic hierarchy process is used to evaluate the risk factors. The combination of subjective experience and objective data not only makes up for the purely subjective one-sidedness but also overcomes the limitations of pure objectivity. Through case analysis, risk control measures are proposed to provide reference for effective risk management of other projects.

In order to explore the risk assessment effect of overseas infrastructure projects, this paper constructs the BP-ANN algorithm, and uses the fusion algorithm to carry out the project risk assessment system to improve the risk assessment effect of overseas infrastructure projects.

2. Related Work

Literature [4] proposed that the definition of fuzzy set does not connect a given set with fuzzy elements. Due to the unclear and difficult to quantify factors in reality evaluation, fuzzy set theory uses mathematical methods to formulate and apply it for a suitable framework. Literature [5] describes a fuzzy connection expert system with learning ability, which adopts a fuzzy operator method for knowledge acquisition and allows the rule to be transformed into an equivalent connection network. The system developed by the fuzzy operator method was used to judge the credit risk of corporate loans and compared it with the existing conventional system. Literature [6] believes that because the definition of class is inherently vague, fuzzy set theory can provide a suitable framework for pattern classification. Based on the fuzzy pattern matching process, the fuzzy set theory is discussed, which combines partial matching values of given attributes. A new method based on fuzzy integral and possibility theory is proposed, and the statistical method and the supervised learning process are critically tested with the experimental test results of actual data.

Literature [7] proposes that the Analytic Hierarchy Process (AHP) allows rank maintenance (ideal mode) or allows rank reversal (distribution mode), which is an additive synthesis of priorities, and is therefore used in general feedback network decision-making structures with a hierarchical structure. Multi-linear vectors to reduce multi-dimensional measurements to a one-dimensional ratio scale. When using the analytic hierarchy process, the conditions under which the feature vector is sensitive to the judgment change should be determined. In order to extend the scale from 1–9 to 1-R, the selected indicators should be homogeneous. The analytic hierarchy process is simple, practical, flexible, and convenient. It combines qualitative indicators with quantitative indicators, decomposes the evaluation objectives in layers, compares the indicators at each level, and converts the comparison results into a judgment matrix, and checks the consistency of the constructed judgment matrix, to achieve the evaluation goal [8].

Literature [9] believes that the core of risk management is to accurately find out all possible risk factors of the project. Literature [10] proposes that the risks of overseas infrastructure projects can be divided into international risks and project risks. The former is caused by differences in political economy and investment environment, while the latter is related to the project level, such as construction, operation, financing, income. Literature [11] divides the risks from the different development stages of the project life cycle. Literature [12] believes that the risks of overseas infrastructure models can be classified from two perspectives, namely, whole-process risks and partial risks. The literature [13] analyzes the internal and external environment of the overseas infrastructure model, which is classified into macro risks, medium risks, and micro risks. The external risks of the project are macro risks, the internal risks in project implementation are medium risks and the project benefits. The way of cooperation between stakeholders and the risk of income distribution are micro-risks. Literature [14] divides overseas infrastructure risks into specific risks and system risks. Specific risks refer to risks related to the project, and system risks mainly refer to risks related to the global political and economic environment. Literature [15] classified the risks of overseas infrastructure projects from two perspectives: macro risks and micro risks. The macro aspects

mainly include political, economic, legal, and natural reasons, and the micro aspects mainly include financing, construction, operation, and cooperation. Researched from the perspective of micro-risk factor list identification, the literature [16] analyzed the risks of overseas infrastructure projects from the international level, project level, and customer level, citing the main sources of risks, including economic, political, legal, and technical, financing, construction, operation, user purchase, and other risks. Literature [17] divides the risks of overseas infrastructure into 7 categories in more detail: political, legal, credit, construction, market, financial, and natural environment risks, and identifies 33 key risk indicators. Literature [18] uses a questionnaire survey method to identify 20 key risk factors for overseas infrastructure projects. Literature [19] analyzes the overseas investment business of Chinese companies and proposes that the main sources of risk include: politics, corporate culture, information management, vicious competition, single investment structure, and insufficient international management capabilities. Literature [20] put forward five sources of risk: market, resources, capacity, and legal risks. Literature [21] analyzed the main risks in overseas infrastructure projects and put forward a list of risks.

3. Risk Assessment Combined with BP-ANN Algorithm

The establishment of neural network is based on MATLAB, which can easily call the neural network toolbox to establish the network model.

In order to avoid slow learning speed and speed up the network learning speed, the input value can be normalized so that the input signal of all samples varies between −1 and 1.

In MATLAB, the normalization of the data is generally processed by the mapminmax function, and the formula for the function is [22]:

$$(p_i)_n = 2 \times \frac{p_i \cdot (p)_{\min}}{(p)_{\max} \cdot (p)_{\min}} - 1. \tag{1}$$

Among them, (p_i) and p_i are the standard value and the original value of the parameter in the experimental data group, respectively, and $(p)_{\max}$ and $(p)_{\min}$ are the maximum and minimum values of the original value of the corresponding parameter, respectively.

When the final data is output, the result is denormalized to obtain the standard value of the result. The denormalization function can be expressed by (2):

$$p_i = \frac{[(p_i)_n + 1][(p)_{\max} - (p)_{\min}]}{2} + (p)_{\min}. \tag{2}$$

The range of the parameters after data normalization is between −1 and 1, avoiding the generalization problem of the network. At the same time, the convergence speed of NNs is accelerated.

In this paper, a feed-forward NNs model is established. A combination of tan-sigmoid and linear transform functions is used in multi-layer NNs and applied to the hidden layer and output layer, respectively.

The algorithm designs the number of network layers and the number of neurons contained in each layer. The number of input and output neurons of NNs is determined by the actual problem to be solved, which has nothing to do with network performance. This article considers 10 influencing parameters, that is, set 10 input values, and set an output value, that is, the shear capacity.

The superiority of the network greatly depends on the number of hidden layers and the number of neurons in the hidden layer. In order to select the optimal network, we generally refer to the results obtained by empirical formulas (3) and (4) to perform comprehensive test verification.

$$l = \sqrt{(m+n)} + a, \tag{3}$$

or

$$l = \sqrt{\left(0.43mn + 0.12n^2 + 2.54m + 0.77n + 0.35 + 0.51\right)}. \tag{4}$$

Among them, m and n are the number of neurons in the input layer and the number of neurons in the output layer, and a is a constant between 1 and 10.

The algorithm sets the learning rate (Ir) and momentum factor (mc). Based on experience and actual conditions, Ir-0.01 and mc = 0.4 are selected. At the same time, a convergence condition needs to be set, and the selection of this condition can neither be too harsh nor too relaxed. Too harsh conditions will lead to too fast convergence and inaccurate results. Too loose conditions will result in too slow calculation speed considering comprehensively.

When any one of the conditions is met, the algorithm stops training and outputs the result. The matrix expression of the BP-ANN structure is [23]:

$$O = f_3(LW_2 f_2(LW_1 f_1(IW \times I + b_1) + b_2) + b_3). \tag{5}$$

In (5), f_1, f_2 represents the hidden layer of the nonlinear (tan-sigmoid) function (6), and f_3 represents the application of the linear transform function (7) to the output layer. Its function expression form is

$$y_{ij} = \frac{1}{1 + \exp\left[-IW_{ijk}X_k + \theta_{ij}\right]}. \tag{6}$$

In the formula, y_{ij} is the output of the j-th neuron in the i-th layer, X_k is the k-th input, θ_{ij} is the j-th threshold of the i-th layer, and θ_{ij} is the weight of the i-th layer X_k corresponding to y_{ij} [24].

$$O = \sum_{k=1}^{n} LW_{3k} \times y_{3k}. \tag{7}$$

The BP-ANN model predicts the training data, test data, and verification data, respectively, and the results are shown in Figure 1. According to the comparison between the predicted results of the three sets of test data and the test values, the following results can be obtained. (1) The mean and variance of Vses/V xatit of training group, test group, and verification group are 1.049, 1.031, 0.977, and 0.012,

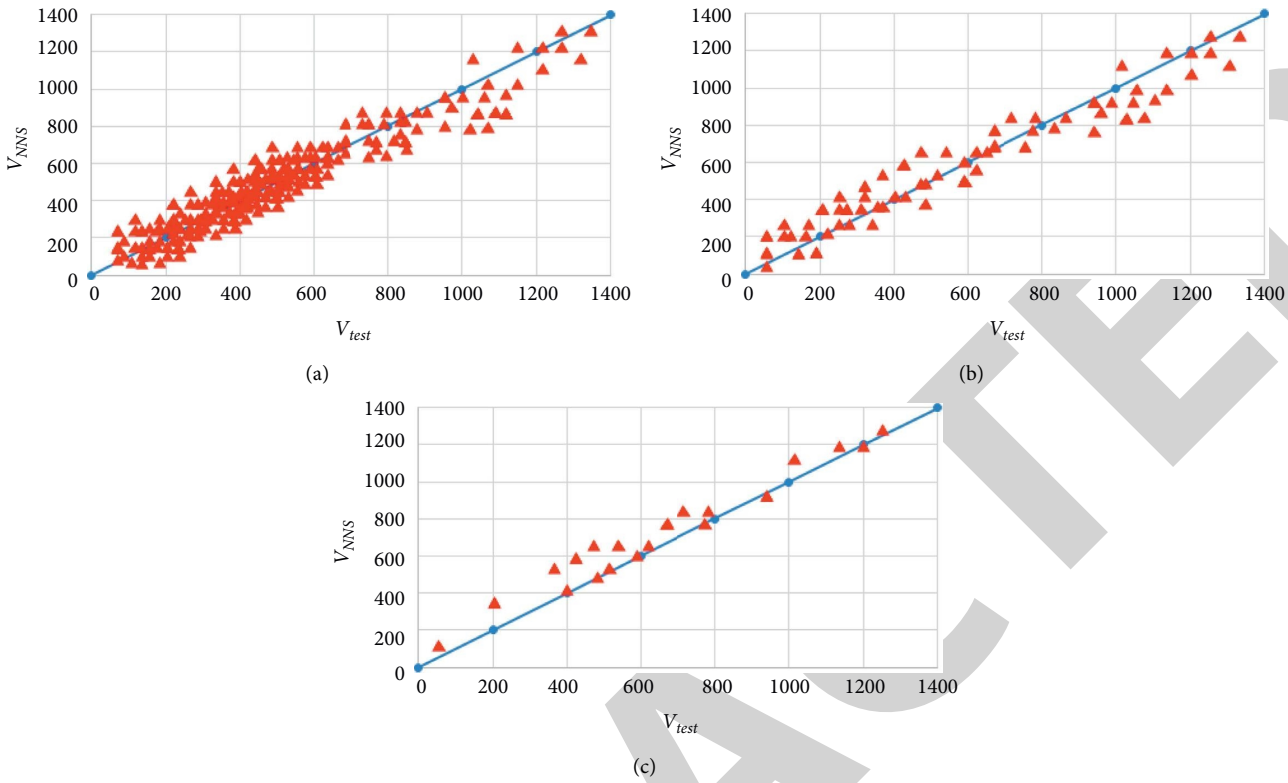


Figure 1: Comparative analysis of model training. (a) Training group. (b) Test group. (c) Verification group.

0.059, 0.020, respectively. (2) The shear capacity predicted based on the BP-ANN model is basically consistent with the experimental value, and the dispersion is small.

Monte Carlo (MC) method is a mathematical simulation method. This method uses random probability distribution sampling to construct random input variables in a given model, and then determines its sensitivity factors based on the model calculation values of random input variables. The analysis process is shown in Figure 2.

The sensitivity analysis (SA) method is a very practical tool in the process of modifying the parameters of the model. Through SA method analysis, we can intuitively see the influence of each input parameter in the model on the output value. Therefore, the input parameters with greater sensitivity can be given priority in the model optimization process. The parameters that are less sensitive, that is, have minimal impact on the output value of the model, can be eliminated, and the model can be optimized by reducing the complexity of the model.

At present, the importance of the SA method is recognized by most scholars, but most researchers have not made effective use of the SA method in the process of establishing the model. The main reason is that the calculation process is more complicated and the calculation results are difficult to explain clearly.

Sensitivity analysis includes global sensitivity analysis (Global Sensitivity Analysis, GSA) and local sensitivity analysis (Local Sensitivity Analysis, LSA). LSA only calculates the influence of a single parameter on the output value of the model, and the average value of other parameters. However, GSA calculates the total influence of multiple parameters on the model output value, and analyzes the influence of the coupling between the parameters on the model output value. The difference between LSA and GSA is that each input value changes within an infinite or finite range, and the change in model output value caused by a certain input value change is global. That is, the change of model output value is carried out under the joint action of all input values. GSA method can be divided into quantitative GSA method and qualitative GSA method. The qualitative GSA method only qualitatively analyzes the influence of the change of each input value of the model on the model result, also known as the factor screening of sensitivity analysis, which can sort the sensitivity of each input value of the model with a small amount of calculation. The quantitative GSA law is to quantitatively give the contribution rate of each input value change to the model output value change [25].

The advantage of LSA is strong operability. However, LSA also has several shortcomings. It only considers single factor changes, and can only analyze a single factor individually each time, which is very complicated in terms of calculation.

The LSA method only analyzes single-factor variables each time, so its calculation results ignore the influence of the coupling between the input parameters of the model on the output value. This is because when a single factor variable is analyzed, the changes of other input parameters will also affect the final sensitivity value. Therefore, the current research on SA is gradually biased towards the GSA method.

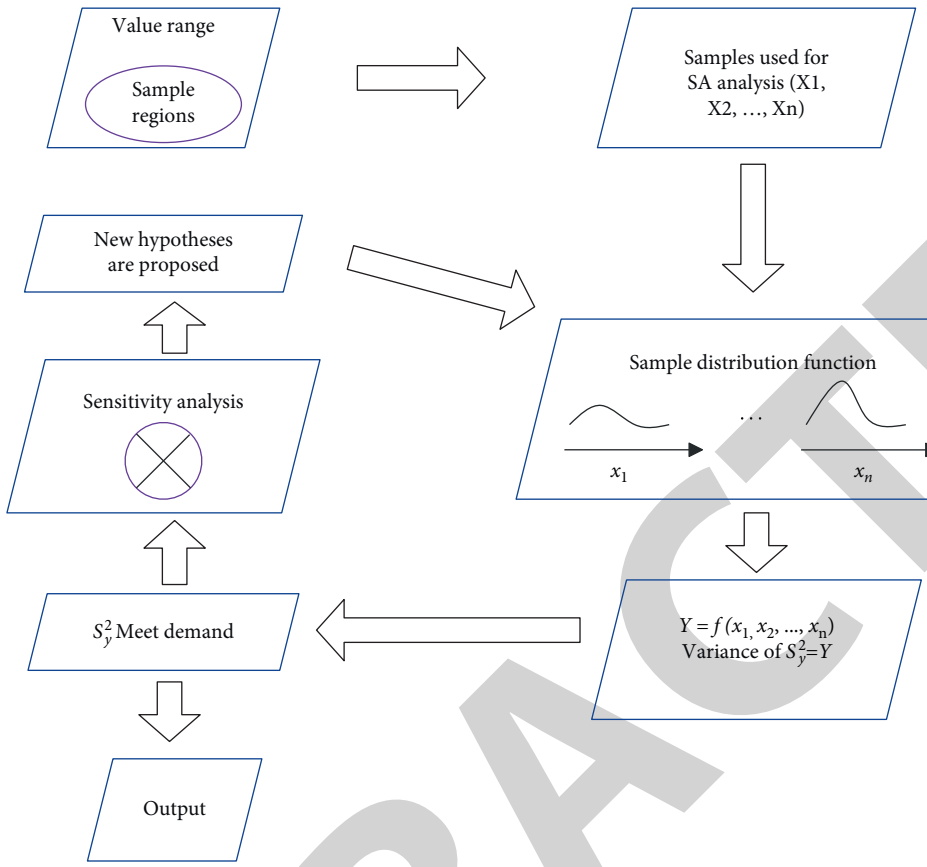


Figure 2: Sensitivity analysis steps.

As the domestic recognition of GSA is not high, almost all adopt LSA method at present.

LSA is also called single conversion method. Its calculation method is to control an input parameter separately, and set a fixed value for other parameters, and calculate the sensitivity value through the change of the model output value when the input parameter changes. There are two main methods. One is the single-factor transformation method, that is, the selected input parameter is incremented or decremented by 10% each time. The other is partial differentiation. Generally, the sensitivity coefficient is used as the calculation standard for the results of the SA method. The common sensitivity coefficient expressions are [26]:

$$S_i = \frac{dv}{dp_i}. \tag{8}$$

In the formula, p_i is the sensitivity value of the i-th input parameter, v is the predicted value of the model, and p_i is the i-th parameter.

The general view is that if the model is less sensitive to parameter errors, then the model is suitable for different situations, but this view is wrong. Because the parameter error in actual application may be far more than the change within the range of 10% or 20%, and may even reach a change of 2 times or 10 times. If the initialization parameters of the model are wrong, the model is insensitive to the 10% amplitude of parameter changes.

The global sensitivity analysis is as follows:

3.1. Multiple Regression Method. The multiple regression method based on Latin Hypercube Sampling (LHS) was published in 1979 by McKay. This method divides the cumulative distribution of the input parameter probability into multiple equidistant intervals, and LHS is more comprehensive and efficient than the ordinary random allocation sampling method. It divides the y-axis of each input value distribution probability function into multiple equidistant intervals from 0 to 1, and each equidistant interval corresponds to an equal probability parameter interval on the x-axis. Therefore, the value range of the probability function is divided into multiple equal probability parameter intervals. On the y-axis, the algorithm randomly samples in each divided interval to obtain the corresponding parameters on the x-axis.

For example, there are n input parameters in the model, and the probability distribution of each input parameter is equally divided into m intervals, and there are $n \times m$ sample combinations. In fact, the LHS method only takes m samples. The method is to list the values of the n input parameters as a matrix with n rows and m columns, and to disorder the value of each column of the matrix to obtain m inputs of each parameter. Each row of the matrix is used as the input value of each parameter, and the predicted value is

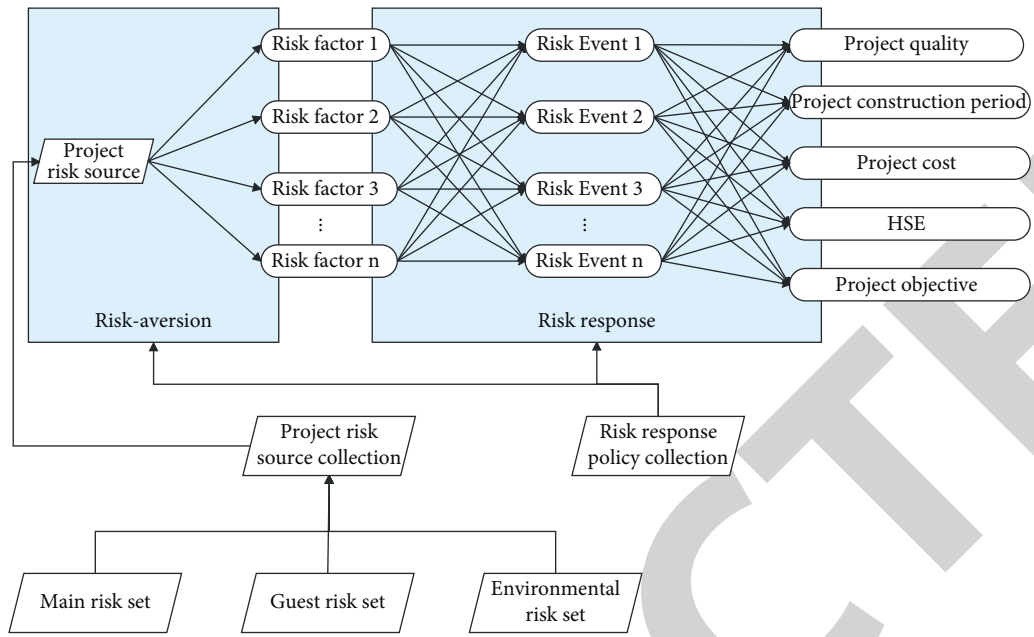


Figure 3: The risk assessment model for overseas infrastructure projects that integrates BP-ANN algorithm.

obtained by inputting the model. The sensitivity can be expressed by the multiple regression coefficient between the predicted value and the input value.

3.2. Extended Fourier Amplitude Sensitivity Test Method. The extended Fourier amplitude sensitivity test (EFAST) obtains the expansion of the Fourier series by Fourier transformation. According to a suitable search function, the model $y = f(x_1, x_2, \ldots, x_n)$ can be transformed into $y = f(k)$ through Fourier transformation:

$$\begin{aligned} y &= f(k) \\ &= \sum_{-\infty}^{+\infty} \left\{ A_j \cos\ jk + B_j \sin\ jk \right\}. \end{aligned} \tag{9}$$

Among them,

$$\begin{aligned} A_k &= \frac{1}{2\pi} \int_{-\pi}^{+\pi} f(k) \cos\ jk \mathrm{d}k, \\ B_k &= \frac{1}{2\pi} \int_{-\pi}^{+\pi} f(k) \sin\ jk \mathrm{d}k. \end{aligned} \tag{10}$$

In the formula, $j \in Z = \{-\infty, \ldots, -1, 0, 1, \ldots, +\infty\}$.

The expansion curve of the Fourier series is defined by $\Lambda_j = A_j^2 + B_j^2$, where $j \in Z$, $A_{-j} = A_j$, $\Lambda_{-j} = \Lambda_j$. The variance of the model result caused by the uncertainty of parameter x_i is

$$\begin{aligned} V_i &= \sum_{p \in Z^0} \Lambda p w_i \\ &= 2 \sum_{p=1}^{+\infty} \Lambda p w_i. \end{aligned} \tag{11}$$

Among them, $Z^0 = Z - \{0\}$. The total variance is

$$\begin{aligned} V &= \sum_{j \in Z^0} \Lambda_j \\ &= 2 \sum_{j=1}^{+\infty} \Lambda_j. \end{aligned} \tag{12}$$

Among them, $[-\pi, \pi]$ is taken at equal distances in the interval of b, and each k corresponds to an input parameter model after multiple runs of the model, and A_j and B_j can be approximated by the following equations:

$$\begin{aligned} A_j &= \frac{1}{Ns} \sum_{k=1}^{Ns} f(s_k) \cos(j s_k), \\ B_j &= \frac{1}{Ns} \sum_{k=1}^{Ns} f(s_k) \cos(j s_k). \end{aligned} \tag{13}$$

Among them, $j \in \overline{Z}$, and N_s is equal to the number of samples, $\overline{Z} = \{-Ns - 1/2, \ldots, -1, 0, 1, \ldots, Ns - 1/2\}$. From the frequency w_i corresponding to A_j and B_j and the parameter x_i, the variance Vi corresponding to each parameter and the total variance V of the calculated value are obtained by formulas (11) and (12). Through $S_{i_1, i_2, \ldots, i_s} = V_{i_1, i_2, \ldots, i_s} / V$, the sensitivity of each parameter can be obtained. Through $S_{T_i} = \sum S_{(i)}$, the overall sensitivity of parameter x_i can be calculated.

The advantage of EFAST is that the amount of calculation is much smaller. EFAST only needs one sampling to obtain the primary sensitivity and total sensitivity of a certain parameter at the same time. However, EFAST requires that the input parameters of the model are irrelevant.

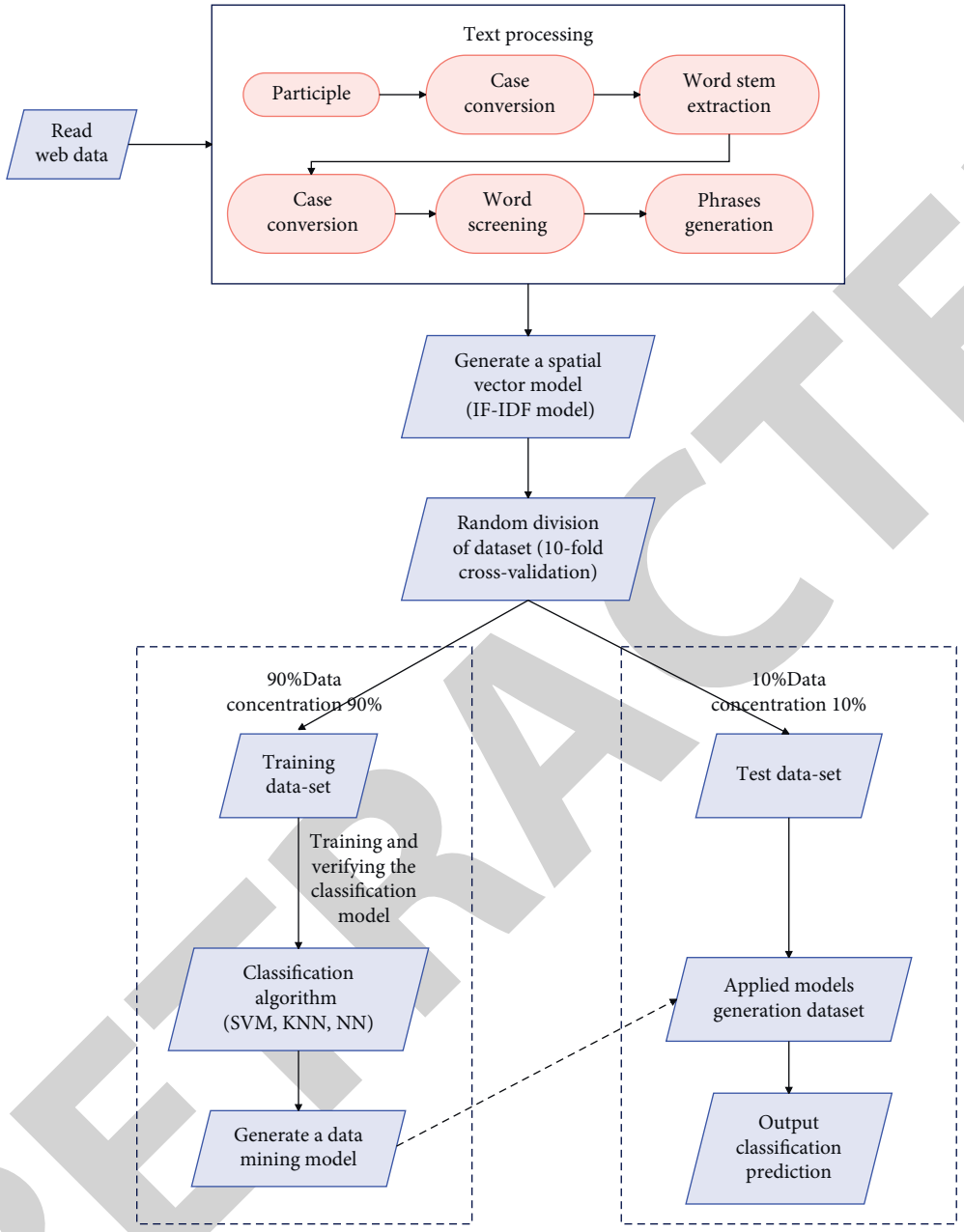


Figure 4: Schematic diagram of the text classification model process.

3.3. Morris Method. The Morris method maps the value range of each parameter to [0, 1], and then discretizes to consider the $m \times k$ $(m = k + 1)$ matrix B:

$$\begin{bmatrix} 0 & 0 & 0 & \ldots & 0 \\ 1 & 0 & 0 & \ldots & 0 \\ 1 & 1 & 0 & \ldots & 0 \\ 1 & 1 & 1 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 1 & 1 & 1 & 1 & 1 \end{bmatrix}, \tag{14}$$

and increment $\Delta B_{i,j} = s/n - 1$, where s is the variable factor and n is the number of parameter samples. Only one parameter of two adjacent rows in the matrix $\triangle$B has a different value, and the increment is $\triangle$. Therefore, by using two adjacent rows as model input parameters, the output values y_1 and y_2 of the model can be obtained.

$$\partial_i(x) = \frac{(y_1 - y_2)}{\Delta}. \tag{15}$$

Formula (12) can calculate the sensitivity of model input parameters. The sensitivity of all n input parameters can be obtained by taking all n groups of adjacent row elements as the input parameters of the model. Therefore, it can be obtained that the sensitivity of n input parameters can be obtained by random sampling once, so the calculation efficiency is very high.

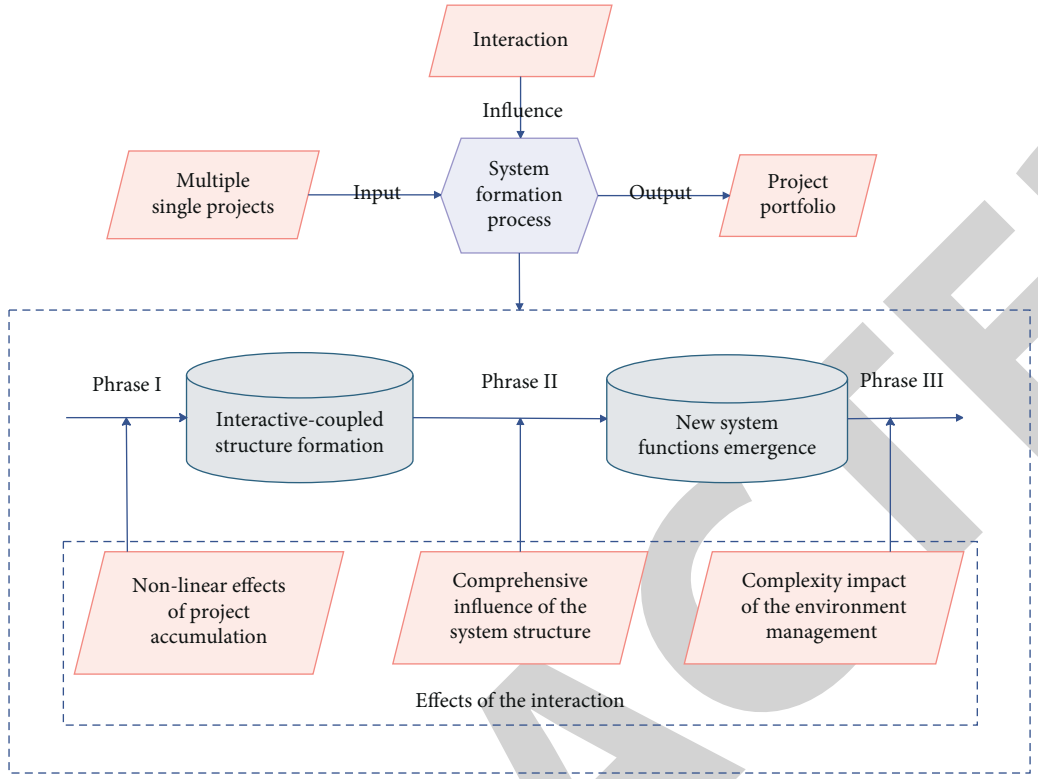


Figure 5: The formation process of the project portfolio system.

The Morris method can be used to calculate the average value and standard deviation. The average value represents the sensitivity of the input parameter, and the order of sensitivity is determined by sorting from large to small. The standard deviation can represent the degree of coupling between input parameters. A small standard deviation means that the degree of coupling between the input parameter and other input parameters is small. Conversely, if the standard deviation is large, it means that the degree of coupling between the input parameter and other input parameters is large.

4. Risk Assessment of Overseas Infrastructure Projects Integrating BP-ANN Algorithm

The objective function model of this paper is as follows.

4.1. Establish a Risk Hierarchy Index Structure.

(1) Target layer

(2) Criterion layer

(3) Subcriteria layer

4.2. Construct the Judgment Matrix. Construct the judgment matrix according to the risk hierarchy and assign values.

$$A = \begin{bmatrix} A_{11} & \cdots & A_{1n} \\ \cdots & \cdots & \cdots \\ A_{n1} & \cdots & A_{nn} \end{bmatrix}. \tag{16}$$

A is represented as a judgment matrix.

4.3. Calculate the Eigenvectors of the Matrix and Calculate the Index Weights. (1) Sum the columns of the matrix

(2) Normalize each column

$$B_{ij} = \frac{A_{ij}}{\sum A_{ij}}. \tag{17}$$

The value of $\sum A_{ij}$ is the sum of the values in the columns. Use the above formula to obtain a new matrix B.

(3) Sum each row and calculate the feature vector.

(4) Normalize the feature vector to get the index weight

4.4. Consistency Test. (1) Calculate the largest eigenroot.

$$\lambda_{\max} = \frac{\sum (\mathrm{AW})i}{\sum nWi}. \tag{18}$$

A is multiplied by w, which means that the two matrices are multiplied, and the result is a column vector, and then each element in the column vector is divided by the product of the order and the corresponding weight.

(2) Judge the consistency index of the matrix.

$$\mathrm{CI} = \frac{\lambda_{\max - n}}{n - 1}. \tag{19}$$

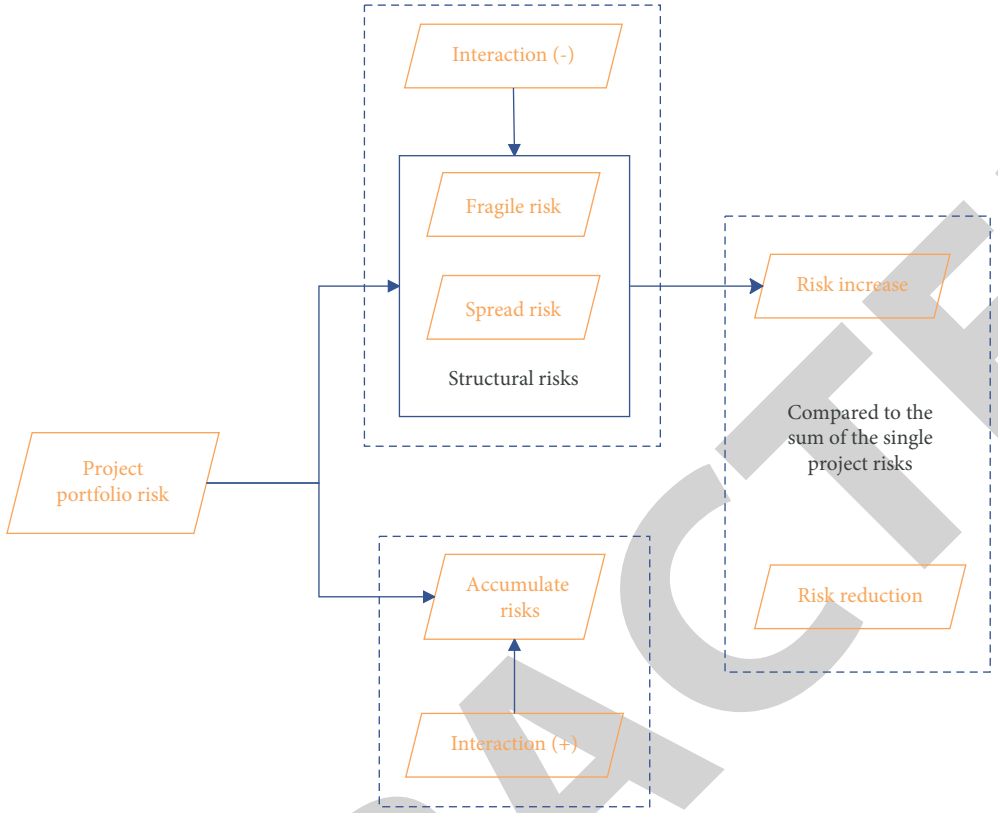


Figure 6: The risk composition of the project portfolio from the perspective of interaction effects.

(3) Obtain the consistency ratio.

$$CR = \frac{CI}{RI}. \quad (20)$$

RI is the standard value of matrix order, when CR < 0.1, the inconsistency of A is acceptable.

In this study, in order to construct information about the whole process of recording engineering project risk from generation to result, the related concepts of risk are redefined on the basis of previous research, To set the model hyper-parameters of ANN, using the cross-validation method, setting the target function, and taking the strategy for avoiding overfitting, and an information table is set up to record basic project information and risk-related information. The risk assessment model of overseas infrastructure projects that incorporates the BP-ANN algorithm can be represented in Figure 3.

In this study, a variety of classification algorithms are used to compare with each other to construct the classification model. Although the types of algorithms used are different, the classification models are all based on the same process shown in Figure 4. The implementation process of the text classification algorithm in Rapidminer is similar to the construction process of the above decision tree.

A single project is the constituent element of the project portfolio, and the accumulation of elements is the first step in the formation of the project portfolio system. The process of project accumulation is not carried out independently, and it will be affected by the nonlinear effects of different scales of interaction effects. The accumulated project group has an interactively coupled system structure, and the comprehensive effects of various associations on the system structure give the project portfolio new functions and behavior characteristics. This is the second step in the formation of the system. The function and behavior of the project portfolio are affected by the management process and the activities of the managers. Various management decisions, regulations, and implementation plans will affect the operation of the project portfolio system, which constitutes the third step of the formation of the system. The process of project portfolio system formation is shown in Figure 5.

The negative effect of the interaction effect on the project portfolio risk refers to the fact that under the influence of the interaction effect, the project portfolio has new risks that a single project does not have, which makes the overall risk of the project portfolio increase. Project portfolio is a complex system that is different from a single project. It has system functions and behavioral characteristics that a single project does not have. When new functions emerge, it also brings new risks. Based on the evolution process of project portfolio risk, the comprehensive impact of interaction effects on the system structure and the complexity of the management environment are the sources of its negative effects. Based on the different utility of interaction effects on project portfolio risk, the composition of project portfolio risk is shown in Figure 6.

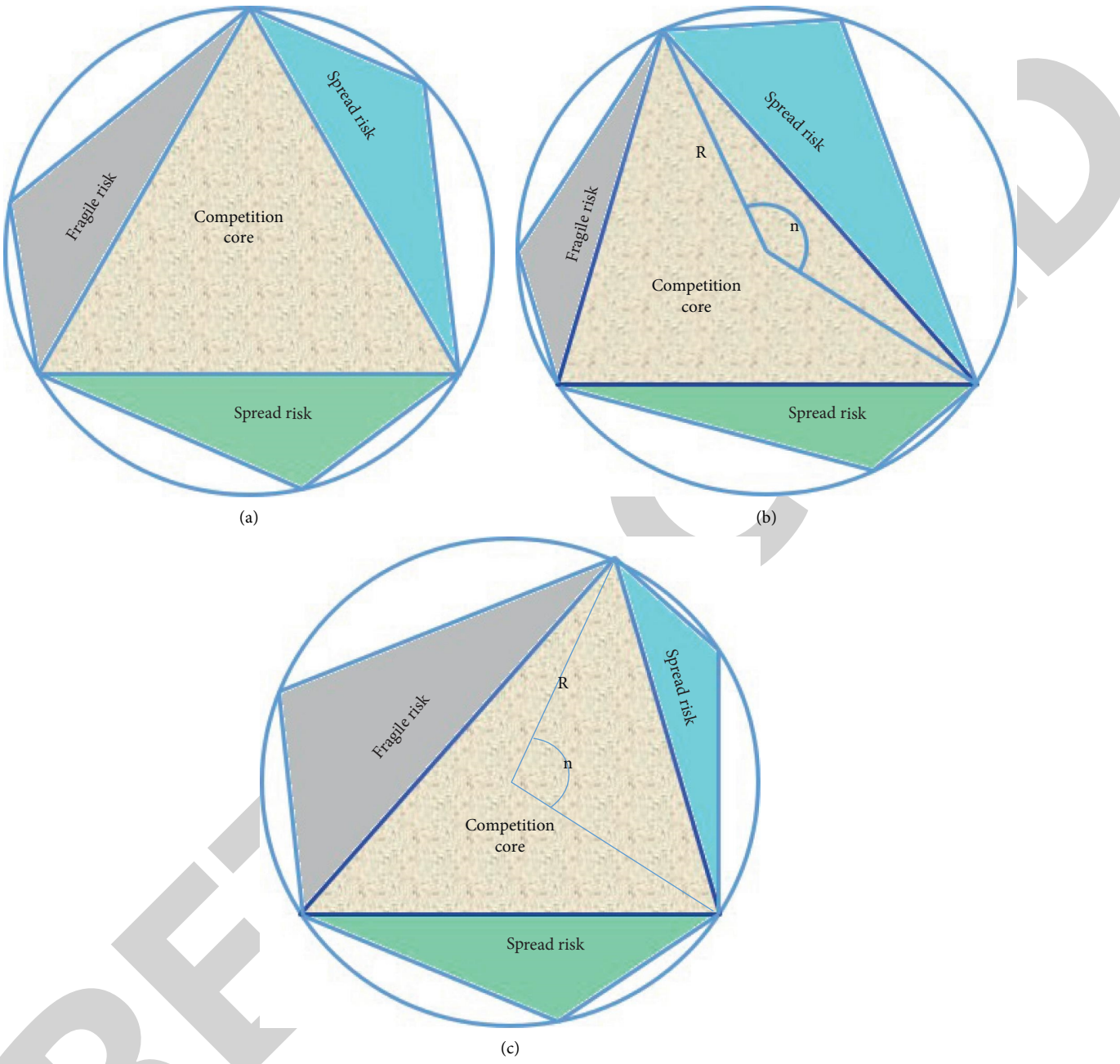


Figure 7: Competitiveness measurement architecture. (a) Competitive strength structure of project portfolio risk. (b) Progressive. (c) Conserve.

Construct a comprehensive measurement framework for project portfolio risk as shown in Figure 7, which is called the competence measurement framework. Competitiveness refers to the power comparison of the risk formed by the different effects of the interaction effect on the overall risk. The competitiveness measurement framework of project portfolio risk comprehensively reflects the competitive situation of the two forces of risk diversification and the addition of new risks. By comparing the magnitude of the two forces, the overall trend of project portfolio risk can be determined.

In Figure 7(a), the triangle at the core of the competition divides the circumcircle into three modules. There is an inscribed triangle for each module, and the area of this triangle represents the utility strength of the corresponding measurement content on the risk of the project portfolio. The core of competition in Figure 7(c) is an equilateral triangle, which divides the three modules equally. However, managers with different attitudes towards risk make the prerequisites for diversifying risks and emerging risks to be different, which leads to the competition results under different split ratios as shown in Figures 7(b) and 7(c). At

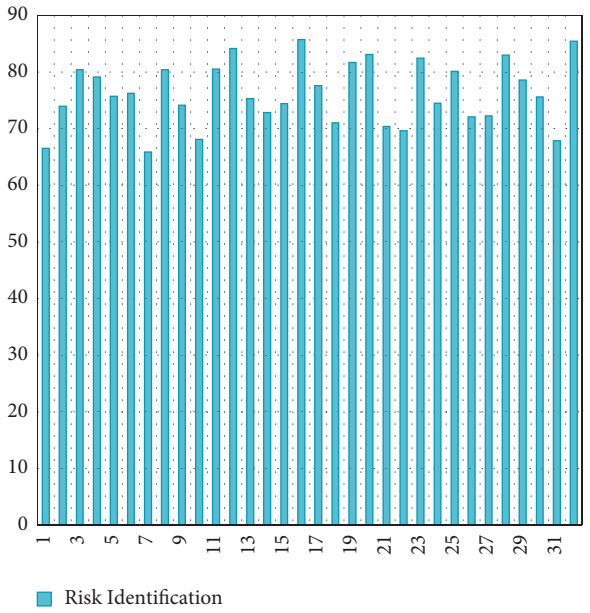


Figure 8: Statistical diagram of risk factor identification data.

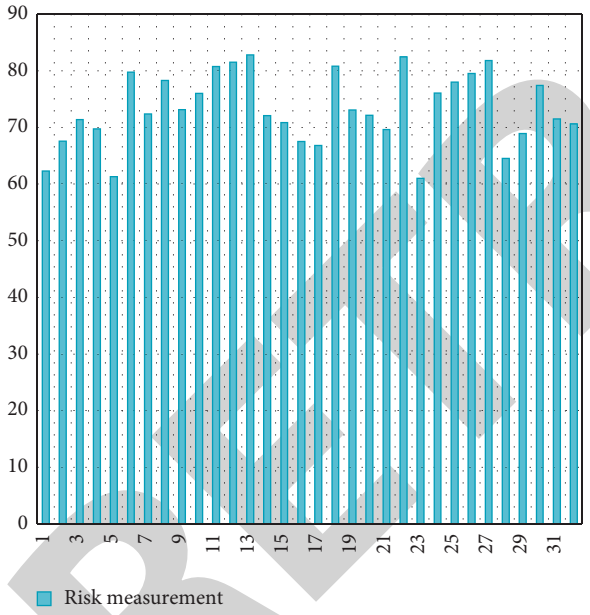


Figure 9: Statistical diagram of risk measurement data.

this time, the core of competitiveness becomes an irregular triangle under the subjective influence of risk.

From the above, the risks of overseas infrastructure projects can be evaluated. Therefore, this paper uses experimental research to verify the effect of the risk assessment model of overseas infrastructure projects that integrates the BP-ANN algorithm. This article collects existing overseas infrastructure project cases through the Internet as a sample, and the risk factors and risk measurement have actual data. On this basis, the system model of this article is used to identify the risk factors and analyze the risk measurement in these cases, and the statistical accuracy rate is used to verify the effectiveness of the algorithm in this article. The statistical risk factor identification and risk measurement effect evaluation are shown in Tables 1 and 2, Figures 8 and 9, respectively.

Table 1: The risk factor identification effect of the risk assessment model of overseas infrastructure projects that integrates the BP-ANN algorithm.

Sample number	Risk identification	Sample number	Risk identification
1	66.50	17	77.59
2	73.97	18	71.01
3	80.40	19	81.71
4	79.12	20	83.08
5	75.70	21	70.36
6	76.21	22	69.60
7	65.84	23	82.43
8	80.37	24	74.46
9	74.10	25	80.11
10	68.10	26	72.06
11	80.50	27	72.24
12	84.12	28	82.96
13	75.31	29	78.57
14	72.81	30	75.57
15	74.43	31	67.84
16	85.71	32	85.42

Table 2: The analysis effect of risk measurement of the risk assessment model of overseas infrastructure projects that integrates the BP-ANN algorithm.

Sample number	Risk measurement	Sample number	Risk measurement
1	62.28	17	66.84
2	67.59	18	80.83
3	71.37	19	73.06
4	69.72	20	72.12
5	61.33	21	69.62
6	79.76	22	82.45
7	72.38	23	61.02
8	78.28	24	76.06
9	73.12	25	78.03
10	75.99	26	79.52
11	80.75	27	81.80
12	81.50	28	64.52
13	82.78	29	68.90
14	72.06	30	77.43
15	70.84	31	71.48
16	67.50	32	70.59

The method in this paper is compared with the literature [17], mainly to verify the effect of project risk assessment, and the results are shown in Table 3.

From the above research, it can be seen that the risk assessment model of overseas infrastructure projects that integrate the BP-ANN algorithm proposed in this article has a good risk analysis effect and has a certain effect on improving the risk assessment of overseas infrastructure projects.

Table 3: Comparison of project risk assessment effects.

Number	The method of this paper	The method in [17]	Number	The method of this paper	The method in [17]
1	81.13	75.14	17	83.58	76.41
2	84.86	80.08	18	85.31	80.40
3	84.16	77.11	19	87.82	78.75
4	85.42	74.98	20	82.26	72.71
5	84.36	79.41	21	82.99	76.51
6	81.91	75.14	22	82.52	75.12
7	83.19	74.27	23	86.83	82.12
8	83.21	77.05	24	86.00	75.17
9	83.73	75.06	25	88.49	80.32
10	81.46	71.04	26	85.12	74.08
11	83.33	76.70	27	81.84	74.65
12	86.15	75.42	28	88.21	80.90
13	82.36	72.13	29	82.50	75.50
14	85.50	74.59	30	83.09	76.25
15	88.61	79.33	31	88.51	81.68
16	81.36	74.23	32	87.48	78.14

5. Conclusion

Compared with the general projects, overseas infrastructure construction projects have the characteristics of political relevance, non-profitability, public use, government agency, and huge fixed cost precipitation. In addition, financial risks, income risks, operational risks, and systematic risk management arising from the characteristics of large investment scale, high financing leverage, and long construction and investment cycles are the keys to the success of overseas infrastructure projects. In order to explore the effect of risk assessment of overseas infrastructure projects, this paper constructs the BP-ANN algorithm, and builds a project risk assessment system through fusion algorithms to improve the effect of risk assessment of overseas infrastructure projects. The research shows that the risk assessment model of overseas infrastructure projects integrating the BP-ANN algorithm proposed in this article has a good risk analysis effect and has a certain effect on improving the risk assessment of overseas infrastructure projects.

Data Availability

The labeled dataset used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare no conflicts of interest.

Acknowledgments

This study was sponsored by Anhui Provincial Quality Project Applications in the Year 2020 (2020mooc148).

References

[1] X. Guo and N. Capucu, "Examining stakeholder participation in social stability risk assessment for mega projects using network analysis," *International Journal of Disaster Risk Management*, vol. 1, no. 1, pp. 1–31, 2019.

[2] R. F. A. Eskander, "Risk assessment influencing factors for Arabian construction projects using analytic hierarchy process," *Alexandria Engineering Journal*, vol. 57, no. 4, pp. 4207–4218, 2018.

[3] T. K. Biswas and K. Zaman, "A fuzzy-based risk assessment methodology for construction projects under epistemic uncertainty," *International Journal of Fuzzy Systems*, vol. 21, no. 4, pp. 1221–1240, 2019.

[4] O. V. Efimova and D. A. Koroleva, "Development of a financial analysis tool: risk assessment in the process of studying the investment projects efficiency," Чуманитарни Балкански изследвания, vol. 3, no. 4, pp. 57–61, 2019.

[5] A. Nesticò, G. De Mare, and G. Maselli, "An economic model of risk assessment for water projects," *Water Supply*, vol. 20, no. 6, pp. 2054–2068, 2020.

[6] B. Shi, J. Jiang, R. Liu, A. U. Khan, and P. Wang, "Engineering risk assessment for emergency disposal projects of sudden water pollution incidents," *Environmental Science and Pollution Research*, vol. 24, no. 17, pp. 14819–14833, 2017.

[7] R. Ketabchi and M. R. Ghaeli, "An application of fuzzy BWM for risk assessment in offshore oil projects," *Journal of Project Management*, vol. 4, no. 3, pp. 233–240, 2019.

[8] Y. Li and X. Wang, "Risk assessment for public–private partnership projects: using a fuzzy analytic hierarchical process method and expert opinion in China," *Journal of Risk Research*, vol. 21, no. 8, pp. 952–973, 2018.

[9] M. Liu, J. Yang, and G. Guan, "Frazil jam risk assessment for water diversion projects," *Water Supply*, vol. 20, no. 2, pp. 428–439, 2020.

[10] A. Shaktawat and S. Vadhera, "Risk management of hydropower projects for sustainable development: a review," *Environment, Development and Sustainability*, vol. 23, no. 1, pp. 45–76, 2021.

[11] K. U. Birant, A. H. Işık, M. Batar, H. Bora, and A. Burak, "Risk assessment and management method for distributed software development projects with fuzzy approach," *International Journal of Computer Systems Science and Engineering*, vol. 8, no. 6, pp. 133–139, 2019.

[12] A. Valipour, N. Yahaya, N. Md Noor, J. Antucheviciene, and J. Tamosaitiene, "Hybrid SWARA-COPRAS method for risk assessment in deep foundation excavation project: an iranian case study," *Journal of Civil Engineering and Management*, vol. 23, no. 4, pp. 524–532, 2017.

Hindawi
Security and Communication Networks
Volume 2024, Article ID 9826419, 1 page
https://doi.org/10.1155/2024/9826419

Retraction

Retracted: Application of User Experience Gene Extraction Model Based on Industrial Design

Security and Communication Networks

Received 8 January 2024; Accepted 8 January 2024; Published 9 January 2024

This article has been retracted by Hindawi following an investigation undertaken by the publisher [1]. This investigation has uncovered evidence of one or more of the following indicators of systematic manipulation of the publication process:

(1) Discrepancies in scope

(2) Discrepancies in the description of the research reported

(3) Discrepancies between the availability of data and the research described

(4) Inappropriate citations

(5) Incoherent, meaningless and/or irrelevant content included in the article

(6) Manipulated or compromised peer review

The presence of these indicators undermines our confidence in the integrity of the article's content and we cannot, therefore, vouch for its reliability. Please note that this notice is intended solely to alert readers that the content of this article is unreliable. We have not investigated whether authors were aware of or involved in the systematic manipulation of the publication process.

Wiley and Hindawi regrets that the usual quality checks did not identify these issues before publication and have since put additional measures in place to safeguard research integrity.

We wish to credit our own Research Integrity and Research Publishing teams and anonymous and named external researchers and research integrity experts for contributing to this investigation.

The corresponding author, as the representative of all authors, has been given the opportunity to register their agreement or disagreement to this retraction. We have kept a record of any response received.

References

[1] Z. Yu, "Application of User Experience Gene Extraction Model Based on Industrial Design," *Security and Communication Networks*, vol. 2022, Article ID 7366480, 14 pages, 2022.

Hindawi
Security and Communication Networks
Volume 2022, Article ID 7366480, 14 pages
https://doi.org/10.1155/2022/7366480

Research Article

Application of User Experience Gene Extraction Model Based on Industrial Design

Ziwei Yu

College of Humanities and Arts, Hunan International Economics University, Changsha 410205, China

Correspondence should be addressed to Ziwei Yu; dghl@jou.edu.cn

Received 20 May 2022; Revised 8 June 2022; Accepted 23 June 2022; Published 4 August 2022

Academic Editor: Fang Liu

Product design DNA is a new concept produced by applying the idea of genetic engineering to the field of industrial design, involving multiple knowledge fields, aiming to give products a unique shape and style image to build a brand. This paper systematically summarizes the current situation and progress of product design DNA research at home and abroad, focusing on the expression structure, application research progress, and research on key technologies. The law of DNA generation and derivation; explore the user's cognitive mechanism for product design DNA; realize the connection between product design DNA reasoning and production. The designed user experience gene extraction based on industrial design provides new ideas for product design and has strong guiding significance.

1. Introduction

China is becoming a global manufacturing base but "made in China" should not be synonymous with "imitation." China is striving to "create in China," and rapid product innovation and brand building will become the focus of Chinese enterprises in the next step. With the homogenization of technology, products no longer only meet the functional requirements [1]. How to give products a special form and style image to shape a unique brand has become one of the important works of product development. In those famous enterprises, the style of products always maintains a certain inheritance in continuous innovation such as Mercedes Benz, BMW, and Nokia. No matter how many generations of their products are updated, people can always identify them from the products of many brands. However, because product design is full of fuzziness and uncertainty, designers usually map the design intention to the new design with their own experience, intuition, and inspiration. Due to the lack of rational support, it is difficult to form a set of practical style-oriented product design methods. Industrial design is not equal to appearance design. It contains more internal factors including culture and brand, which not only maintains the continuity of product design style but also has innovation. In product innovation design, an important means is to adopt the gene design method for user experience to realize the serialization of products facing different needs or products with greater deformation ability [2].

Today's economic forms are diverse, with the emergence of new terms such as "leisure economy," "tourism economy," "silver hair economy," and "fitness economy," as well as the topic of "experience economy." With the emergence of the "experience economy," as the basis of providing economy, the attributes of products also change with the change of economic form. Product design is the product of the industrial revolution. It is the internal reflection of the times, economy, technology, and culture. The development of the "experience economy" drives the development of "experience design."

However, when it comes to the "user experience" of products, most of us only stay on the interactive interface, and even narrow it down to the "screen." We think "experience" should only be the category of interaction design, and the software is appropriate. We should know that a good product is not only based on interactive software development and design but also includes a hardware system covering many factors such as color, material, size, design psychology, and so on. Not only at home, but also abroad,

few people mention the concept of software and hardware of product design and the systematic research of such design at the same time.

DNA stores the information of parents and guides the development and functional operation of organisms through instructions. In nature, the previous generation of organisms copied their DNA into their offspring to realize inheritance, so that their traits can be maintained; at the same time, DNA will also change, and the traits of offspring will change accordingly. Due to the continuous progress and development of science and technology, various disciplines intersect and learn from each other, and there is a trend of high integration among interdisciplinary disciplines. In this context, relevant researchers have also applied the idea of gene and genetic engineering to the field of industrial design, and a new concept of "product design DNA" has emerged. Its main focus is on how to endow products with unique form and style images, so as to shape the brand under the trend of increasing homogenization of technology among manufacturers. After hundreds of years of development, the product styles of famous foreign enterprises always maintain a certain degree of inheritance and continuous innovation. Therefore, consumers can always identify them from many brand products [3].

2. State of the Art

The source of "user experience design" is the "user and man-machine interface experience." In the early design process, the development of the man-machine interface is independent of the development of the functional core and often starts at the end of the whole development process. The result is that the products developed lack "user experience" data, resulting in risky failure and almost difficult to obtain satisfactory results. Therefore, someone proposed to implement "user experience" in interface design. "Product user interface experience," as an important bridge between users and products, has not received corresponding attention. Design is often lost in "modeling" and "style," and forgets to deeply study the deep meaning between "user" and "product." "As far as consumers are concerned, the interface is a product." Paying attention to the user experience can achieve satisfactory results.

When consumers buy products, they are no longer limited to the investigation of product functions, but also gradually pay attention to whether the products can meet their own spiritual needs, as the first element of transmitting product information, product form is particularly important in the process of industrial design because product form not only affects the use function of products but also reflects the spiritual connotation of science and culture that designers want to convey. Today, with the serious homogenization of product form and its modeling technology, innovative research on product form design technology has become an important field of industrial design research. At present, the research on product form design technology at home and abroad mainly includes product gene, QFD and TRIZ, combinatorial innovation principle, fuzzy theory, grey theory, and so on. However, with the continuous cross integration of biology and industrial design, the research on product genes has become a frontier and hot topic in industrial design. Feng et al. also put forward the insufficient research on the key characteristics of gene transcription technology and the use of gene transcription technology [4]. Chen and Luo proposed that product design must extract the explicit and implicit features of product family DNA from many aspects such as syntax and semantics [5]. Lu et al. proposed the DNA reasoning method of product design based on shape grammar [6]. Yan et al. proposed the coding technology of using the set of morphological parameters as the target problem coding [7]. Gero and Kazakov studied genetic engineering and applied it to genetic algorithm genetic engineering [8]. These scholars have studied the product gene and related technology from different fields to a large extent, reflecting the related technology of product gene, and have good scientific and advanced nature.

However, in the current product design, the DNA extraction of user experience is not mature enough. This paper proposes a user gene extraction algorithm based on industrial design. By using gene extraction for users of product functions and product appearance, it provides the design of industrial products reference guidance. The overall process is shown in Figure 1 [9].

Based on the in-depth study of product genetic characteristics and morphological gene theory, the product form gene hybridization technology aims to provide new technologies for product form design and improve product form through the extraction and coding of product form genes and the study of gene hybridization algorithms, design efficiency, and design quality.

3. Methodology

3.1. Definition of Product Design DNA. Design is a creative process, and this does not mean that new products or components must appear, but should be created on the basis of existing knowledge in an effective way, and the existing design elements should be reintegrated and developed under given constraints. Most of the previous design knowledge is fragmented and scattered in various fields, and the expression method of design knowledge is mainly to classify these fragments, which often leads to the segmentation of design knowledge, isolation, limitation in their respective scope, and lack of coherence and organic connection. The concept of product design DNA appears to solve these problems.

The so-called product design, DNA refers to introducing the concepts of DNA similarity and inheritance into the internal genetic and variation characteristics of product design. In the process of product development and design, all new products are related to previous products but not exactly the same. At present, there is no standard definition of product design DNA. According to relevant materials, it can be summarized that product design DNA should have the following characteristics: (1) Just as biological DNA determines and controls the growth and development sequence and process of organisms, product design DNA should also determine the cycle, process and stage of product

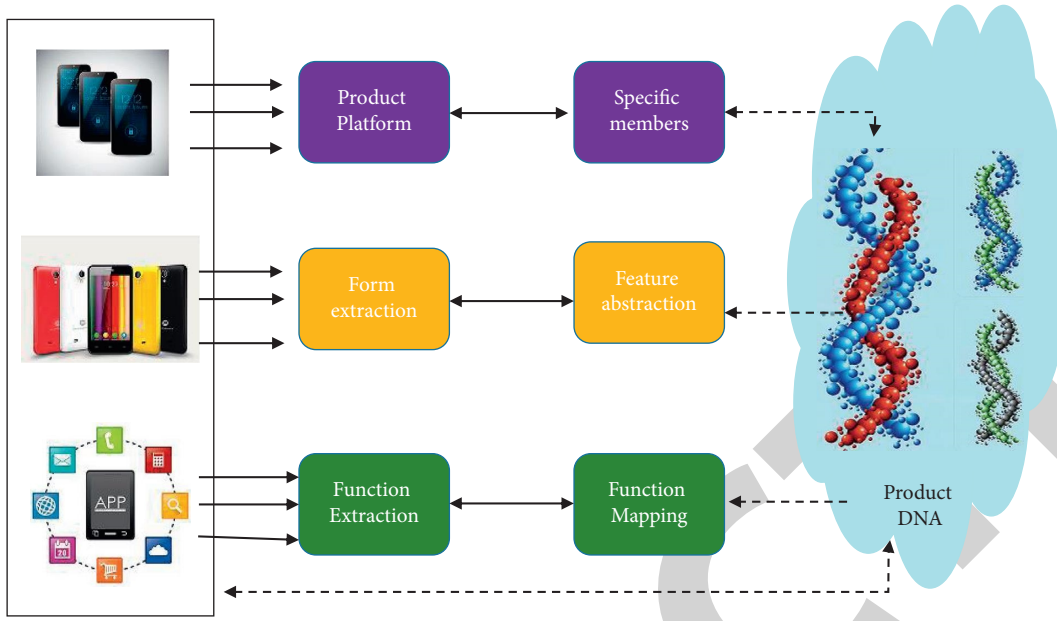


Figure 1: The user experience gene extraction based on industrial design.

design to a great extent; (2) Product design DNA should be confirmed by practice, product design information with genetic value, that is, it has the significance and value of inheritance and reference for other product design; (3) Product design DNA should be standardized product information to facilitate the management and use of product information; (4) Product design DNA is based on coding oriented and function-oriented knowledge. It can produce new product forms that meet the requirements under given constraints [10].

Product gene is the application of genetic engineering in product design. This concept was first proposed by Gero and Kazakov [8]. Feng et al. [4] and Chen and Luo [5] of Zhejiang University were the earliest researchers in China to understand product design with the concept of the gene. The early research on product genes mostly focused on the field of mechanical design, but recently it gradually shifted to the field of industrial design and increased the attention to perceptual images [11]. There are many types of research on product optimization in the evolutionary algorithms, which focus on optimization efficiency and quality, and do not pay special attention to the product design problem itself.

In a specific application, product design DNA has the following characteristics: (1) Flexible knowledge structure. Since the external conditions often change in the actual situation, the design knowledge should be able to be flexibly transformed and effectively responded to; (2) With the rapid and rapid application, product design DNA can be divided into two design knowledge domains (discussed in detail below), including several basic knowledge units such as morphological features, expert knowledge, organization and management, creativity, working principle, patented technology, operating mechanism, and value utility, these knowledge units ensure the rapid application of design knowledge under constraints; (3) Easy to read. Product design DNA can be expressed by unitary structure and graphic way, which is easy to read by users and design software [11].

3.2. Knowledge Structure of Product Design DNA. Turbon and Aronson proposed that knowledge can be divided into implicit knowledge and explicit knowledge, which are closely related to each other. According to this theory, the design knowledge in the system of product design DNA is divided into two parts: morphological knowledge domain and functional knowledge domain. There is a mapping relationship between the two domains, as shown in Figure 2.

As can be seen from Figure 2, the morphological knowledge domain includes invisible knowledge and other knowledge concepts, which are composed of morphological features, expert knowledge, organization and management, creativity, etc. Expert knowledge is an important criterion for evaluating design, which corresponds to the working principle and patent in the field of functional knowledge; organizational management represents the knowledge structure and the connection of various knowledge units, which corresponds to the operation mechanism in the functional knowledge domain; creativity refers to the creative thinking in product design, which is related to working principle, patented technology, operation mechanism, and value utility. The functional knowledge domain includes explicit knowledge such as working principles, patent technology, operation mechanism, and value utility. They also form a mapping relationship with each knowledge unit in the morphological knowledge domain. Given constraints will ultimately determine the specific mapping relationship [12].

Taking the mobile phone as an example, according to the product design DNA knowledge construction method proposed above, the knowledge structure of mobile phone design DNA is established as follows, as shown in Figure 3.

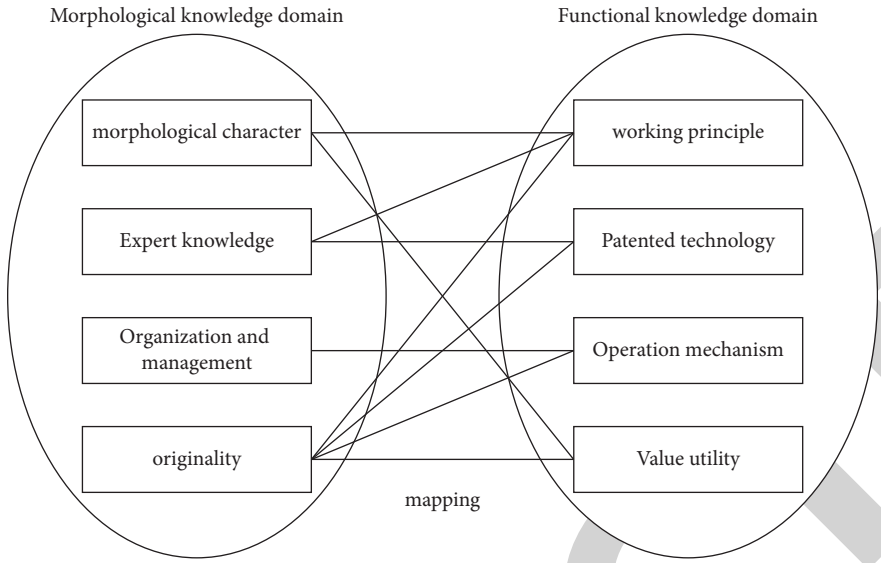


Figure 2: The two knowledge domains and their mapping relationship.

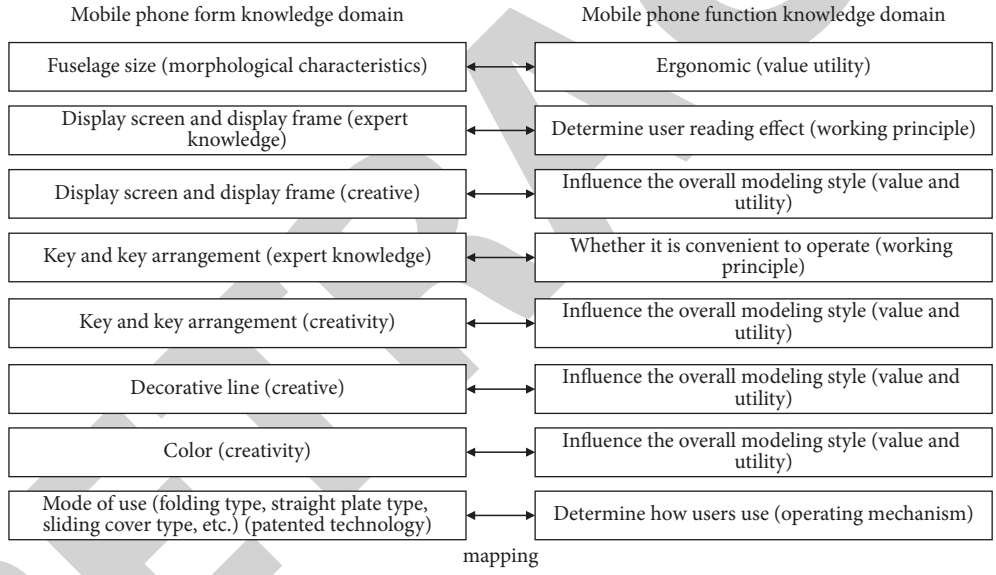


Figure 3: The knowledge structure of DNA design of the mobile phone.

3.3. Analogy between Product Design DNA and Biological DNA. Referring to the molecular model structure of biological DNA, try to establish the structural model of product design DNA. Take the mobile phone as an example, as shown in Figure 3. The product design DNA in the figure has a linear double helix structure, which consists of two "chains"—morphological knowledge domain and functional knowledge domain—and their mapping relationship, as shown in Figure 4.

When the new product design starts, the two chains of product design DNA will be spun and transcribed under the design constraints (such as cost, cycle, market division, and consumer preference) and become two knowledge systems leading the design, and product design mRNA and product design tRNA. This is just as if the DNA of an organism is transcribed into mRNA and tRNA under the action of a biological enzyme (enzm and ENA T are the enzymes in biology, and DNA is transcribed under their binding action). In biology, mRNA, that is, messenger RNA, carries genetic information and serves as a template in protein synthesis; tRNA is the transport RNA (transfer RN a), which transports the activated amino acids to the ribosome by matching itself and the mRNA template to synthesize protein. In contrast, product design mRNA refers to the knowledge space structure with mapping relation formed by rearrangement and combination of each knowledge unit in product design DNA, while product design tRNA determines the organizational relationship of each knowledge unit according to external constraints. Furthermore, product design mRNA is converted into coding, which contains the feature information of product parts; tRNA is transformed into anti coding, which can make the components form the whole

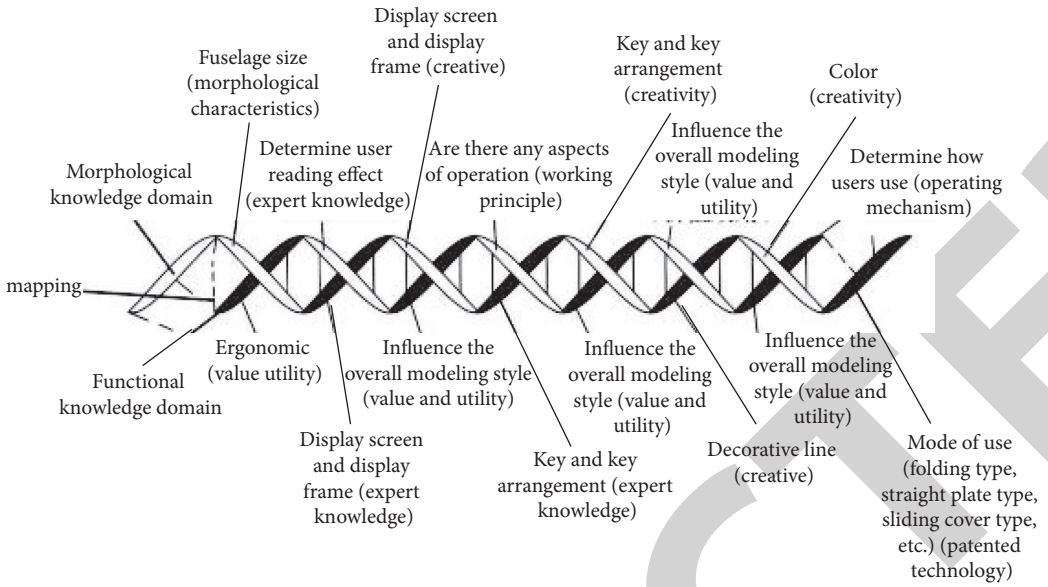


Figure 4: The structural model of mobile phone design DNA.

product characteristics under the constraints by transmitting the relationship information between the components. Heebyun gives an analogy between product design DNA and biological DNA, as shown in Figure 4.

3.4. Product Design DNA and Product Family Design DNA. In recent years, the concept of "product family design DNA" has been put forward by scholars of Zhejiang University. A product family is a group of related products based on a product platform and by adding different personality modules to meet the personalized needs of different customers. mey Er,A product platform is the foundation of a product family, and it is a reusable module set that can be shared by a series of products. Generally, it has a relatively stable structure. An effective product platform is the core of the product family and the foundation of related series products within the product family. It has the common characteristics of all products within the product family, product family design is the core content of mass customization. The similarity between DNA family and product design is studied and put forward [13]

Through comparative analysis and research, it is considered that the connotation of the two concepts of "product family design DNA" and "product design DNA" are very close. The reason is that the core of the product family is a basic product platform, so the product family is a general designation of products with a large number of the same or similar characteristics, which means that the product members in the product family are changing, but they enjoy many common characteristics, so that the products of the enterprise have common identification elements. Then, the product family design DNA can also be considered as the product design DNA of the product platform in the product family, as shown in Figure 5.

The first type is the potential relationship between similar elements in the two sub-networks of "design parameter network" and "image target network." According to the types of node parameters, there are two methods for discovering this kind of edges: Pearson correlation and Spearman correlation. The value of node parameters is a continuous variable. When the data distribution conforms to the normal distribution, the Pearson correlation between the two groups of parameters is used to calculate its correlation. This is also a common way in the process of building biological gene networks.

The specific calculation method is:

$$r = \frac{\sum (x - \overline{x})(y - \overline{y})}{\sqrt{\sum (x - \overline{x})^2}\sqrt{\sum (y - \overline{y})^2}}. \quad (1)$$

In the above formula, X and y are the values of two design elements, $\overline{x}$, $\overline{y}$ are the mean values of the two. R is the correlation coefficient between the two sets of parameters. The closer R is to 1, the higher the correlation between them. On the contrary, the closer R is to 0, the lower the correlation between them.

When the parameters in the nodes are classified as variables or the distribution does not conform to the normal distribution, and the Pearson correlation method cannot be used, Spearman correlation is generally used to calculate the correlation degree between nodes. The calculation method is as follows:

$$r = 1 - \frac{6 \sum d_t^2}{n\left(n^2 - 1\right)}, \quad (2)$$

where: n is the number of genes; Du is the order difference between two genes.

No matter that calculation method is used, a correlation value r can be obtained. Set a correlation threshold $[R]$ for it.

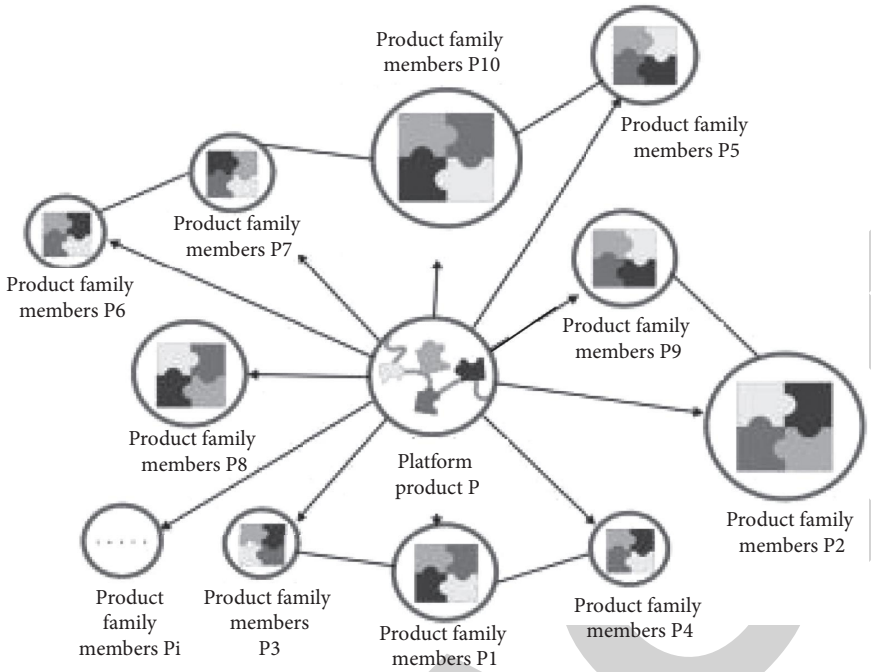


Figure 5: The product family member structure relationship.

When the correlation coefficient r exceeds this threshold, it is considered that the two nodes are associated, and a connection can be established between the two nodes.

In order to find all the edges in the sub-network of the product modeling gene network, the correlation between all nodes in the network needs to be calculated by formula. Finally, the gene network model of product modeling is established [14].

The second type is the mapping relationship between two different nodes, namely, the "design parameter subnet" and "image target subnet." This kind of edge connection can be obtained by comparing the design parameter characteristics of the vehicle models classified by each image target in the process of constructing the image target subnet with the "indirect method."

3.5. Product Gene Network Feature Recognition. Through the identification of the shape and characteristics of the product gene network, we can get the macro knowledge that can directly assist the designer in the design process. It is mainly divided into two parts:

① In the product gene network model, there are two main values associated with nodes for the identification of node characteristics:

One is the number of connections between the node and other nodes, that is, the degree of this node. It can be determined by equation (3)

The threshold R is obtained by statistics. This value represents the centrality of the node.

The second is the node variance, which is calculated as follows:

$$V = \frac{1}{m-1}\sum_{i=1}^{m}\left(x_i - \overline{x}\right)^2. \tag{3}$$

In the formula, all samples are divided into m equally large intervals according to the value definition field of this parameter. X is the number of samples at the i-th level in the parameter arrangement among all samples, and X is the average value of the number of samples at all levels of this parameter.

The above formula expresses whether the parameter distribution probability density curve of this node has a tendency, that is, the influence of the change of this node parameter on the overall evaluation can be simply described as the sensitivity of the node.

Through the calculation and statistics of "centrality" and "sensitivity" of nodes in the network, they can be divided into four categories, as seen in Table 1.

Key node parameters are related to many other nodes. At the same time, they are worthy of change and have a great impact on the product itself, which requires special attention. Although independent nodes have a great impact on products, they are not strongly related to other nodes and can be considered independently. The value of passive nodes has little impact on the overall product, but it is affected by many other nodes based on its high psychological characteristics. The value of secondary nodes is not obviously related to other nodes, and the change of value has little impact on the overall evaluation of products, so such nodes can be appropriately ignored.

Table 1: The classification of nodes in product GRN.

Node type	Centrality	Sensitivity
Key node	High	High
Independent node	Low	High
Passive node	High	Low
Secondary node	Low	Low

② For the identification of node groups, in the product gene network model, it can be observed that several nodes are associated with each other and obviously have edges with each other. It can be seen that these parameters play a common role in the expression of products. In this paper, the correlation threshold method is used to identify the node group. According to the formula, the correlation between nodes in the product gene network is a continuous variable. The setting of the threshold directly affects the presence or absence of the inner edge of the network structure, that is, under different threshold R values, the product gene network will show different density differences according to the connection strength between nodes. By adjusting the correlation threshold, we can gradually and clearly show the division of node groups in gene networks. The identification process and results of these node groups can provide designers with clear reference and auxiliary information: which elements can be considered independently, which elements need to be considered uniformly, and which elements are most firmly related.

3.6. Design Method of Emotional Interaction. Good interactive attention function, excellent interactive attention to emotion. To make the interactive design have an emotional function, it is necessary to make products have an emotional connection with people. In this way, users can have some feelings of pleasure, pleasure, and passion.

When we design a product, we need to use a variety of design elements such as modeling language, color matching, material performance, and so on. If we combine these elements in different ways, people need to invest in different emotions to understand these combinations, so the emotional interaction between the product and people will arise. In essence, interaction design is a design of user behavior. Emotional interaction can affect user behavior from the inside out. This influence is subtle. We often say that to make emotional interaction, we should treat the user as a moody person because this is in line with people's irrational nature. Emotion is something suppressed by reason. To break through reason and make emotional interaction, we need to pay more attention to users.

It must be noted that a certain emotion expressed by emotional products must consider whether it meets the needs of target users. For example, medical products should be compatible and safe, and children's toys should be interesting. It is very important that the personality of emotional products should be consistent with the personality expected by users.

Back to creating emotional interaction, there are basically the following design methods: integrate the elegantaesthetic experience into the product. Everyone has a love of beauty. Beauty can affect people's feelings through people's senses, and even affect people's behavior. A product has external formal beauty that can infect people, which can make users have the impulse to use it when they see it, and this formal beauty does not separate the logical relationship with the product function.

4. Result Analysis and Discussion

The design parameters of the product include all kinds of information in all dimensions such as color, size, and texture. To completely define a product with the parameters of each dimension, the information of each dimension needs to be rewritten to facilitate statistics and analysis, so as to build a network. Therefore, the complete gene network model of product industrial design is very complex. This paper aims to prove the existence of gene networks in complex product modeling and extract relevant knowledge, so only the dimension of shape features is selected. Product modeling gene network has been demonstrated in simple products such as water bottles. In this paper, the automobile is selected as the research carrier of modeling design gene network, because the modeling structure of the automobile is complex, involving a free-form surface and a large amount of modeling information in space. The application of the gene network model in automobile modeling has better universal significance.

4.1. Design Parameter Network of Automobile Modeling

4.1.1. Determination of Automobile Modeling Design Parameters. Automobile modeling is one of the most complex industrial design objects. Its complexity is mainly reflected in: there are many design parameters that need to be assigned in the design process, and there are many perceptual evaluation images as design objectives. Under the influence of these image objectives, there are a lot of implicit relationships between design elements only through the accumulation of long-term work experience can designers grasp these potential relationships perceptually, which leads to the industry characteristics of high entry threshold and long design cycle in the automotive industry design industry. Therefore, how to use CAD technology improves the work efficiency of the automotive design industry has always been a research hotspot. At present, most CAD technologies prefer automation, and intelligence can be grafted into this industry to replace the work of designers. This kind of solution ignores the evaluation goal with absolute certainty, which is different from mechanical products. The evaluation of automobile design results is mostly perceptual image evaluation with complexity and fuzziness. The designer's participation is stripped from the design activities to completely rely on computer technology for a design solution, which inevitably leads to the deviation between the

solution result and the expected value, and the practical value is limited. Therefore, in complex industrial design tasks such as automobile modeling design, it is difficult to completely rely on CAD technology to solve the design object. The designer's decision is still an important guarantee to control the design quality. The combination of CAD technology and designer decision-making is undoubtedly an important means to solve this problem. The specific goal of this chapter is to excavate the potential relationship between the primary and secondary structures and periods in each "design assignment parameter" and "image evaluation target" by building the genetic network model of automobile modeling, and to excavate and output relevant knowledge through the means of information visualization, To assist designers in decision-making.

The automobile design involves many free surfaces, and the number of design parameters to be assigned is huge. But no matter how complex the shape is.

The information transmission of its geometric features has no information hierarchy of points, lines, and faces.

That is, the visual effect of automobile modeling depends on the dimension relationship of each part and the shape of the feature surface.

The size of the local dimension and the shape of the feature surface depend on the shape constraints of feature curves. Automobile modeling example.

The experiment shows that three types of modeling such as area line, form line, and crown line, are proved.

Feature lines have a great influence on the car shape, and these characteristic curves are determined by the coordinates or relative position relations of key points. In other words, automobile modeling can be obtained indirectly by the dimension parameters between the key points. It can be simply considered that the process of automobile design is the process of assigning the position dimension parameters that determine the key points. So these parameters are selected as the design elements of automobile modeling in this chapter.

Based on the above ideas, this paper takes the model of Audi A6 model of 2006 as an example to extract the design elements.

Firstly, the rough a-plane features of the vehicle body are obtained by three-dimensional modeling. A total of 23 basic modeling feature curves are involved during the construction, as shown in Table 2. The shape and spatial position of these 23 modeling feature curves are determined by the spatial position relationship of 106 key points. For the whole process of automobile design, these parameters are only a small part of the design elements to be assigned in the process of design and do not contain all the modeling details. But these parameters constrain the most important body features the body and have a decisive influence on the overall style of the body shape. For the construction of the product modeling gene network, these data contain the position information of key points in the projection surface of the vehicle body modeling, which has enough complexity. This chapter will take 106 parameters as nodes to construct the network of vehicle design parameters, as seen in Table 2.

Table 2: The names of key styling lines for automobiles.

Line number	Line name
1, 2, 3	Side view top profile
4, 5	Side window boundary line
7	Wheel housing boundary line
8	Waistline
9	Front ceiling lamp line
10	Lower edge of front window
11	Lower edge of front window
12	Rear window side line
13	Side line of top wall
14	Curvature line of wheel housing
15	Hood style line
17	Along the lower A-pillar
18	Along the lower C-pillar
21	Headlamp boundary line
22	Boundary line of air inlet grille
23	Tail lamp boundary line
24	Front bumper side line
25	Rear bumper side line
27	Front lower boundary
36	Side view underbody profile

4.1.2. Design Parameter Network Modeling. After the market selection, the product will produce more appearances under the contemporary aesthetic trend.

Unified evaluation standard. Under this evaluation standard, many parameters in automobile modeling show potential connections, which are reflected in.

The relation and restriction between parameters. The network of automobile design parameters is precisely used to describe the potential correlation among various design parameters.

The model of the vehicle is an important link between the perceptual evaluation image and the design parameters of the vehicle modeling.

It is proposed to extract this connection in the actual existing brand car funds.

In the process of network construction, it is very important to select samples. The quantity and quality of samples are all important to the quality of network construction.

It has a decisive impact. In reality, all kinds of car funds, as the products tested by the market, can be regarded as conforming to the requirements.

In the previous sample of the evaluation criteria for the vehicle models, this study collected more than 300 pictures of each brand. The appearance and design style of products is affected by social, time, and cultural factors. The purpose of building a product modeling gene network is to assist the appearance design of cars in the future, so it is not suitable to choose too old cars. This paper selects cars of various brands since 2000. Considering the accuracy of statistical results, similar models of the same brand are excluded and only one is included. At the same time, the constructed automobile modeling gene network should be the summary and refinement of general vehicle design modeling knowledge in a fixed era. Considering the universality of the results, too-

personalized cars are eliminated. Finally, 146 models of 32 automobile brands were selected as the experimental samples, as seen in Tables 3 and 4.

Through the identification and extraction of relevant design parameters in these parameterized vehicle models, the 146 vehicle models can be obtained.

A total of 106 shape design parameters of this.

When the design element nodes are identified, finding the connections between nodes is the main task of gene network modeling.

The size assignment parameters in automobile modeling are continuous variables, so this paper finds the continuous variables through the Pearson correlation coefficient Connect.

By setting different correlation thresholds, a limited number of important nodes can be presented to designers.

4.1.3. Help of Design Parameter Network to Designers. Modeling design has great perceptual factors, and the role of designers (that is, to determine the value of each design element) is very important at present.

It is still irreplaceable by technical tools. Design elements are the objects directly operated by designers, so their network has a great influence on designers.

The auxiliary function is mainly reflected in alleviating the combination explosion caused by a large number of assignments and improving the efficiency of the designer's manual optimization, Instead of directly calculating the optimal value of a design element.

The basic idea of using a design parameter network to solve a combination explosion is to find out the most "important" from many design elements.

Give priority to nodes, or find closely related node groups for unified processing.

The degree and sensitivity of nodes are common indicators to measure the importance of nodes in the network.

(1) Degree of a node.

The number of nodes connected to other nodes in the complex network is expressed as the number of nodes connected to other nodes.

The number of relationships between them. When the correlation threshold $[R] = 0.2$, the five nodes with the highest degree in the automobile modeling design parameter network, as seen in Table 5.

(2) Node sensitivity.

Node sensitivity refers to the tendency of the distribution law of the value of a design element in the sample, which can be determined through the node.

The variance of the value is calculated. The smaller the variance, the more average the distribution of node values in each value range.

The smaller the tendency is, that is, the change of node value has little impact on the number of samples and is not sensitive. Otherwise, it indicates sensitivity.

Table 3: The sources of model samples.

Number	Brand	Quantity
01	Alfa Romeo	4
02	Audi	10
03	BMW	13
04	Mercedes Benz	7
05	Honda	8
06	Peugeot	3
07	Dachia	1
08	Daewoo	1
17	Lexus	4
18	Renault	3
19	Suzuki	1
20	Mazda	7
21	Martha	2
22	Muscoviti	1
23	Opel	1
24	Pontiac	3

Table 4: The model sample source 2.

Number	Brand	Quantity
09	The masses	8
10	Dalem	1
11	Fiat	2
12	Toyota	8
13	Ford	6
14	Jaguar	5
15	Larda	1
16	Rolls-Royce	2
25	Kia	1
26	Nissan	15
27	Mitsubishi	9
28	Sparus	3
29	Kodak	1
30	Modern	4
31	Chevrolet	2
32	Citroen	9

There is a big gap between the value ranges of various size parameters in automobile modeling, so the discrete coefficient is introduced here.

(Coefficient of variation) the concept eliminates the influence of value difference between parameters. The formula is:

$$C.V = \frac{\sigma}{\mu} \times 100\%, \tag{4}$$

Where C.V is the dispersion coefficient of the parameter value, and O is the standard deviation of the parameter, μ is the mean value of the parameter.

(3) Node group.

In gene networks, some nodes will form relatively independent groups based on close internal interaction, that is, they do not interact with each other.

Table 5: The nodes with the largest degree (relevance threshold $[r] = 0.2$).

Number	Design element node	Degree
1	Car windshield height Y @ Top	65
2	Front windshield width Z@Top	64
3	Distance between the midpoint of the front window and the front of the front window Y@side	61
4	X@top on side line 2	61
5	Front windshield length X@side	61

The isolated sub-network connected with other nodes is called "node group" in this paper. It is beneficial to the identification of node groups.

There is a potential connection in the analysis of genes, which needs to be unified the size of data considered.

When the correlation threshold $[R] < 0.5$, the connections between the nodes of the design parameter network are too complex for the designer to identify valid groups of nodes from them

The designer interview shows that the number of nodes in the node group is controlled at about five.

It is more suitable for comprehensive consideration. Based on this demand, the correlation threshold $[R] = 0.96$ is taken to design the nodes of the parameter network.

Through the modeling of automobile modeling design parameter network and the analysis of node degree, sensitivity and node group.

Analysis, combined with the designer's demand interview and in-depth interpretation, the following macro knowledge can be obtained from the analysis:

(1) Influence of wheel size on design.

"Wheelhouse radius @ side" is the most sensitive node, but at the same time, the centrality is not high, and it is not a central node, indicating that.

"Wheelhouse radius @ side" is an independent node. The wheel size has a great impact on the vehicle shape. But this conclusion is true.

The real reason is that the wheel size has been relatively standardized, the size change is small in any model, and the design space is small, therefore, the conclusion of "high sensitivity" will be obtained. The same high-sensitivity design elements are also reflected in other values.

Fixed size.

(2) Automobile side shape design.

The nodes at the key points of car side modeling have higher degrees, and their degrees are roughly the same.

Part of the shape has a large correlation with other aspects, and the degree of correlation is relatively unified. In terms of sensitivity, the middle and front parts of the car body.

The sensitivity of the rear is relatively high, while the front and rear are more constrained, which limits its morphological extension. For this part.

During design activities, the modeling can be focused on the middle position, and the front end and back end can be combined according to the modeling of the middle.

Assign values to other related nodes. Because the relevant nodes of the side rear end shape are more sensitive than those of the front part.

In the design process, it can be handled in the later detail trimming stage of conceptual design according to the specific situation.

(3) Car roof and window design.

It can be seen from the node degree list that the top three nodes are related to the front windshield shape of the car. And these three.

The sensitivity of each node is not high [15]. That is, the shape of the front windshield is greatly affected by other nodes, but its own variation.

During design activities, the modeling can be focused on the middle position, and the front end and back end can be combined according to the modeling of the middle.

Assign values to other related nodes. Because the relevant nodes of the side rear end shape are more sensitive than those of the front part.

In the design process, it can be handled in the later detail trimming stage of conceptual design according to the specific situation.

(4) Design of automobile item shed and window.

It can be seen from the node degree list that the top three nodes are related to the front windshield shape of the car. And these three.

The sensitivity of each node is not high. That is, the shape of the front windshield is greatly affected by other nodes, but its own variation.

However, it may not affect the design of other parts. The nodes related to the shape of the rear window are all low-degree nodes, and their values are important to the whole.

Little impact. Therefore, post-processing can be set in the design process. Comparing the node group list, you can see that node group 3 and node.

Group 5 is related to the shape of the rear windshield and luggage cover. Explain that in the shape of the top of the car, the front windshield and ceiling are.

There is a close relationship between the dimensions of the luggage compartment and the upper cover of the luggage compartment, which should be considered uniformly.

(5) Automobile hood design.

There are four highly sensitive nodes in the hood modeling nodes, which determine the length and arc path of the hood, respectively.

However, their degree is not large. It can be seen that this part of the shape has a certain degree of design freedom and is different from other parts.

It is not obvious that it can be designed independently, or even considered to be carried out in parallel with the morphological design of other parts [16].

The above analysis of the design parameter network based on automobile product gene provides a reference for designers' design activities, explicit knowledge of definite operability.

4.2. Image Target Network of Automobile Modeling

4.2.1. Determination of Image Goal of Automobile Modeling. The perceptual image of vehicle modeling evaluation is the general summary of automobile appearance in a specific era and culture.

The usual design goal of automobile modeling. Image target is generally expressed as a series of adjectives. Zhao Jianghong through questionnaire survey.

Analysis, positive and negative screening, category filtering, sentence slot judgment, and other statistical methods, summed up 30 groups of commonly used words for vehicle evaluation.

Sink**,** as shown in Table 6, Zhu Yi investigated the shape of the car, and the expert group made a study of Kansei based on perceptual engineering.

This paper optimizes and deletes the above words on the basis of the two taking these 20 pairs of image adjectives as nodes, this paper constructs the image target network of automobile modeling [17]. The main work includes two aspects: constructing an image target network, discussing the implicit relationship between image target and design parameters, and identifying image target network characteristics of collaterals.

4.2.2. Image Target Network Modeling. Due to the subtle differences in model shapes, it is difficult for the general public to clearly classify and evaluate them.

Employees engaged in relevant work for a long time are sensitive to changes and differences in product appearance. In order to increase the image evaluation.

Reliability, 22 designers who have been engaged in design for more than three years were recruited as subjects. The 22 designers were wanted It is required to evaluate 20 pairs of image adjectives for the above 146 models. In order to improve efficiency, the evaluation adopts.

Classification method. The subjects selected the appropriate image adjectives for each vehicle model to mark (up to 3), as far as possible.

Reduce the influence of image, color, angle, and other factors on the overall modeling judgment, and select the same angle and material rendering model, The image evaluation data are combined and counted, and each person matches a vehicle type with a perceptual evaluation adjective.

Take one score and get the score statistics of perceptual image, Table 6. It can be seen from the table that the car models are in two opposite words.

The scores of image targets show a considerable tendency, which indicates that designers recognize the relationship between the appearance and image style of the car.

The reliability of this table is high. The Pearson correlation coefficient between the image evaluation indexes in the table is calculated to obtain the relationship between perceptual images' relevance of the statistics entry is shown in Table 6. The node degree in the image network expresses the relevance between this adjective and other adjectives, but it is not limited to positive phase off, that is, these perceptual evaluation words have definite coincidence (positive correlation) in signifier or signifier when evaluating automobile modeling

or deviation (negative correlation). Theoretically speaking, there should be a strong negative correlation between pairs of adjectives, but in fact this is not entirely true, indicating that there are still some deviations in users' cognition of automobile modeling image, which needs to be further studied.

Nodes with large degrees can be considered to represent a strong user image tendency, so it needs to be tested in the design process.

. Taking a lower correlation threshold can sort the degree of each image node, in which the first four height sections.

The calculation method of node sensitivity is similar to the design parameter network, which expresses the influence of vehicle shape change on the image index.

The intensity of influence, or the feasibility of the image through modeling design. The five most sensitive sections There will also be a mutual influence, restraint, and integration between the image objectives of automobile modeling, which is shown in the image network.

It is now connected to a relatively independent node group. Table 6 shows the image targets when the correlation threshold is 0.47.

Through the identification of the key nodes of the image target network and the analysis of the topology, the following pairs of designs can be separated.

Useful auxiliary knowledge for personnel.

"Gorgeous-dynamic-smooth-gorgeous-high-grade-smooth-rigid" nodes constitute the largest node group in the perceptual image network, in which "smooth" is the most sensitive node and also has a high degree. It shows that the user's cognition of this perceptual evaluation is relatively

Table 6: high-frequency adjectives for car styling.

Thin-thick	Gorgeous-simple	Fluency-intermittent	Strong-soft
Strong-weak	Ordinary-personality	Full-withered	Rough-meticulous
Coordinated-misaligned	Static-dynamic	Upscale- low	Messy-neat
Conservative-open	Rational-perceptual	Rigid-smart	Exquisite-humble
Rough-smooth	Strong-weak	Elegant-showy	Generous-shy

unified, and the image target is closely related to many other targets, so enough attention should be paid to the design activities [18].

As the node with the highest degree, "gorgeous" is related to many image targets, but its sensitivity is low.

It is because designers have different perceptions of the appearance of the car when evaluating it, or it may be that it belongs to a passively affected goal Mark.

The six image targets of "low-grade-simple," "maladjusted–messy," and "strong-tough" form three pairs of relatively close node groups. It is obvious that there is a strong potential relevance in the evaluation of these adjectives, which can be used in the design.

Consider them together.

4.3. Discovery of Association between Design Parameters and Image Targets in Gene Networks. The discovery of the second kind of edge in product gene regulation network, namely, "design parameter image target," is the focus of this paper.

Another important task. The identification of such related information can clearly reflect the mapping relationship between image evaluation and design parameters, provide accurate design suggestions for designers, and transform the inefficient modeling design process into accurate "gene surgery" [19].

The discovery of such edges is obtained by constructing the image target network through "indirect method." The idea is to classify the image target first.

The design parameter network is established for the vehicle type under the condition of; then, through the characteristics of the design parameter network of the vehicle model under the classification of each image target.

Feature analysis establishes the relationship between image objectives and design parameters; finally, by comparing the design parameters associated with each image target. The similarities and differences of node sets further establish the relationship between image targets. The specific operation methods are as follows:

First, image target vehicle classification: according to the results of the evaluation experiment, the vehicle types are classified as image targets.

The reliability of the results is added to make the following provisions for the classification of vehicle models: ① if there are models in the image evaluation of mutual antonyms.

If there are votes, they will be classified as the style of more votes, and if the votes are the same, they will not be classified. ② To solidify the wind.

The first 30 models are selected according to the scores of the vehicles classified under the same perceptual evaluation.

Second, sensitivity calculation of design parameters under style.

Sensitivity is calculated. According to the definition of sensitivity, the sensitivity of the image expresses the influence of this parameter on the evaluation of the image target. In other words, the relationship between the value of nodes with higher sensitivity and the evaluation of the image target.

The closer it is, and vice versa. The sensitivity coefficients of each parameter under image target evaluation are obtained here. Third, the connection between different types of nodes is constructed: the design parameter nodes under the same image target are entered according to the sensitive value.

Row sort set a sensitivity threshold. The edge between the design parameter node and the perceptual evaluation node that exceeds the threshold value is connected [20]. Repeat the above work to complete the construction of the edge among all design parameters and image objectives. It is worth noting to ensure all the edges have similar firmness, and the edge connection should be based on the same evaluation standard, so all sensitivity threshold values need, it is the same. In order to better represent the correlation between design parameters and image targets, the sensitivity threshold q is set to 85%. Finally, the relationship between image targets is established: the design parameter nodes mapped by each image target can be regarded as a section point set writing [21]:

$$I_m = \{P_1, P_2, P_3, \ldots, P_n\}, \tag{5}$$

where: I_m is the set of design parameters under an image target, PI, P2, and PP. Design parameters for each of the sets.

The similarity between sets can be obtained by the method of the Jaccard similarity coefficient The formula is as follows:

$$I(I_m, I_n) = \frac{|I_m \cap I_n|}{|I_m \cup I_n|}, \tag{6}$$

where J (IM, in) is the Jaccard similarity coefficient between the image target set $1m$ and in.

If two nodes have high similarity, the image target corresponding to them is designed similar The effect of the parameters. It can be seen that there is a high potential correlation between the two image targets. The setting of the Jaccard similarity coefficient Threshold, the image target subnet can be obtained by building an edge between the image target nodes that exceed the threshold.

The abovementioned methods can be used to construct the image target network in addition to the construction of the image target network subnet [22].

The connection between nodes of the subnet is established to form a dichotograph network, as shown in Table 7.

Table 7: The image target and design parameter association table.

Image target	Front turning point and front end Y of the hood, style line length X under the front end
Neat	Line Length X
Exquisite	Bonnet forward pivot point and front Y
Shabby	Lateral line 2 and front end height Y
Generous	The distance between the front turning point of the hood and the front end X
Shy	Lateral line 2 and front end height

The information contained in this table is for the design work.

The auxiliary significance is very important, and it is the key point of knowledge mining. See "hood turning point and front end distance$Y$@Side. Side line 2 and front height$Y$@ Side. front and bottom style line length X@Side, side line 1, and front end height Y@Side" The four design parameters are closely related to the image objectives [23]. It can be seen that they are the design parameters that have the greatest influence on image style judgment. The key points of the design controlled by these four design parameters are the position of the body appearance, which should be paid special attention to in the design activities.

5. Conclusion

This paper presents the basic structure of the automobile gene network model and the technical method of constructing two sub-networks of design elements and image objectives. Based on the preliminary analysis of the two networks, this paper produces some relevant knowledge to assist designers to carry out design activities. The existence and stability of the gene network model are demonstrated. The existence of a gene network shows that there are potential relationships between the elements of the two subnetworks of automobile modeling. The mining and identification of these relationships, it lays a foundation for improving the design efficiency and success rate [24]. Gene networks can help transform the traditional design activities that rely on experience and perceptual judgment into targeted and accurate operation of "gene surgery."

Although the two sub-networks in this paper can be obtained through an independent modeling process, they are not in their own independent state, in fact, the mapping relationship between them can be obtained by constructing the image target network through the "indirect method." This mapping relationship helps to accurately find the design element node group that affects an image target. This paper also puts forward the identification method of this kind of association, which is the key content of further knowledge mining.

Product design DNA is a new concept produced by the application of the idea of genetic engineering in the field of industrial design, which involves many knowledge fields. It aims to give products a unique form and style image to shape the brand. This paper systematically summarizes the current situation and progress of product design DNA research at home and abroad, focusing on the expression structure, application research progress, key technologies, and the shortcomings of existing research. Finally, the hot spots and trends of product design DNA research are: revealing the generation and evolution law of product design DNA in the whole life cycle; Explore the cognitive mechanism of users for product design DNA; realize the connection between product design DNA reasoning and production links, as a new industrial design method, product design DNA draws lessons from the idea of genetic engineering, which provides a feasible path for realizing the rapid response of the design to market changes and establishing brand positioning. This paper systematically introduces the research status and latest progress of product design DNA for industrial design, points out the shortcomings of existing research, looks forward to the development trend of future research and holds that it is necessary to reveal the generation and evolution law of product design DNA in the whole life cycle, explore the cognitive mechanism of users for product design DNA, and realize the connection between product design DNA reasoning and production links, it will become the focus of future research work.

How to find a suitable carrier form, how to reduce the learning cost of users, and improve the use efficiency of users have become a difficult problems in front us. The emergence of the interaction design method points out the way forward for us. We use the old cognitive model formed in people's life experiences to recognize new product forms, strengthen the relationship between the two, and make users as handy as using old products. This paper mainly studies the application method of interactive design based on cognitive psychology in industrial design, establishes the mapping relationship between new products and old cognitive models, abstracts and summarizes the new elements in product design into the old cognitive models, and enables users to recognize and use new products naturally and efficiently through their natural matching.

In order to make a product easy to use, or even a product that users like to use, the design must be people-oriented, take the inner emotional needs of users as the central focus, and integrate the emotional factors of users into the product, so that users can obtain emotional experience results in the process of using the product. As for how to get an emotional design, the idea of interaction design provides designers with new ideas.

Method 1: integrate an elegant aesthetic experience into the product. Method 2: write the real scene, express the truth and trigger Association. Method 3: game interactive behavior.

Method 4: expand the participation of users and make users have the fun of creating. Method 5: the product should be in harmony with the use scene.

Hindawi
Security and Communication Networks
Volume 2023, Article ID 9854917, 1 page
https://doi.org/10.1155/2023/9854917

Retraction

Retracted: Multitarget Tracking Algorithm in Intelligent Analysis of Football Movement Training Stance

Security and Communication Networks

Received 13 September 2023; Accepted 13 September 2023; Published 14 September 2023

This article has been retracted by Hindawi following an investigation undertaken by the publisher [1]. This investigation has uncovered evidence of one or more of the following indicators of systematic manipulation of the publication process:

(1) Discrepancies in scope

(2) Discrepancies in the description of the research reported

(3) Discrepancies between the availability of data and the research described

(4) Inappropriate citations

(5) Incoherent, meaningless and/or irrelevant content included in the article

(6) Peer-review manipulation

The presence of these indicators undermines our confidence in the integrity of the article's content and we cannot, therefore, vouch for its reliability. Please note that this notice is intended solely to alert readers that the content of this article is unreliable. We have not investigated whether authors were aware of or involved in the systematic manipulation of the publication process.

Wiley and Hindawi regrets that the usual quality checks did not identify these issues before publication and have since put additional measures in place to safeguard research integrity.

We wish to credit our own Research Integrity and Research Publishing teams and anonymous and named external researchers and research integrity experts for contributing to this investigation.

The corresponding author, as the representative of all authors, has been given the opportunity to register their agreement or disagreement to this retraction. We have kept a record of any response received.

References

[1] C. Li and Q. Peng, "Multitarget Tracking Algorithm in Intelligent Analysis of Football Movement Training Stance," *Security and Communication Networks*, vol. 2022, Article ID 6579066, 8 pages, 2022.

Hindawi
Security and Communication Networks
Volume 2022, Article ID 6579066, 8 pages
https://doi.org/10.1155/2022/6579066

Research Article

Multitarget Tracking Algorithm in Intelligent Analysis of Football Movement Training Stance

Changrui Li[1] **and Qiuping Peng**[2]

[1]*School of Physical Education and Health, Nanning Normal University, Nanning 530001, China*
[2]*School of Physical Education and Health Science, Guangxi University for Nationalities, Nanning 530006, China*

Correspondence should be addressed to Qiuping Peng; pqp2022@126.com

Received 8 April 2022; Revised 16 June 2022; Accepted 3 July 2022; Published 4 August 2022

Academic Editor: Fang Liu

In recent years, with the continuous development of computer technology, deep learning has been widely applied to computer vision tasks and has achieved great success in areas such as visual detection and tracking. On this basis, making deep learning techniques truly accessible to people becomes the next objective. Target detection and tracking in football gesture training is a quite challenging task with great practical and commercial value. In traditional football training methods, target trajectories are often extracted by means of a recording chip carried by the player. However, the cost of this method is high and it is difficult to replicate in amateur stadiums. Some studies have also used only cameras to process targets in football videos. However, due to the similarity in appearance and frequent occlusion of targets in football videos, these methods often only segment targets such as players and balls in the image but do not allow them to be tracked. Target tracking techniques are of great importance in football training and are the basis for tasks such as player training analysis and match strategy development. In recent years, many excellent algorithms have emerged in the field of target tracking, mainly in the categories of correlation filtering and deep learning, but none of them are able to achieve high accuracy in player tracking for football training videos. After all, the problem of locating clips of interest to athletes from a full-length video is a pressing one. Traditional machine learning-based approaches to sports event detection have poor accuracy and are limited in the types of events they can detect. These traditional methods often rely on auxiliary information such as audio commentary and relevant text, which are less stable than video. In recent years, deep learning-based methods have made great progress in the detection of single-player video events and actions, but less so in the detection of sports video events. As a result, there are few sports video datasets that can be used for deep learning training. Based on research in computer vision and deep learning, this paper designs a multitarget tracking system for football training. To be specific, this algorithm uses multiple cameras for image acquisition in the stadium in order to accurately track multiple targets in the stadium over time. Furthermore, the framework for a single camera multitarget tracking approach has been designed based on deep learning-based visual detection methods and correlation filter-based tracking methods. This framework focuses on using data correlation algorithms to fuse the results of detectors and trackers so that multiple targets can be tracked accurately in a single camera. To sum up, this research allows for robust and real-time long-term accurate tracking of targets in football training videos through multitarget tracking algorithms and the intercorrection of multiple camera systems.

1. Introduction

The vast majority of information that humans obtain from the outside world comes from vision. As a result, vision becomes the most important form of information acquisition for humans [1]. In recent years, with the rapid development of computers and information technology, people are increasingly using computers to participate in everyday production and life [2, 3]. To be specific, computers can significantly extend human brainpower and perception, and the use of computers to simulate human visual perception has led to the creation of computer vision [4]. Computer vision is the science of acquiring and processing visual information through cameras and computers, with the

ultimate goal of enabling computers to perform some of the functions of human vision in order to understand the three-dimensional world [5]. What is more, computer vision is a multidisciplinary intersection and combination of mathematics, image processing, biology, computer science, and so on [6, 7]. As one of the most important tasks in computer vision, target tracking technology has become a hot research topic in recent years due to its promising applications and market demand. The goal of computer vision research is to enable computers to adapt to their environment autonomously and to observe and understand the world as humans do [8]. With the development of deep learning theory in recent years, computer vision has made promising advances in a number of tasks such as classification, detection, recognition, and tracking. Target tracking is the process of tracking an object of interest in the first frame of a video sequence to obtain the motion parameters associated with the target, including position, velocity, and trajectory [9]. The object is then recognised and tracked and its behaviour understood to perform subsequent higher level vision tasks. Target tracking technology has been widely used in many fields such as unmanned vehicles [10], intelligent video surveillance [11], smart construction [12], military guidance [13], and smart medical care [14].

With the rapid growth and distribution of videos on the Internet, there is an urgent need to find the video clips that people need quickly. Sports videos are a very important part of our daily lives and play a large part in people's entertainment [15]. Football is one of the most popular sports around the world, and videos of popular football matches are widely distributed and watched. For fans, they want to be able to watch the full match directly from the event they are interested in. For video editors, they want to be able to quickly organise the video content they need from a large number of sources, or even automatically generate video summaries or highlight reels [16]. What is more, for athletes and coaches alike, the analysis of players' movement data from video footage of football matches is one of the most important tasks in order to train better [17]. After all, the coaches need some of the motion data in the video for their analysis and the players themselves want to be able to record their own motion data in real time, which needs to be extracted from the target motion traces in the video. For professional football, these needs can be met, as this is only possible with the support of costly human and material resources [18]. For amateur football matches, which are much larger in scale, a low-cost target detection and tracking solution is of great practical value and relevance. As a result, event detection for football training videos has been an important topic in multimedia research.

Target detection, which focuses on determining the size and location of a target in a video image, is a core problem in machine vision [19]. However, target detection has always been one of the most challenging problems in machine vision due to a number of factors such as variations in illumination, object occlusion, and complex background conditions. In recent years, target detection algorithms have become a hot issue in the field of machine vision [20]. Many efficient algorithms such as twin algorithms (Figure 1) have emerged and are widely used in target detection and tracking. The target tracking technology plays an essential role in football video analysis [21]. As the most watched sport in the world, football is a rich and widespread sport with huge commercial value. When watching football videos, different actors have different requirements for football videos. The average viewer tends to focus on a particular player of interest when watching a video of a football match. As a result, there is a need to provide viewers with high-level semantic analysis of video summaries, highlights, player movement recognition, and so on. The target tracking technology is the basis for these high-level semantic functions [22]. For professionals such as team coaches, there is a need for detailed information on the field of play to analyse matches and develop training programmes and game strategies, such as player trajectories, distances travelled, running speeds, and other movement parameters. Then the target tracking technology can provide this data directly [23]. In addition, for the referee on the field of play, there is a need for a variety of auxiliary information to ensure fair play, such as precise positioning of players, football trajectory analysis, and foul play recognition, in order to avoid potentially controversial calls during the game due to fierce competition. To sum up, researching and analyzing player tracking in football video is a fundamental research task for many practical applications and has important theoretical and practical value.

With the rise of deep learning theory in recent years, deep learning-based target tracking algorithms have been gaining prominence in the relevant industry in recent years [24]. However, the application of deep learning to target tracking has not been smooth. Unlike vision fields such as classification and recognition, the main problem with deep learning in target tracking is the lack of training data. Deep models can perform well by learning effectively from large amounts of labelled data, whereas tracking tasks only provide the first labelled image as training data [25]. In this case, it is quite difficult to train a deep model from scratch. The main idea of current deep learning-based tracking algorithms is to pretrain the depth model offline using the marker data and finetune the pretrained tracker online with the current samples during tracking. This migration learning approach will reduce the need for training samples and improves the feasibility of deep learning-based tracking algorithms [26]. Target detection is one of the main areas of research in computer vision and is widely used in areas such as video surveillance, face recognition, defect detection, and robot navigation. The goal of target detection is to find the exact location of the target of interest in the image and to give an accurate classification of the target. Deep learning is a data-driven approach that learns the features of a target from a large amount of data, and the features obtained from deep learning are often better than those designed by hand [27]. In the field of image detection, deep learning has achieved the best results to date, and the reason for this is that the large amount of training data allows the network to learn abstract, high-level features that are highly expressive of the target.

In fact, the target tracking technology is based on image processing techniques and aims to obtain the true position of

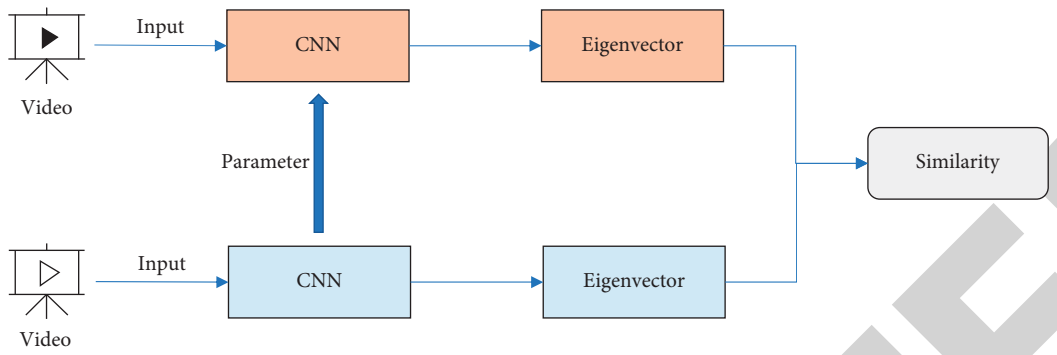


Figure 1: Basic framework of twin algorithm.

a target from a video sequence and to analyse it [28]. However, there are many difficulties in the practical application of video target tracking. Firstly, the similarity between the target and the background makes it difficult to capture the differences between the two. Secondly, the appearance of the target changes continuously over time. On the one hand, the object itself changes in shape, which is particularly noticeable in long-term tracking. On the other hand, external conditions such as lighting have an effect on the target. In addition to this, the position of the target in the video is constantly changing, and occlusion may occur. What is more, tracking has to balance the need for accuracy in target location with the need for real-time performance. As a result, there is a wide range of video target tracking algorithms available, but they lack generality. As shown in Figure 2, target tracking algorithms can be divided into different categories depending on the use of target tracking information.

The target tracking algorithm based on contrast analysis uses the difference between the target and the background to track the target and can be classified as form-focused tracking, centre-of-mass tracking, and edge tracking depending on the tracking reference point [29]. The algorithm does not work well in complex environments but is quite effective in situations where the difference between target and background is significant. What is more, the algorithm is computationally simple, responsive, and, in some cases, has great tracking accuracy. However, it is susceptible to external disturbances, has high random errors, and is poor for violent movements and occlusions. Matching-based tracking algorithms can distinguish between the attributes of a target and other things [30]. To be specific, a matching-based tracking algorithm begins by extracting the features of the target and matching them in each frame of the video sequence. The main features used in target tracking are feature points, contours, edges, colors, textures, etc. The main idea of motion detection-based tracking algorithms is to detect the difference between the motion of the target and the background in order to determine the position of the target, thus enabling the tracking of the target. This algorithm highlights the difference in time or space between the motion of the target and the background, avoiding the need for complex modelling of the target, and is now increasingly used. Finally, the detection-based tracking algorithm can essentially transform the tracking problem into a binary classification problem, i.e., distinguishing between the target and the background [31]. These methods often train a detector that detects the location of the target frame by frame in the whole image and then connects it to the complete motion trajectory of the target. The biggest challenge for detection-based tracking algorithms is to train an effective detector and to ensure that the algorithm is real-time.

In recent years, deep learning techniques have been widely applied to computer vision tasks, with great success in areas such as vision detection and tracking [32]. Building on this foundation, the implementation of deep learning techniques is the next step and it even can be used in construction [33]. However, there are relatively few datasets for temporally bounded tagging of events in video. Some of the existing event annotation datasets are mostly mixed event types, and there are no datasets specifically for football video events. For deep learning methods, adequate labelled datasets are an important prerequisite for the development of related techniques. This study is based on football video, in which all players are tracked and the trajectory of each player in a normal match is extracted. Previously, this task has been carried out using a chip attached to the player to record the player's movement, but this is expensive and does not allow for real-time output of player movement data. The hardware in this research is able to accurately extract the player's entire movement data using only a camera. It can save costs, improve the user experience, and can be used in real life scenarios, which can become great reference for the football players as well as coaches.

2. Module Analysis

The video analysis system for target detection and tracking in football training is divided into four main modules: image acquisition module, storage system module, target detection, and tracking module, as well as VGA display module. The overall system block diagram is shown in Figure 3.

The main function of this system is to detect moving objects in the video image by means of an algorithm. In addition to this, the moving object can be extracted from the background image and then the background can be separated from the moving object according to the motion and stillness, and then the target can be tracked by the algorithm.

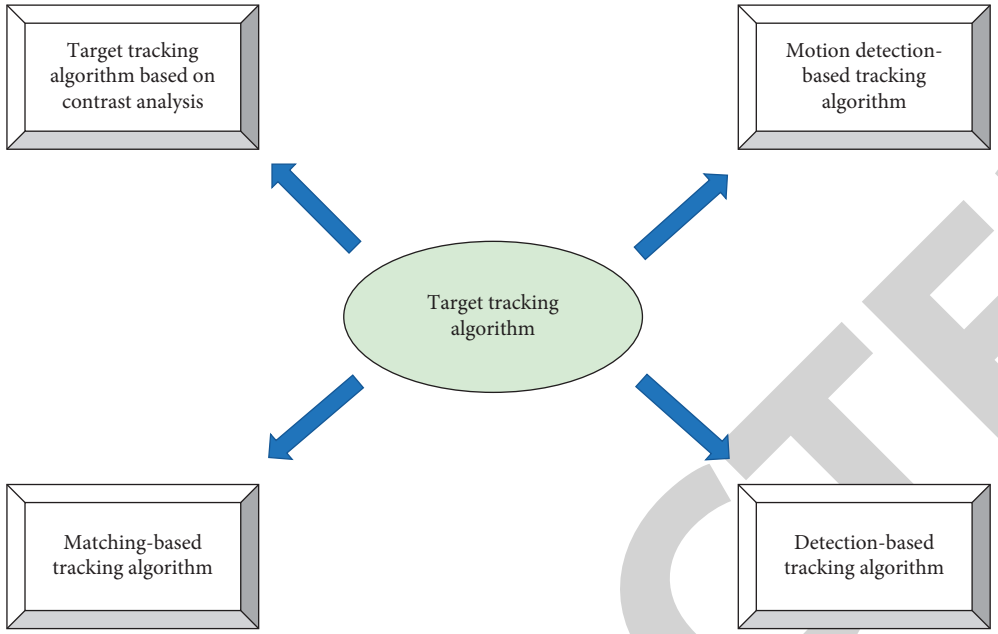


Figure 2: Various target tracking algorithms.

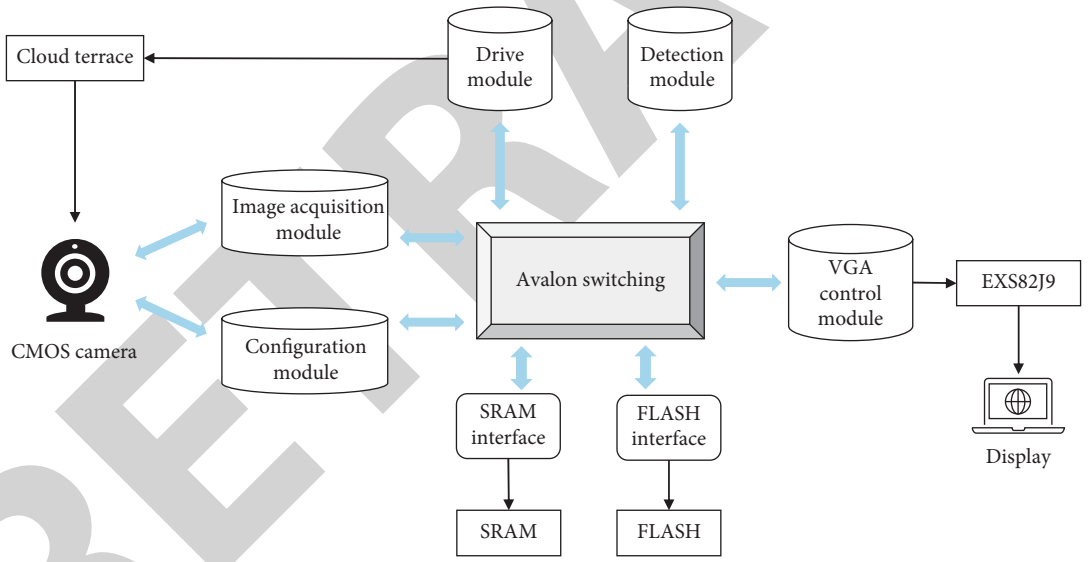


Figure 3: Overall system block diagram.

2.1. Image Acquisition Module. The video image capture module uses a CMOS video capture camera, the core of which is an internal large scale integrated circuit chip, a RAM chip that can be read and written. The core part of the video capture camera is the chip, which converts each pixel of the captured image into its own charge and voltage. The basic unit of the CMOS digital integrated circuit is a voltage-controlled amplifier with the advantages of high interference immunity and low-static power consumption.

2.2. Storage System Module. The storage module mainly applies a synchronous dynamic random storage memory as a picture memory. This memory receives a clock signal before it receives a response, enabling it to be synchronised with the computer system bus.

2.3. Target Detection and Tracking Module. The internal structure of the FPGA chip consists of seven modules: programmable input and output units, configurable logic modules, digital clock management modules, embedded modules, wiring resources, underlying embedded functional units, and embedded dedicated cores. When the chip is powered up, the data is read into the on-chip programmable RAM memory and when the match is completed, the chip starts to operate and the logic inside returns to its original state when the power is removed. The chip can therefore be

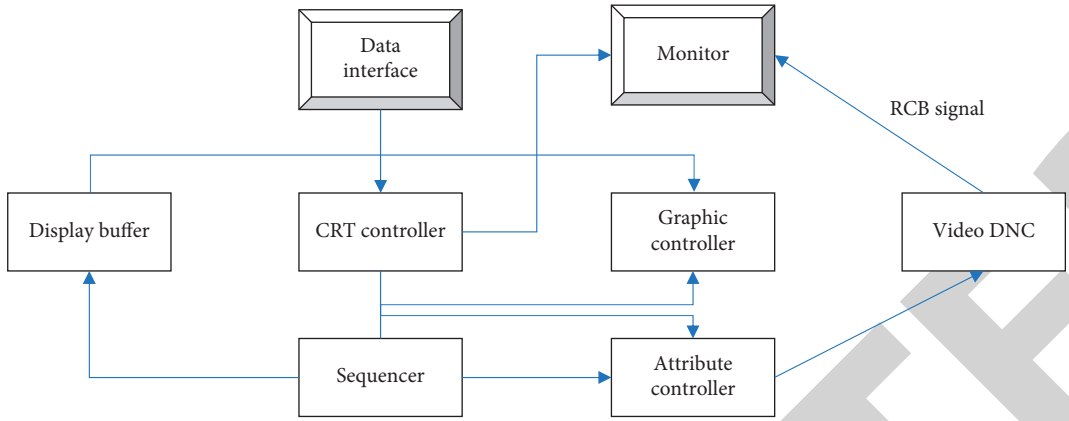


Figure 4: Control circuit of the VGA display module.

used repeatedly. When you want to change the function of the circuit, you can simply change the EPROM chip and write a different programming language, thus enabling different functions to be changed.

2.4. VGA Display Module. The VGA display system consists of three main modules: the control circuit, the display cache, and the video BIOS program. The control circuit is shown in Figure 4.

The control circuit is responsible for the chronological occurrence, display buffer data manipulation, master clock selection, and other functions. The display module enables the synchronisation of the display data update and the display.

3. Multitarget Tracking Algorithm

3.1. Feature Selection. The first step in the tracking task is to take the target features. To enhance the feature representation, conventional features and depth features are extracted separately. In terms of feature processing, discrete features are transformed into continuous features to enhance the feature representation and factorization is used to reduce the computational complexity. The output is corrected for tracking drift using prediction speed. Target feature extraction is an important part of the visual tracking task and the quality of the features directly affects the final tracking result. Target features can be divided into traditional manual features and depth features. Traditional manual features are an older form of feature representation and are usually represented using both global and local features, including colour and texture features. As one of the most widely used features, colour features are robust to angle changes and pose changes. Unlike the colour feature, the texture feature is not a pixel point-based feature. In particular, it requires a statistical calculation over a region containing multiple pixel points. Texture features have good nondeformation to illumination. In fact, conventional features rely heavily on the representation of the appearance of the object. However, due to the human factor of photography and various environmental factors, the actual images obtained often show large variations in appearance. As a result, progress in traditional manual characterisation has been slow and it has been difficult to achieve significant breakthroughs in accuracy.

The football video tracking task mainly focuses on tracking the target player in the long shot. Firstly, the position of the target player is obtained in the initial frame and the position of the player is determined in the following frames. The rectangular frame corresponding to the player's position is denoted as (a, b, k, j), where (a, b) represents the horizontal and vertical coordinates of the upper left corner of the rectangular frame, k represents the width of the rectangular frame, and j represents the height of the rectangular frame. The player's position is given in the initial frame as the target frame, and the images in the target frame are extracted and the tracker model is built. In subsequent frames, the images in the candidate frame are analysed and processed to determine the player's location. The candidate frame is the area where the target player is likely to be located, which is the search area for the tracking algorithm, as shown in Figure 5.

The candidate box area does not need to be the whole picture as the position of the player does not change much between the two frames. The candidate box is a square box centred on the target positioned in the previous frame, with sides as shown in the following equation:

$$L = \sqrt{[(\theta \times k) \times (\theta \times j)]}, \quad (1)$$

where L refers to the side of the candidate box and θ refers to the proportion of candidate areas.

3.2. Feature Extraction. Depth features and FHOG features are extracted separately from the feature representation of the target, and these two features are then fused to obtain the final feature representation. The depth model uses a pretrained model trained offline on the ImageNet classification task and finetuned online during the target tracking phase. As the tracking task in this paper only requires feature extraction on the VGG model and not target classification, only the first 14 convolutional layers of the VGG model are

Figure 5: Candidate frame of feature selection.

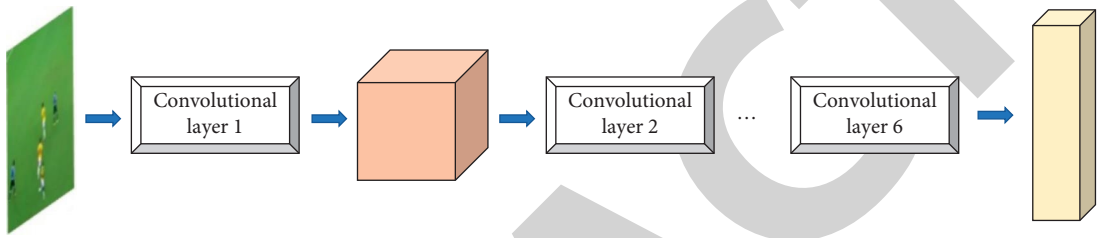


Figure 6: Feature output size.

used. The network model consists of 6 convolutional groups, with two to three convolutional layers within each convolutional group. The input to the network model is $64 \times 64 \times 3$ and the outputs of layers 3 and 7 are extracted as shallow and deep features, respectively. The feature output size of layer 3 is $16 \times 16 \times 68$ and that of layer 7 is $9 \times 9 \times 212$, as shown in Figure 6.

3.3. Feature Continuity. To address the need to improve the accuracy of the tracking results, an extension of the discrete features to a continuous approach is devised. This approach can not only improve the expressiveness of the features but also can result in a continuous response map. At the same time, precise subpixel positions can be achieved during target localization, thus providing further improvements in tracking accuracy. The conversion of discrete features to continuous features naturally involves interpolation, as shown in Figure 7. Three spline interpolations are performed on the extracted features. As the tracking is performed in the frequency domain, the feature interpolation operation is also an interpolation process in the frequency domain by first transferring the features from the spatial domain to the frequency domain via a Fourier transformation.

The basic process of cubic spline interpolation in one dimension is to fit a continuous function with a segmented set of cubic equations. The solution of this set of cubic equations requires four constraints, namely equal function values at the nodes, equal first-order derivatives at the nodes, equal second-order derivatives at the nodes, and zero second-order derivatives at the endpoints, to be solved, respectively. To be specific, the implicit representation can be expressed by the following equation:

$$f(x, v) = \sum_{i=0}^{I-1} x(m) \times n \times \left(v - \frac{V}{I} \times i \right), \tag{2}$$

where v, i refers to the variables in the continuous and discrete domains, respectively, V, N indicates the boundary values in the continuous and discrete domains, respectively, $f(x, v)$ refers to the continuous function, x indicates the discrete function, and n is the interpolation function.

3.4. Multitarget Tracking. The multitarget tracker is based on a detector and a single-target tracker. The entire video is first decomposed into a number of tracking cycles, each containing a number of consecutive frames. In each tracking cycle, the first frame is detected and the next few frames are tracked. The results of the two adjacent tracking cycles are then fused by means of data correlation, as shown in Figure 8.

In each tracking cycle, the first frame will detect all the target positions in the image and then initialise the tracker with the initial position of each target. The tracker is then initialised with the initial position of each target. A short track is then performed over the remainder of the image sequence to obtain the trajectory of each target. The next step is to assign the corresponding numbers to all the tracks in the sequence, which is done by means of a data association algorithm. The data association algorithm matches the trajectories of each numbered target from the previous cycle with all the trajectories of the current cycle and then assigns the corresponding numbers to these trajectories and saves them.

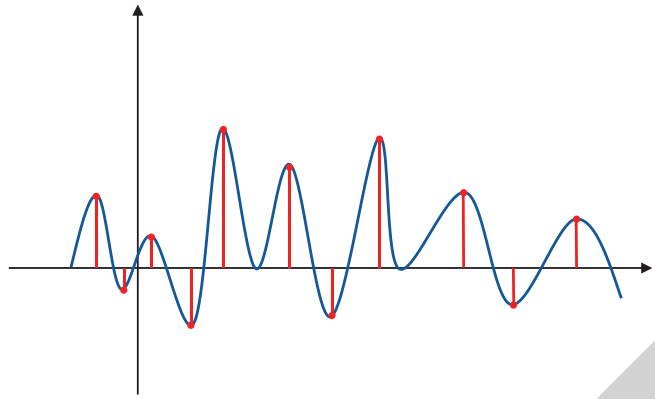


Figure 7: Conversion of discrete features to continuous features.

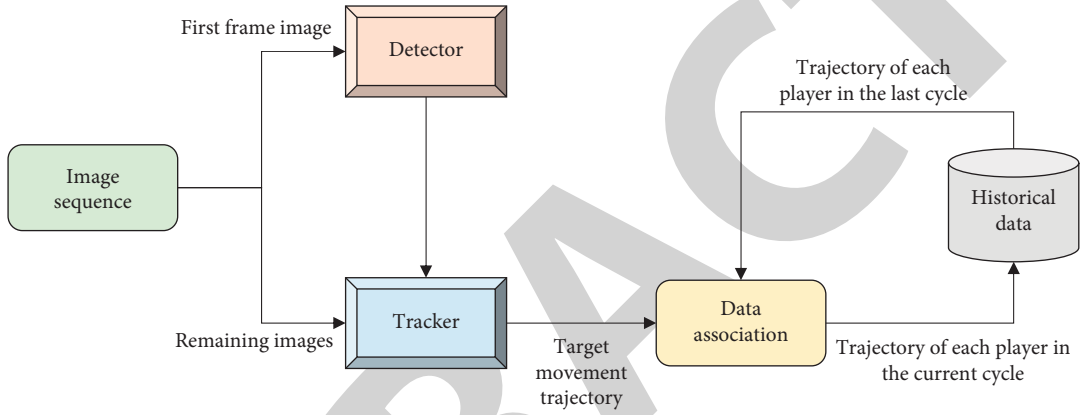


Figure 8: Framework of multitarget tracking algorithm.

4. Conclusion

In recent years, deep learning-based detection algorithms have been developed rapidly. On the basis of this, deep learning has continued to improve in terms of real time and accuracy. As a result, correlation filter-based trackers have been widely used due to their excellent tracking speed and accuracy. The target tracking technology plays an essential role in football match video analysis, with implications for player training, strategy development as well as football event detection. This research focuses on target detection and tracking algorithms in football video, and designs a multitarget tracking method based on a deep learning detector. First of all, this study designs a framework for multitarget tracking in football video and investigates the detection, tracking, and data association modules. This can enable the accurate tracking of multiple targets in a single camera. In the feature extraction process, a combination of traditional manual features and depth features was used to extract the FHOG features and the depth features of the VGG network model, respectively. The discrete features were transformed into continuous features in the frequency domain using cubic spline interpolation in order to improve the feature representation capability and the accuracy of the results. To speed up tracking and reduce the effects of overfitting, the dimensionality of the features is significantly reduced using factorization.

However, although the multitarget tracking algorithm designed in this research performs well in terms of accuracy, several problems still remain. Firstly, the predicted speed is not accurate enough. Although a moving target will maintain its inertia and move smoothly in a realistic scene, camera movement can cause the smoothness of the target's trajectory to be significantly reduced in the video frame. In fact, offsetting camera movement can significantly improve the accuracy of the predicted velocity. In addition, there is no dynamic adjustment for factorization dimensionality reduction. The dimensionality reduction matrix remains constant during the tracking process and cannot be targeted in subsequent features, which may reduce the accuracy of the tracking results to a certain extent.

Data Availability

The labelled data set used to support the findings of this study is available from the corresponding author upon request.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Hindawi
Security and Communication Networks
Volume 2024, Article ID 9759083, 1 page
https://doi.org/10.1155/2024/9759083

Retraction

Retracted: Path Selection Strategy of Communication Network Based on Graph Convolutional Neural Network

Security and Communication Networks

Received 8 January 2024; Accepted 8 January 2024; Published 9 January 2024

This article has been retracted by Hindawi following an investigation undertaken by the publisher [1]. This investigation has uncovered evidence of one or more of the following indicators of systematic manipulation of the publication process:

(1) Discrepancies in scope

(2) Discrepancies in the description of the research reported

(3) Discrepancies between the availability of data and the research described

(4) Inappropriate citations

(5) Incoherent, meaningless and/or irrelevant content included in the article

(6) Manipulated or compromised peer review

The presence of these indicators undermines our confidence in the integrity of the article's content and we cannot, therefore, vouch for its reliability. Please note that this notice is intended solely to alert readers that the content of this article is unreliable. We have not investigated whether authors were aware of or involved in the systematic manipulation of the publication process.

Wiley and Hindawi regrets that the usual quality checks did not identify these issues before publication and have since put additional measures in place to safeguard research integrity.

We wish to credit our own Research Integrity and Research Publishing teams and anonymous and named external researchers and research integrity experts for contributing to this investigation.

The corresponding author, as the representative of all authors, has been given the opportunity to register their agreement or disagreement to this retraction. We have kept a record of any response received.

References

[1] X. Zhang, "Path Selection Strategy of Communication Network Based on Graph Convolutional Neural Network," *Security and Communication Networks*, vol. 2022, Article ID 9548441, 14 pages, 2022.

Hindawi
Security and Communication Networks
Volume 2022, Article ID 9548441, 14 pages
https://doi.org/10.1155/2022/9548441

Research Article

Path Selection Strategy of Communication Network Based on Graph Convolutional Neural Network

Xiaojun Zhang

College of Software Technology, Henan Finance University, Zhengzhou 450000, China

Correspondence should be addressed to Xiaojun Zhang; castorly@hafu.edu.cn

Received 14 April 2022; Accepted 24 June 2022; Published 18 July 2022

Academic Editor: Zhiping Cai

In order to improve the efficiency of communication network path selection, this paper combines the graph convolutional neural network to formulate the communication network path selection strategy and selects the enhanced decoding algorithm as the fixed-point decoding algorithm. For the quantization scheme based on the enhanced decoding algorithm, the selection of the fixed-point integer bit width of each operation variable in the SISO decoder is analyzed and determined by the method of statistical characteristic analysis. Moreover, this paper calculates the normalized threshold value according to the proposed state metric normalization scheme. In addition, this paper constructs an intelligent communication path selection system. Through research, it can be seen that the communication network path selection system based on graph convolutional neural network proposed in this paper can effectively improve the effect of multicommunication path selection.

1. Introduction

In recent years, with the rapid development of mobile communication technology, the cost of intelligent sensing devices such as smartphones and tablet computers has become lower and lower, and the communication capabilities have become stronger and stronger. The mobile ad hoc network (MANET) is a network composed of the above-mentioned smart devices, which has also developed rapidly and is widely studied in the field of network and its communication. The biggest feature of the MANET is that it can be self-discovered, configured, and self-organized, so it has the advantages of not requiring infrastructure support, highly dynamic, and mobile communication. Therefore, it has been widely used in marine organisms, forest fires, biomedicine, environmental monitoring, and other highly dynamic extreme environments that cannot be perceived in real time by humans and provides information collection, transmission, and processing services in extreme environments. For example, in-vehicle sensor network collects data through in-vehicle sensors or mobile phone devices, has mobility and can effectively cover the collection area, and is suitable for large-scale urban data collection. Wildlife tracking network collects animal behavior, physical condition, and movement information by deploying sink nodes, static nodes, and mobile nodes. In addition, the hybrid monitoring network in smart healthcare automates common medical processes to provide location, status, and tracking information for patients and assets. In the above-mentioned practical ad hoc network applications, the communication signal is attenuated due to the constant movement of nodes, the sparse network topology, and the occlusion of obstacles, which in turn makes the traditional MANET communication mode unable to operate normally. Ultimately, the network cannot be connected most of the time. Because MANET can only determine the next hop node after establishing the route between the communication endpoints, it needs to ensure that at least one link exists when the message is transmitted, and otherwise, the routing protocol of MANET cannot find the destination node.

When designing the algorithms and protocols of wireless ad hoc networks, the inherent characteristics of wireless ad hoc networks must be considered, and existing design ideas and methods for wired networks cannot be copied, so as to effectively support wireless ad hoc network applications. Algorithms and protocols in wireless ad hoc networks must

have the characteristics of distributed autonomy, computational and storage efficiency, scale adaptability, and scalability. On the one hand, the wireless ad hoc network does not need to rely on any preset network facilities. It can be deployed at anytime and anywhere. There is usually no central control point similar to the base station in the network, and the nodes have equal status. The nodes coordinate their behaviors through layered protocols and distributed algorithms, quickly and automatically form an independent network, and support the dynamic joining and leaving of nodes. On the other hand, compared with personal computers, terminals in wireless ad hoc networks usually have small memory, low CPU processing capacity, and limited power supply, which requires that the software algorithms designed for wireless ad hoc networks must be simple and practical. Computational and storage costs are low. In addition, the scale of wireless ad hoc networks is usually large, ranging from dozens of nodes to thousands of nodes. The communication between any node in wireless ad hoc networks needs to involve multiple intermediate nodes. Especially when the network is large, it will inevitably have problems in communication security, load balancing, and other aspects, and put forward higher requirements for algorithms and protocols.

This paper combines the graph convolutional neural network to formulate the communication network path selection strategy, constructs an intelligent system, and improves the scientificity of the communication network path selection strategy.

2. Related Work

Graph data mining mainly includes graph clustering and subgraph pattern mining. The main researches on clustering algorithms in uncertain graphs are hierarchical clustering algorithm and K-nearest neighbor query algorithm [1]. A heuristic stochastic algorithm for solving the correlation clustering problem is proposed which can be used to solve the uncertain graph clustering problem [2]. An approximate algorithm for computing fuzzy clustering of uncertain graphs is proposed [3]. The research contents of subgraph pattern mining mainly include frequent subgraph patterns and dense subgraph patterns. Frequent subgraph pattern mining mainly studies the frequent subgraph pattern mining under the conditions of expectation and probability [4]. The goal of expected frequent subgraph pattern mining on uncertain graphs is to mine subgraph patterns with high expected support from the uncertain graph database, while the goal of probabilistic frequent subgraph pattern mining is to mine probabilistic frequent subgraph patterns in the uncertain graph database. *Subplot Mode.* Literature [5] proposes a search space pruning technique and an efficient expected support calculation method to improve efficiency. Literature [6] proposes the RAKING algorithm which combines random walk and uncertainty of uncertain mode. Dense subgraph mining mainly includes dense vertex subset mining and top-k maximal clique mining [7]. Graph clustering algorithms have many applications in communication networks and social networks.

In graph theory, the shortest path problem is a classical problem that has been widely studied and has a wide range of applications in transportation networks, communication networks, and social networks. In uncertain graphs, the research on the shortest path problem mainly includes the shortest path problem under probabilistic semantics and the shortest path problem under expectation semantics [8]. Literature [9] defines the shortest path problem under probabilistic semantics and proposes a shortest path algorithm based on probability threshold. Literature [10] defines the expected shortest path problem and proposes a random sampling approximation algorithm.

Maximum Flow Problem. The maximum flow problem is a classic combinatorial optimization problem in operations research, which is widely used in transportation networks, water supply networks, and financial systems. The Edmonds–Karp algorithm is a classic algorithm for solving the problem of determining the maximum flow in a graph. In uncertainty graphs, the most reliable maximum flow problem is mainly studied [11]. Literature [12] proposed a simple path-based algorithm and an algorithm based on space partitioning. Literature [13] proposed a state space partitioning algorithm based on probability and cutset double filtering. Literature [14] proposed three algorithms, which are NWCE algorithm based on negative weight community elimination, SPEA-t algorithm based on time constrained priority single ring elimination, and SPEA-p algorithm based on probability threshold constrained priority single ring elimination.

Minimum spanning tree has a wide range of applications. For example, it has applications in urban traffic construction and network design. Literature [15] studied the reliability of the minimum spanning tree in uncertain graphs and proposed a reliability calculation method based on the idea of edge set partitioning and optimized the method with the union search set. Literature [16] proposed an optimal spanning tree and the concept of suboptimal spanning tree; literature [17] studied the top-k spanning tree in uncertain graphs and proposed a PTopK query algorithm based on spanning tree filtering and a PTopK query algorithm based on combined filtering.

Literature [18] proposed an algorithm for dynamically modifying honeynet data. By dynamically sorting and modifying the data in the honeynet that may be accessed by the attacker to mislead the attacker, the deception ability of the honeynet is enhanced, so as to deceive the intruder who intends to destroy the completeness of the data. In addition, by deploying a honeynet transparent to attackers in the honeynet, the honeynet is separated from the business network where the honeynet is deployed, so that the traffic in the honeynet can be dynamically controlled according to the security requirements. Literature [19] proposes a software-defined honeynet (SDH) based on the idea of SDN. This honeynet can find the bottleneck of the link by calculating the relevant parameters of each link in the honeynet and use the SDN controller to dynamically Therefore, a dynamically generated fake honeynet topology can be presented to the attacker in the honeynet. Literature [20] proposes an SDN virtual honeynet for network attack situations. The honeynet

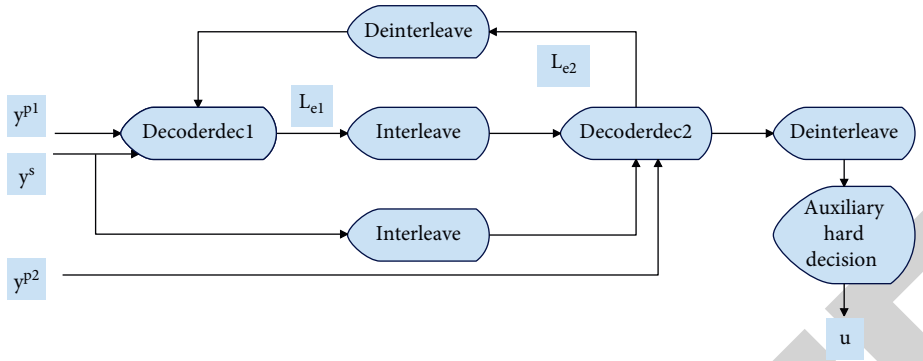


Figure 1: Schematic diagram of iterative decoding structure of turbo code.

system combines mimic defense and adopts SDN technology to realize flexible and dynamic control of honeynet traffic and realize the separation of honeynet data control layer and forwarding layer, which enhances the scalability and maintainability of the honeynet. At the same time, the validity of the dynamic transformation mechanism of the virtual honeynet is verified by using game theory.

3. Fixed-Point Turbo Code Decoding and Its Implementation

In the communication network constructed in this paper, in order to achieve better decoding performance of turbo codes, the decoding of component codes must use soft-input and soft-output decoding algorithms. Thus, the exchange of soft information between the component decoders in the iterative decoding process is realized. The structure of turbo code iterative decoder is shown in Figure 1.

The basic decoding process is that the received code sequence is demultiplexed, and the demodulated systematic bits y^s, check bits y^{pl}, and the deinterleaved outer information given by the second component decoder dec2 in the previous iteration are sent to the first component decoder dec1. The extrinsic information generated after decoding by dec1 is interleaved by the interleaver as a priori information of the second component decoder dec2 and sent to dec2 together with the interleaved demodulated systematic bits and the check bit y^{p^2}. The outer information generated by dec2 is deinterleaved and sent to the first component decoder decl for the next round of iterative decoding. When the number of iterations is completed or the stop iteration decision condition is reached, the log-likelihood ratio LLR generated by dec2 is deinterleaved and assisted by hard decision to obtain the final decoding output sequence. It can be seen from the above decoding process that the external information of the turbo code is fed back from another decoder, and the structure is like a turbo engine (turbo), which is the origin of the name "turbo code."

Under the condition of additive white Gaussian noise channel, the codeword received by the decoding receiver is [21]

$$y_k^\ell = \sqrt{E_s} c_k^\ell + n_k^\ell, \ell \in \{s, p1, p2\}, \tag{1}$$

where E_s represents the symbol energy of the symbol. When using BPSK modulation, $E_s = 1 \circ c_k^l$ is the encoded codeword, and the value is 1, −1. n_k^ℓ is Gaussian noise with zero mean variance σ^2. y_k^ℓ represents the codeword received by the decoding end.

The log-likelihood ratio (LLR) is defined as follows:

$$L(u_k) = \log\left(\frac{p\left(u_k = +1 | y_1^N\right)}{p\left(u_k = -1 | y_1^N\right)}\right). \tag{2}$$

Based on the decision rule of the maximum a posteriori probability MAP criterion, we can get

$$\widehat{u}_k = \text{sign}[L(u_k)]. \tag{3}$$

Among them, sign[.] is the sign function.

Further derivation from formula (2), we can get

$$\begin{aligned} L(u_k) &= \log\left(\frac{p\left(u_k = +1 | y_1^N\right)}{p\left(u_k = -1 | y_1^N\right)}\right) = \log\left(\frac{\sum_{U+} p\left(s_{k-1} = s', s_k = s, y_1^N\right)}{\sum_{U-} p\left(s_{k-1} = s', s_k = s, y_1^N\right)}\right) \\ &= \log\left(\frac{\sum_{U+} p\left(s', y_1^{k-1}\right) p(s, y_k | s') p\left(y_{k+1}^{N-1} | s\right)}{\sum_{U-} p\left(s', y_1^{k-1}\right) p(s, y_k | s') p\left(y_{k+1}^{N-1} | s\right)}\right) \\ &= \log\left(\frac{\sum_{U_+} \alpha_{k-1}(s') \gamma_k(s', s) \beta_k(s)}{\sum_{U-} \alpha_{k-1}(s') \gamma_k(s', s) \beta_k(s)}\right). \end{aligned} \tag{4}$$

It can be seen from the above formula that when calculating $L(u_k)$, it is necessary to calculate the forward state metric $\alpha_{k-1}(s')$, the branch metric $\gamma_k(s', s)$, and the backward state metric $\beta(s)$.

The forward state metric $\alpha_k(s)$ can be calculated by the following recursive calculation method:

$$\begin{aligned}\alpha_k(s) &= p\left(s, y_1^k\right) = \sum_{s'} p\left(s', s, y_1^k\right) = \sum_{s'} p\left(s', s, y_k, y_1^{k-1}\right) \\ &= \sum_{s'} p\left(s, y_k | s', y_1^{k-1}\right) p\left(s', y_1^{k-1}\right) = \sum_{s'} p\left(s, y_k | s'\right) p\left(s', y_1^{k-1}\right) \\ &= \sum_{s'} \alpha_{k-1}(s') \gamma_k(s', s).\end{aligned} \tag{5}$$

Since $\alpha_k(s)$ is calculated recursively from forward to backward, an initial value needs to be assigned at time 0. For example, in the LTE standard, the initial state of coding is the 0 state, so the probability value of the forward state metric of the zero state at time 0 is 1, and the probability value of the forward state metric of other states is 0, which can be expressed by the following formula:

$$\alpha_0(s) = \begin{cases} 1 & s = 0 \\ 0 & s \neq 0. \end{cases} \tag{6}$$

The backward state metric $\beta_{k-1}(s')$ can be calculated by the following recursive calculation method:

$$\begin{aligned}\beta_{k-1}(s') &= p\left(y_k^{N-1} | s'\right) = \sum_{s} p\left(s, y_k^{N-1} | s'\right) \\ &= \sum_{s} p\left(y_{k+1}^{N-1} | s', s, y_k\right) p\left(s, y_k | s'\right) \\ &= \sum_{s} p\left(y_{k+1}^{N-1} | s\right) p\left(s, y_k | s'\right) \\ &= \sum_{s} \beta_k(s) \gamma_k(s', s).\end{aligned} \tag{7}$$

Since $\beta_{k-1}(s')$ is calculated recursively from backward to forward, an initial value needs to be assigned at the Nth moment. For example, in the LTE standard, it needs to be reset to zero after encoding. Therefore, the probability value of the backward state metric of the zero state at time $N + \nu$ is 1, and the probability value of the backward state metric of other states is 0, which can be expressed by the following formula:

$$\beta_{N+\nu}(s) = \begin{cases} 1 & s = 0 \\ 0 & s \neq 0. \end{cases} \tag{8}$$

The branch metric $\gamma_k(s', s)$ can be expressed as

$$\begin{aligned}\gamma_k(s', s) &= p\left(s_k = s, y_k | s_{k-1} = s'\right) = \frac{p(s', s, y_k)}{p(s')} \cdot \frac{p(s', s)}{p(s', s)} \\ &= p\left(y_k | s', s\right) \cdot p\left(s | s'\right) \\ &= p\left(y_k | u_k\right) \cdot p\left(u_k\right).\end{aligned} \tag{9}$$

The first term on the right side of formula (9) is the conditional probability of receiving y_k under the condition that the information bit u_k is known at time k. From formula (1), there are

$$\begin{aligned}p\left(y_k | u_k\right) &= \frac{1}{\sqrt{2\pi}\sigma} \exp\left[-\frac{\left\|y_k - c_k\right\|^2}{2\sigma^2}\right] \\ &= \frac{1}{\sqrt{2\pi}\sigma} \exp\left[-\frac{\left(y_k^u - c_k^u\right)^2 + \left(y_k^p - c_k^p\right)^2}{2\sigma^2}\right].\end{aligned} \tag{10}$$

The second term on the right side of formula (9) is the state transition probability of the branch in the trellis graph, which is determined by the prior information $L_a(u_k)$ of the information bit u_k, and then, we have

$$p\left(u_k = -1\right) + p\left(u_k = +1\right) = 1, \tag{11}$$

$$L_a\left(u_k\right) = \log\left(\frac{p\left(u_k = +1\right)}{p\left(u_k = -1\right)}\right), \tag{12}$$

$p(u_k)$ can be calculated from formulas (11) and (12), as follows:

$$\begin{cases} p\left(u_k = +1\right) = \dfrac{\exp\left(L_a\left(u_k\right)\right)}{1 + \exp\left(L_a\left(u_k\right)\right)} \\ p\left(u_k = -1\right) = \dfrac{1}{1 + \exp\left(L_a\left(u_k\right)\right)} \end{cases}. \tag{13}$$

Substituting formulas (10) and (13) into formula (9), the calculation formula of branch metric can be obtained as follows:

$$\gamma_k\left(c_k^u, c_k^p\right) = \begin{cases} \dfrac{1}{\sqrt{2\pi}\,\sigma} \exp\left[-\dfrac{\left(y_k^u - c_k^u\right)^2 + \left(y_k^p - c_k^p\right)^2}{2\sigma^2}\right] \cdot \dfrac{\exp\left(L_a\left(u_k\right)\right)}{1 + \exp\left(L_a\left(u_k\right)\right)} & u_k = +1 \\ \dfrac{1}{\sqrt{2\pi}\,\sigma} \exp\left[-\dfrac{\left(y_k^u - c_k^u\right)^2 + \left(y_k^p - c_k^p\right)^2}{2\sigma^2}\right] \cdot \dfrac{1}{1 + \exp\left(L_a\left(u_k\right)\right)} & u_k = -1 \end{cases}. \tag{14}$$

If it is the first component decoding of the first iteration, let the initial value of the prior information be 0. In the subsequent component decoding, the value of the prior information is the value of the extrinsic information L_e obtained by the previous component decoding after interleaving and deinterleaving. Among them, the external information $L_e(u_k)$ can be calculated by the following formula:

$$L_e(u_k) = L(u_k) - \frac{2}{\sigma^2} y_k^u - L_a(u_k). \tag{15}$$

In engineering applications, the MAP algorithm is prone to numerical instability. In order to solve this problem, it is necessary to normalize $\alpha_k(s)$ and $\beta_k(s)$ to ensure that $\alpha_k(s)$ and $\beta_k(s)$ satisfy the following formula, respectively:

$$\sum_{s=0}^{2^v-1} \alpha_k(s) = 1, \quad \sum_{s=0}^{2^v-1} \beta_k(s) = 1. \tag{16}$$

The Log-MAP decoding algorithm is also known as the MAP algorithm in the logarithmic domain. By taking the logarithm, the algorithm converts a large number of multiplication and division operations in the MAP algorithm into the corresponding addition and subtraction operations, which greatly simplifies the operation. In the Log-MAP algorithm, three new probability values are introduced as follows:

$$\begin{aligned} \widetilde{\alpha}_k(s) &= \log(\alpha_k(s)) \\ \widetilde{\gamma}_k(s', s) &= \log(\gamma_k(s', s)) \\ \widetilde{\beta}_k(s) &= \log(\beta_k(s)). \end{aligned} \tag{17}$$

According to the derivation in the MAP algorithm, the calculation of the forward state metric $\widetilde{\alpha}_k(s)$ in the Log-MAP algorithm can be expressed as

$$\widetilde{\alpha}_k(s) = \max_{s'}^{*} \left(\widetilde{\alpha}_{k-1}(s') + \widetilde{\gamma}_k(s', s)\right). \tag{18}$$

Among them, there are

$$\max^{*}(x, y) = \log(e^x + e^y) = \max(x, y) + \ln\left(1 + e^{-|x-y|}\right). \tag{19}$$

The calculation of the backward state metric $\widetilde{\beta}_{k-1}(s')$ can be expressed as

$$\widetilde{\beta}_{k-1}(s') = \max_{s}^{*} \left(\widetilde{\beta}_k(s) + \widetilde{\gamma}_k(s', s)\right). \tag{20}$$

The initial value of the state metric is

$$\widetilde{\alpha}_0(s) = \begin{cases} 0 & s = 0 \\ -\infty & s \neq 0 \end{cases}, \widetilde{\beta}_{N+v}(s) = \begin{cases} 0 & s = 0 \\ -\infty & s \neq 0 \end{cases}. \tag{21}$$

The computation of the branch metric $\widetilde{\gamma}_k(s', s)$ can be expressed as

$$\widetilde{\gamma}_k(s', s) = \begin{cases} -\dfrac{\left(y_k^u - c_k^u\right)^2 + \left(y_k^p - c_k^p\right)^2}{2\sigma^2} + L_a(u_k) - \log(1 + \exp(L_a(u_k))) & u_k = +1 \\ -\dfrac{\left(y_k^u - c_k^u\right)^2 + \left(y_k^p - c_k^p\right)^2}{2\sigma^2} - \log(1 + \exp(L_a(u_k))) & u_k = -1 \end{cases}. \tag{22}$$

The calculation of the log-likelihood ratio $L(u_k)$ can be expressed as

$$\begin{aligned} L(u_k) = {} & \max_{U+}^{*} \left[\widetilde{\alpha}_{k-1}(s') + \widetilde{\gamma}_k(s', s) + \widetilde{\beta}_k(s)\right] \\ & - \max_{U-}^{*} \left[\widetilde{\alpha}_{k-1}(s') + \widetilde{\gamma}_k(s', s) + \widetilde{\beta}_k(s)\right]. \end{aligned} \tag{23}$$

The calculation of external information $L_e(u_k)$ can be expressed as

$$L_e(u_k) = L(u_k) - \frac{2}{\sigma^2} y_k^u - L_a(u_k). \tag{24}$$

There are a large number of $\max^{*}(.)$ operations in the Log-MAP algorithm, which includes exponential and logarithmic operations and still has a very large computational complexity. In order to further simplify the operation, the logarithmic operation $\ln(1 + e^{-|x-y|})$ term in the $\max^{*}(.)$ operation is ignored, which is called the Max-Log-MAP decoding algorithm. In the Max-Log-MAP algorithm, there are only addition and subtraction operations. Compared with the Log-MAP algorithm, the decoding computational complexity is greatly simplified, but the performance is poor.

Generally speaking, (n, p) fixed-point processing includes three steps: absolute quantization, fixed decimal places, and fixed integer bits. Absolute quantization is to convert the real number Y into an integer Y_i for subsequent determination of binary decimal places and binary integer bits. The specific process is as follows:

$$y_i = \lfloor 2^p : y + 0.5 \rfloor. \tag{25}$$

Among them, L means round down. The processing of fixed decimal places is to shift the integer Q to the right by p bits to obtain a real number y_q including p binary decimal places; that is,

$$y_q = \frac{y_i}{2^p}. \tag{26}$$

The number of decimal places in the fixed-point data is related to the minimum resolution of the fixed-point data. The choice of the fixed-point decimal place width and its impact on the performance of bit error rate and frame error rate will be discussed in the performance simulation of this chapter. Limiting is to limit the real number y_q that exceeds

the range of (n, p) fixed-point representation, and its calculation method is

$$y_l = \begin{cases} -2^{n-p-1} + 2^{-p} & y_q \le -2^{n-p-1} \\ y_q & -2^{n-p-1} < y_q < 2^{n-p-1} \\ 2^{n-p-1} - 2^{-p} & y_q \ge 2^{n-p-1} \end{cases}. \quad (27)$$

After the fixed-point decimal bit width P is determined, the following will analyze the fixed-point integer bit width of the data to be decoded, a priori information/external information, branch metrics and state metrics, so as to determine the fixed-point mode.

We assume that under AWGN channel conditions, the BPSK debugging method is adopted, and the coded symbols received at time k can be expressed as

$$y_k^l = c_k^l + n_k^l, \ell \in \{s, p1, p2\}, \quad (28)$$

where y_k^ℓ is the data received by the decoding end, $c_k^\ell \in \{1, -1\}$ represents the coded symbol after BPSK modulation, and n_k^ℓ is a Gaussian noise whose mean variance is σ^2.

First, the fixed-point bit width of the data y_k^ℓ to be decoded needs to be determined. When selecting (n, p) fixed-point processing, the following probability y_k^ℓ should be made small enough; that is,

$$\Pr\left\{y_k^\ell \le -2^{n-p-1} + 2^{-p}\right\} + \Pr\left\{y_k^\ell \ge 2^{n-p-1} - 2^{-p}\right\} = \varepsilon. \quad (29)$$

Since the receiver does not know the codeword information of the sender, it is possible to make the sender's codeword equal to 1 and −1; that is,

$$\Pr\left\{c_k^l = 1\right\} = \Pr\left\{c_k^l = -1\right\} = \frac{1}{2}. \quad (30)$$

Therefore, there are

$$\begin{aligned} &\Pr\left\{y_k^l \le -2^{n-p-1} + 2^{-p}\right\} \\ &= \Pr\left\{y_k^l \le -2^{n-p-1} + 2^{-p}, c_k' = 1\right\} + \Pr\left\{y_k' \le -2^{n-p-1} + 2^{-p}, c_k' = -1\right\} \\ &= \Pr\left\{y_k^l \le -2^{n-p-1} + 2^{-p} | c_k^l = 1\right\}\Pr\left\{c_k^l = 1\right\} + \Pr\left\{y_k' \le -2^{n-p-1} + 2^{-p} | c_k^l = -1\right\}\Pr\left\{c_k^l = -1\right\} \\ &= \frac{1}{2}Q\left(\frac{2^{n-p-1} - 2^{-p} + 1}{\sigma}\right) + \frac{1}{2}Q\left(\frac{2^{n-p-1} - 2^{-p} - 1}{\sigma}\right). \end{aligned} \quad (31)$$

In the same way, we can get

$$\begin{aligned} \Pr\left\{y_k' \ge 2^{n-p-1} - 2^{-p}\right\} &= \frac{1}{2}Q\left(\frac{2^{n-p-1} - 2^{-p} - 1}{\sigma}\right) \\ &+ \frac{1}{2}Q\left(\frac{2^{n-p-1} - 2^{-p} + 1}{\sigma}\right). \end{aligned} \quad (32)$$

The Q-function is monotonically decreasing and decreases rapidly. In order to simplify the formula, the following two approximations are made: the one is that $2^{n-p-1} - 2^{-p} \approx 2^{n-p-1}$ and the other is that the term of $Q(2^{n-p-1} - 2^{-p} + 1/\sigma)$ in formula (31) is ignored. Substituting formulas (30) and (31) into formula (29), we get

$$\Pr\left\{y_k' \le -2^{n-p-1} + 2^{-p}\right\} + \Pr\left\{y_k' \ge 2^{n-p-1} - 2^{-p}\right\} = Q\left(\frac{2^{n-p-1} - 1}{\sigma}\right) = \varepsilon. \quad (33)$$

According to the above formula, it can be estimated that the fixed-point integer bit width $(n-p-1)$ required for the data to be decoded under the condition that the specific overflow probability is ε is

$$\begin{aligned} n - p - 1 &= \left\lceil \log_2\left\{1 + Q^{-1}(\varepsilon) \cdot \sigma\right\}\right\rceil \\ &= \left\lceil \log_2\left\{1 + Q^{-1}(\varepsilon) \cdot \sqrt{\frac{N_o}{R_c E_b}}\right\}\right\rceil, \end{aligned} \quad (34)$$

where $\lceil\ \rceil$ represents rounding up, and $Q^{-1}(\cdot)$ represents the inverse function of the $Q(\cdot)$ function, which can usually be determined by looking up the table. Obviously, for a specific coding scheme and a set signal-to-noise ratio $(E_b/\sigma^2)_{dB}$ interval (often corresponding to a specific reliability performance requirement), the fixed-point integer bit width required for the data to be decoded in the fixed-point decoding algorithm can be calculated by formula (34).

Then, as the prior information for subsequent component decoding, the prior information also approximately obeys the Gaussian distribution; that is, $L_a \propto N(\mu_{L_a}, \sigma_{L_a}^2)$, and $\mu_{L_a} = \mu_{L_e}, \sigma_{L_a}^2 = \sigma_{L_e}^2$. Similar analysis methods can be used to determine the fixed-point way of extrinsic information and prior information. The fixed-point method for

analyzing prior information satisfies the following relationship:

$$\begin{aligned}&\Pr\left\{L_a \le -2^{n_{L_e}-p-1}+2^{-p}\right\}+\Pr\left\{L_a \ge 2^{n_{L_0}-p-1}-2^{-p}\right\}=\varepsilon\\&\Rightarrow Q\left(\frac{2^{n_{b_b}-p-1}-2^{-p}+\mu_{L_o}}{\sigma_{L_e}}\right)+Q\left(\frac{2^{n_{L_b-p-1}}-2^{-p}-\mu_{L_e}}{\sigma_{L_e}}\right)=\varepsilon\\&\Rightarrow Q\left(\frac{2^{n_{b_e}-p-1}-\mu_{L_e}}{\sigma_{L_e}}\right)=\varepsilon.\end{aligned} \tag{35}$$

According to the above formula, it can be estimated that under the condition of a specific overflow probability ε, the fixed-point integer bit width $(n_{L_e}-p-1)$ required by the prior information and the extrinsic information is

$$n_{L_a}-p-1=\left[\log_2\left(\mu_{L_a}+Q^{-1}(\varepsilon)\sigma_{L_e}\right)\right]. \tag{36}$$

Among them, the calculation methods of μ_{L_a} and $\sigma^2_{L_a}$ will be introduced in detail later.

The branch metric data bit width is determined.

In the fixed-point decoding algorithm, formula (22) can be simplified as the following formula:

$$\gamma_k(s',s)=y_k^s\cdot z_k^s+y_k^p\cdot z_k^p+\frac{1}{2}\cdot z_k^s\cdot L_{a,k}. \tag{37}$$

Substituting formula (28) into the above formula, we can get

$$\gamma_k(s',s)=z_k^s\cdot c_k^s+z_k^p\cdot c_k^p+z_k^s\cdot n_k^s+z_k^p\cdot n_k^p+\frac{1}{2}\cdot z_k^s\cdot L_{a,k}. \tag{38}$$

Among them, $z_k^s, z_k^p, c_k^s, c_k^p \in \{1,-1\}$, $n_k^s, n_k^p \sim N(0,\sigma^2)$, $L_{a,k} \sim N(\mu_{L_a},\sigma^2_{L_a})$, it can be obtained that the branch metric obeys the Gaussian distribution, as shown in the following formula:

$$\gamma_k(s',s)\propto N\left(z_k^s\cdot c_k^s+z_k^p\cdot c_k^p+\frac{1}{2}z_k^s\cdot\mu_{L_e},2\sigma^2+\frac{1}{4}\sigma^2_{L_a}\right). \tag{39}$$

It can be seen from the above formula that if the branch metric is fixed-point processing, the overflow probability ε should be made small enough; that is,

$$\Pr\left\{\gamma_k \le -2^{n-p-1}+2^{-p}\right\}+\Pr\left\{\gamma_k \ge 2^{n-p-1}-2^{-p}\right\}=\varepsilon. \tag{40}$$

Different values of (z_k^s, z_k^p) and its relationship with (c_k^s, c_k^p) need to be considered in the calculation of the analysis branch metric. $\gamma_k(s',s)$ can also be represented by $\gamma_k(z_k^s, z_k^p)$, and the corresponding probability can be approximated as

$$\begin{aligned}\Pr\left\{\gamma_k\left(z_k^k,z_k^p\right)\le -2^{n-p-1}+2^{-p}\right\}&=\Pr\left\{\gamma_k\left(z_k^s,z_k^p\right)\le -2^{n-p-1}+2^{-p}|z_k^s=1,z_k^p=1\right\}\cdot\Pr\left\{z_k^s=1,z_k^p=1\right\}\\&+\Pr\left\{\gamma_k\left(z_k^s,z_k^p\right)\le -2^{n-p-1}+2^{-p}|z_k^s=-1,z_k^p=1\right\}\cdot\Pr\left\{z_k^s=-1,z_k^p=1\right\}\\&+\Pr\left\{\gamma_k\left(z_k^s,z_k^p\right)\le -2^{n-p-1}+2^{-p}|z_k^s=-1,z_k^p=-1\right\}\cdot\Pr\left\{z_k^s=-1,z_k^p=-1\right\}\\&+\Pr\left\{\gamma_k\left(z_k^s,z_k^p\right)\le -2^{n-p-1}+2^{-p}|z_k^s=1,z_k^p=-1\right\}\cdot\Pr\left\{z_k^s=1,z_k^p=-1\right\}\\&=\frac{1}{4}\left[\begin{array}{c}Q\left(\frac{2^{n-p-1}-2^{-p}+\left(x_k^s+x_k^p+0.5\mu_{L_o}\right)}{\sqrt{2\sigma^2+0.25\sigma^2_{L_0}}}\right)+Q\left(\frac{2^{n-p-1}-2^{-p}+\left(x_k^s-x_k^p+0.5\mu_{L_o}\right)}{\sqrt{2\sigma^2+0.25\sigma^2_{L_e}}}\right)\\+Q\left(\frac{2^{n-p-1}-2^{-p}+\left(-x_k^2+x_k^p-0.5\mu_{L_0}\right)}{\sqrt{2\sigma^2+0.25\sigma^2_{L_0}}}\right)+Q\left(\frac{2^{n-p-1}-2^{-p}+\left(-x_k^s-x_k^p-0.5\mu_{L_k}\right)}{\sqrt{2\sigma^2+0.25\sigma^2_{L_0}}}\right)\end{array}\right]\\&\approx\frac{1}{4}Q\left(\frac{2^{n-p-1}-\left(\left|x_k^2+0.5\mu_{L_e}\right|+\left|x_k^p\right|\right)}{\sqrt{2\sigma^2+0.25\sigma^2_{L_k}}}\right)\approx\frac{1}{4}Q\left(\frac{2^{n-p-1}-\left(\left|x_k^2\right|+\left|0.5\mu_{L_0}\right|+\left|x_k^p\right|\right)}{\sqrt{2\sigma^2+0.25\sigma^2_{L_0}}}\right)\\&=\frac{1}{4}Q\left(\frac{2^{n-\rho-1}-\left(2+0.5\mu_{L_e}\right)}{\sqrt{2\sigma^2+0.25\sigma^2_{L_e}}}\right).\end{aligned} \tag{41}$$

In the same way, we can get

$$\Pr\left\{\gamma_k\left(z_k^s, z_k^p\right) \geq 2^{n-p-1} - 2^{-p}\right\} = \frac{1}{4}Q\left(\frac{2^{n-p-1} - \left(2 + 0.5\mu_{L_e}\right)}{\sqrt{2\sigma^2 + 0.25\sigma_{L_e}^2}}\right). \quad (42)$$

Substitute formulas (41) and (42) into formula (40), we can get

$$\Pr\left\{\gamma_k \leq -2^{n-p-1} + 2^{-p}\right\} + \Pr\left\{\gamma_k \geq 2^{n-p-1} - 2^{-p}\right\} = \frac{1}{2}Q\left(\frac{2^{n-p-1} - \left(2 + 0.5\mu_{L_o}\right)}{\sqrt{2\sigma^2 + 0.25\sigma_{L_o}^2}}\right) = \varepsilon. \quad (43)$$

According to the above formula, it can be estimated that under the condition of a specific overflow probability ε, the fixed-point integer bit width $(n_\gamma - p - 1)$ required by the branch metric is

$$n_\gamma - p - 1 = \left\lceil \log_2\left\{2 + 0.5\mu_{L_a} + Q^{-1}(2\varepsilon) \cdot \sqrt{2\sigma^2 + 0.25\sigma_{L_a}^2}\right\}\right\rceil. \quad (44)$$

The state metric data bit width is determined.

According to formulas (18) and (20), the state metric is obtained by adding two numbers, which must satisfy $n_s > n_y$, where n_s represents the fixed-point total bit width of the state metric. Since the state metric α (or β) is calculated recursively, its value will continue to increase during the recursive calculation process. In order to prevent fixed-point overflow in the recursive process, α (or β) needs to be normalized. The selection and processing method of normalization will be analyzed in detail in the next section, and the specific integer bit width of the state metric will be determined.

In floating-point computing, the commonly used state metric normalization methods are as follows:

$$\tilde{\alpha}_k(s) = \alpha_k(s) - \max_{s'}\left[\alpha_k(s')\right], \tilde{\beta}_k(s) = \beta_k(s) - \max_{s'}\left[\beta_k(s')\right]. \quad (45)$$

However, the normalization method of the above formula will bring additional calculation delay, and there is no guarantee that the calculation overflow will not occur when the data bit width is limited. Therefore, it cannot be directly extended to the fixed-point decoding algorithm.

In the recursive calculation of state metrics in turbo decoding, a feasible normalization scheme is to judge the values of all state metrics $\alpha_k(s')$ and $\beta_{k+1}(s)$ at the previous moment before recursive calculation. Normalization is performed on recursive computations in cases where computation overflow is possible. The above normalization scheme can be expressed by the following formulas:

$$\alpha_{k+1}(s) = \begin{cases} \max_{s'}\left[\alpha_k(s') + \gamma_{k+1}(s', s)\right] & \text{if } \forall s', \alpha_k(s') < \alpha_{\max} - \omega \\ \max_{s'}\left[\alpha_k(s') + \gamma_{k+1}(s', s) - \omega\right] & \text{if } \exists s', \alpha_k(s') \geq \alpha_{\max} - \omega \end{cases}, \quad (46)$$

$$\beta_k(s') = \begin{cases} \max_{s}\left[\beta_{k+1}(s) + \gamma_{k+1}(s', s)\right] & \text{if } \forall s, \beta_{k+1}(s) < \beta_{\max} - \omega \\ \max_{s}\left[\beta_{k+1}(s) + \gamma_{k+1}(s', s) - \omega\right] & \text{if } \exists s, \beta_{k+1}(s) \geq \beta_{\max} - \omega. \end{cases}, \quad (47)$$

where $\alpha_{\max}$ and $\beta_{\max}$ are the maximum values of the state metric in the fixed-point mode. If the fixed-point mode of the state metric is (n_s, p), then $\alpha_{\max} = \beta_{\max} = 2^{n_s - p - 1} - 2^{-p}$. ω is the preset normalization constant during normalization processing. A simple method is to measure the maximum value of the fixed-point (n_γ, p) manner according to the aforementioned branch metric; that is, $\omega = \gamma_{\max}$. In this way, if some values of the state metrics $\alpha_k(s')$ and $\beta_{k+1}(s)$ at the previous moment exceed the decision threshold $\alpha_{\max} - \omega$ or $\beta_{\max} - \omega$, the aforementioned normalization operation is performed, thereby ensuring that the calculation of the state metrics will not occur calculation overflow. The normalized threshold value ω is required, and the branch metric, a priori information, and the fixed-point mode of the data to be decoded are calculated.

Based on random statistical analysis, an effective method for calculating the Gaussian distribution of prior information/extrinsic information in the iterative process is presented. The calculation formula is as follows:

$$L_e^t = -\ln\left(\exp\left(-L_+\right) + \exp\left(-L_-\right)\right), \quad (48)$$

where the variables L_+ and L_- can be calculated iteratively as follows:

$$\begin{aligned} L_\pm &= \rho_\pm + L_\pm^{(1)} \\ L_\pm^{(i)} &= \delta_\pm^{(i)} - \ln\left(\exp\left(-\eta_\pm^{(i)}\right) + \exp\left(-L_\pm^{(i+1)}\right)\right) \quad i = 1, 2, \ldots, M-1 \\ L_\pm^{(M)} &= \delta_\pm^{(M)} + \eta_\pm^{(M)}, \end{aligned} \quad (49)$$

where $\rho_\pm, \delta_\pm^{(i)}, \eta_\pm^{(i)}$ are independent Gaussian distributed random variables, and their probability distribution characteristics are as follows:

$$\begin{aligned} \rho_\pm &\sim N\left(\mu_r, \sigma_r^2\right) \\ \delta_\pm^{(i)} &\sim N\left((w_0 - 2)\mu_r, (w_0 - 2)\sigma_r^2\right) \\ \eta_\pm^{(i)} &\sim N\left(2\mu_r + \mu_a, 2\sigma_r^2 + \sigma_a^2\right), \end{aligned} \quad (50)$$

where μ_r and σ_r^2 are the mean and variance of the data y_k^ℓ to be decoded. μ_a and σ_a^2 are the mean sum and variance of the current iterative decoding prior information. When $t = 1$, the initial value of the prior information is 0; that is, $\mu_a = \sigma_a^2 = 0$. When $t > 1$, the mean and variance of the prior information are set to the mean and variance of the external information in $(t-1)$ iterations of decoding, respectively. M is the number of sequences with a code weight of 2. In the paper, $M = 2, w_0$ is the minimum codeword weight corresponding to the input sequence of code weight 2, when the component encoder is (1, 15/13), $w_0 = 6$.

$$\varepsilon[\exp(X_i)] = \exp\left(\frac{2\mu_i + \sigma_i^2}{2}\right) \quad i = 1, 2$$

$$m_1 = \varepsilon[\exp(Z)] \sum_{i=1}^{2} \exp\left(\frac{2\mu_i + \sigma_i^2}{2}\right)$$

$$m_2 = \varepsilon\left[(\exp(Z))^2\right] = \sum_{i=1}^{n} \exp\left(2\mu_i + 2\sigma_i^2\right) + 2\sum_{i=1}^{n}\sum_{j=i+1}^{n} \exp\left(\mu_i + \mu_j + \frac{\sigma_i^2 + \sigma_j^2 + 2r_{ij}\sigma_i\sigma_j}{2}\right) \tag{53}$$

$$= \exp\left(2\mu_1 + 2\sigma_1^2\right) + \exp\left(2\mu_2 + 2\sigma_2^2\right) + 2\exp\left(\mu_1 + \mu_2 + \frac{\sigma_1^2 + \sigma_2^2}{2}\right).$$

The logarithmic distributions of the exponential sums involved in formulas (48) and (49) can be approximated by the Fenton–Wilkinson (FW) method, as shown in formulas (51) and (52). The mean and variance of the outer information L_e^t/a priori information L_a^{t+1} of the t-th iteration can be calculated by formulas (48), (49), and (52).

$$Z = \ln(\exp(X_1) + \exp(X_2)), X_1 - N\left(\mu_1, \sigma_1^2\right), X_2 \sim N\left(\mu_2, \sigma_2^2\right), \tag{51}$$

$$Z - N\left(\mu_z, \sigma_z^2\right) \begin{cases} \mu_Z = 2\ln m_1 - \frac{1}{2}\ln m_2 \\ \sigma_Z^2 = \ln m_2 - 2\ln m_1 \end{cases}. \tag{52}$$

Among them, there are

4. Path Selection Strategy of Communication Network Based on Graph Convolutional Neural Network

In the underlying architecture of the system, a set of flow control group policies is implemented through the SDN-based network flow control module, so that the system can adjust the network state according to the analysis results of the network situation information, and control and migrate the flow in the entire network. The system architecture diagram is shown in Figure 2.

The network architecture diagram of the scheme described in this paper is shown in Figure 3. In the entire network, the core gateway is used to control traffic and access to other subnets and also acts as a reverse proxy when the external network accesses the internal network server.

The technical scheme of the flow control module implemented based on the SDN idea adopted in this system is shown in Figure 4. In this technical solution, the modules can be divided into three layers, namely the application layer, the control layer, and the data forwarding layer.

The depth of the graph neural network in this paper is set to 2 layers. The calculation process of the graph neural network is shown in Figure 5. After each layer of network outputs the sample feature matrix, the matrix is reused to calculate its adjacency matrix; that is, the graph structure is updated. Finally, the feature vector of the sample to be classified in the graph structure is taken out, and the softmax function is used to map it to the final classification result.

Figure 6 shows the network structure of the denoising convolutional autoencoder. The amount of feature map parameters decreases layer by layer during the encoding process of the convolutional autoencoder. In order to prevent the loss of too much useful information in the encoding process, skip connections are added between the corresponding encoding and decoding layers when constructing the denoising convolutional autoencoder. The skip connection directly introduces the information of the coding layer into the corresponding deep decoding layer, and the model selects important noise information by adjusting the parameter weights, thereby reconstructing the noise of the signal.

This paper takes the IEEE802.16j/m series of standards and drafts as the platform and takes the multihop relay cellular network based on OFMDA technology as the research object to study its path selection algorithm. In addition, a system performance simulation platform of multihop relay cellular network is built, and the corresponding performance analysis of the proposed path selection algorithm is carried out. The typical multihop relay cellular network scenario based on IEEE802.16j/m series standards is shown in Figure 7.

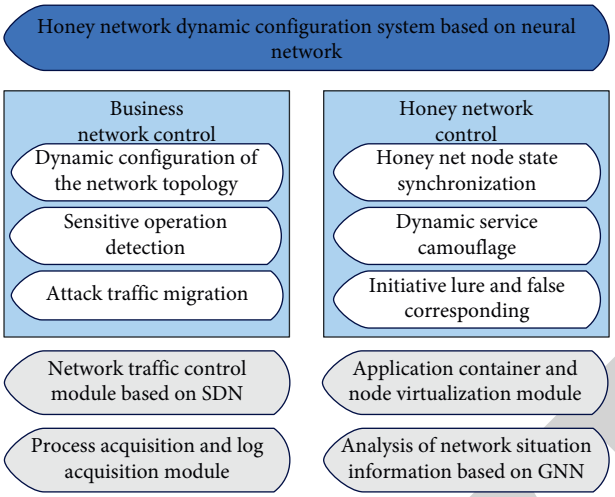


Figure 2: System architecture diagram.

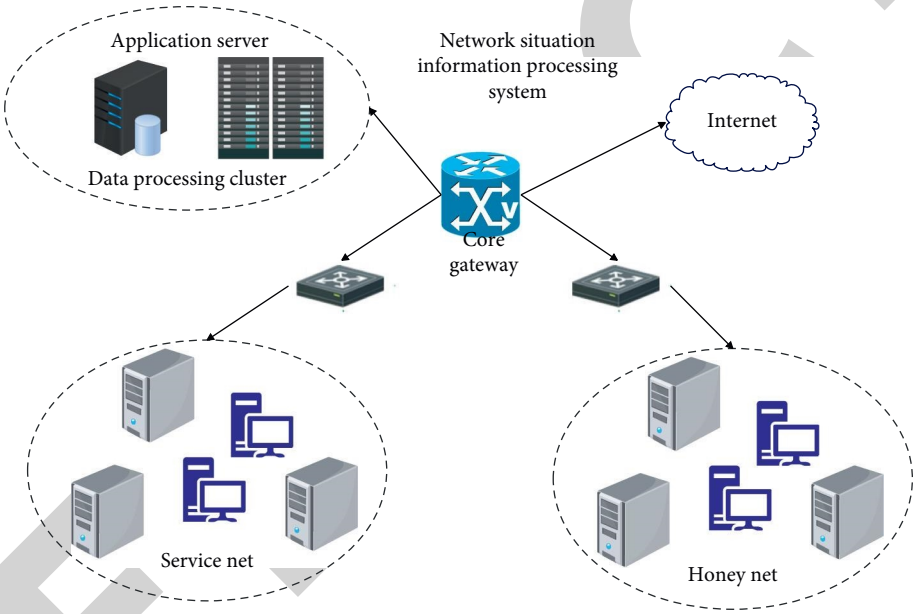


Figure 3: Network architecture diagram.

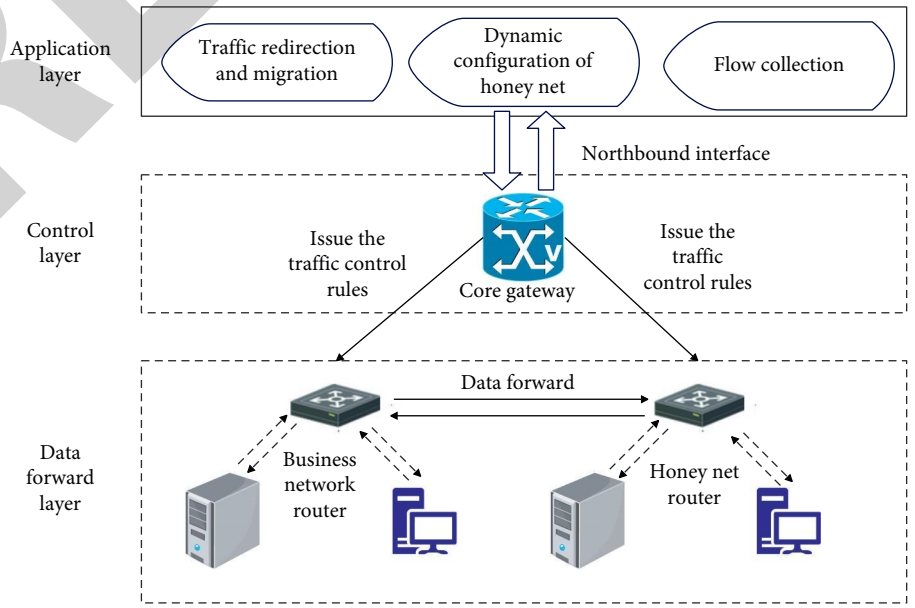


Figure 4: Technical scheme of flow control module.

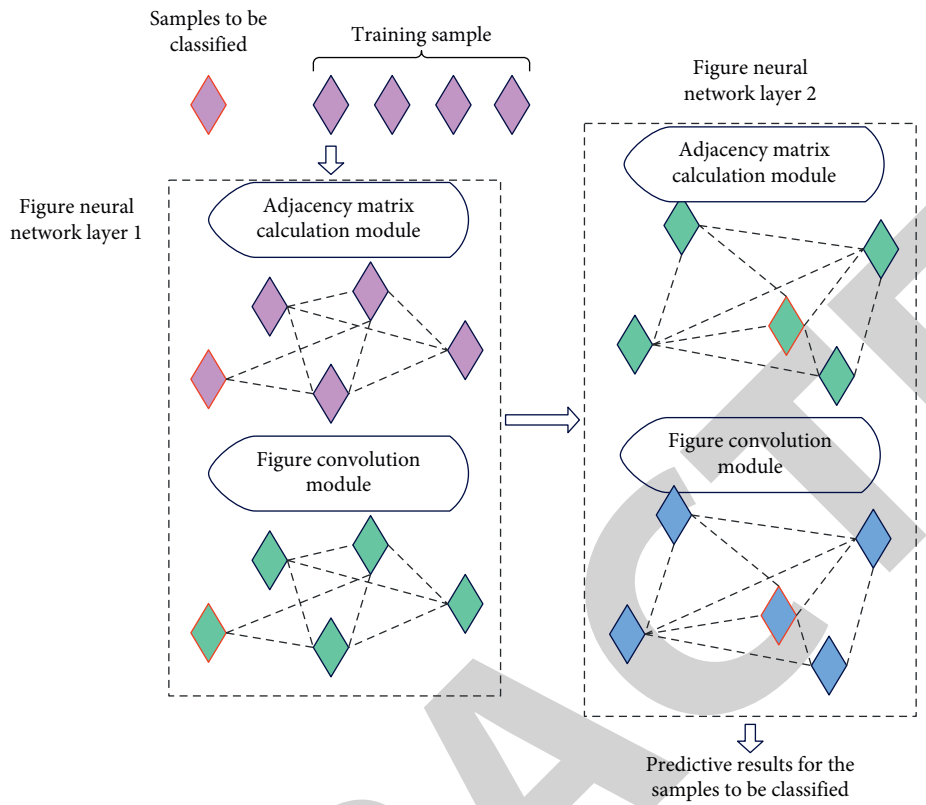


Figure 5: The calculation flow of the neural network.

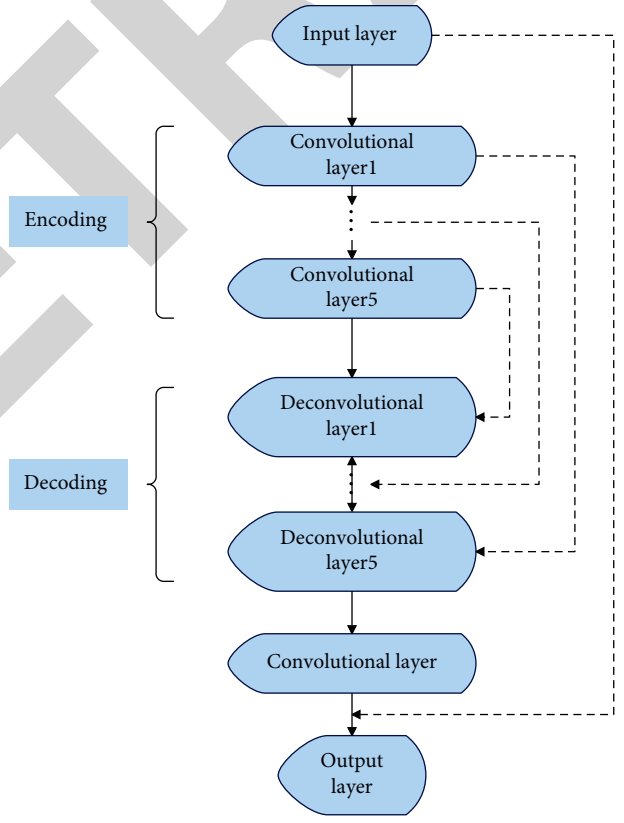


Figure 6: Network structure of denoising convolutional autoencoder.

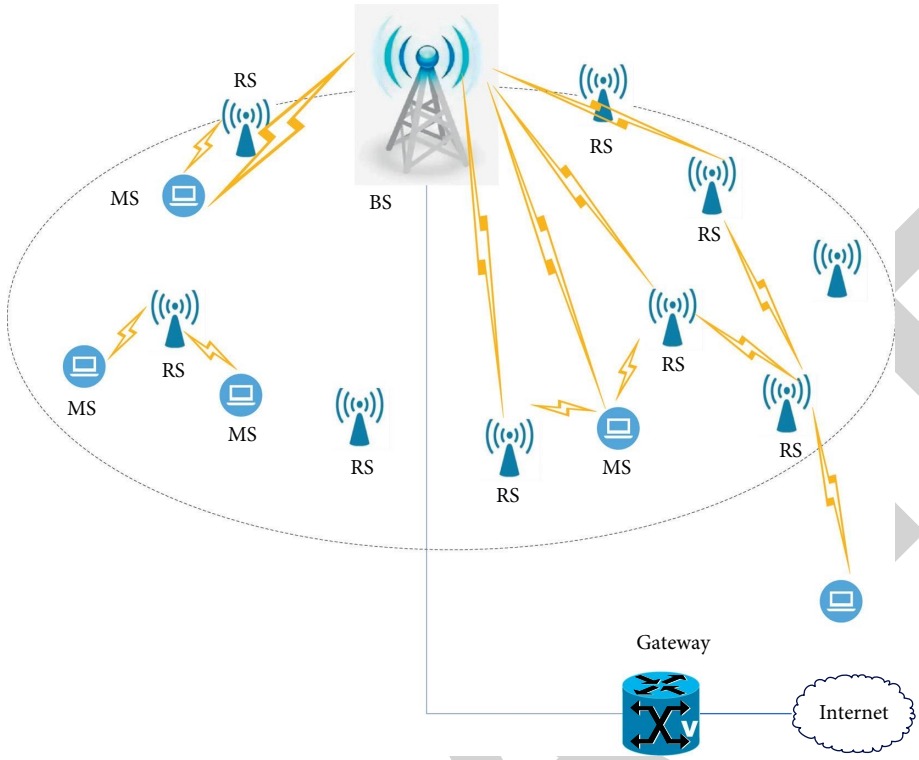


Figure 7: Multihop relay cellular network road scenario.

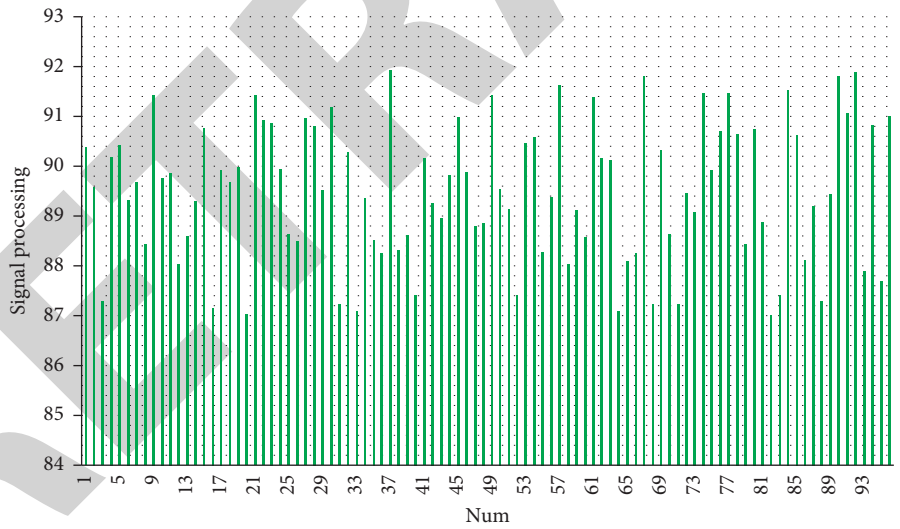


Figure 8: Signal processing effect of communication network path selection system based on graph convolutional neural network.

Based on the scene set in Figure 7, the system model of this paper is constructed and simulated. Moreover, this paper explores the path selection effect of communication network based on graph convolutional neural network. The model is simulated by Matlab, the effect of signal processing and communication path selection is counted in this paper, and the results shown in Figures 8 and 9 are obtained.

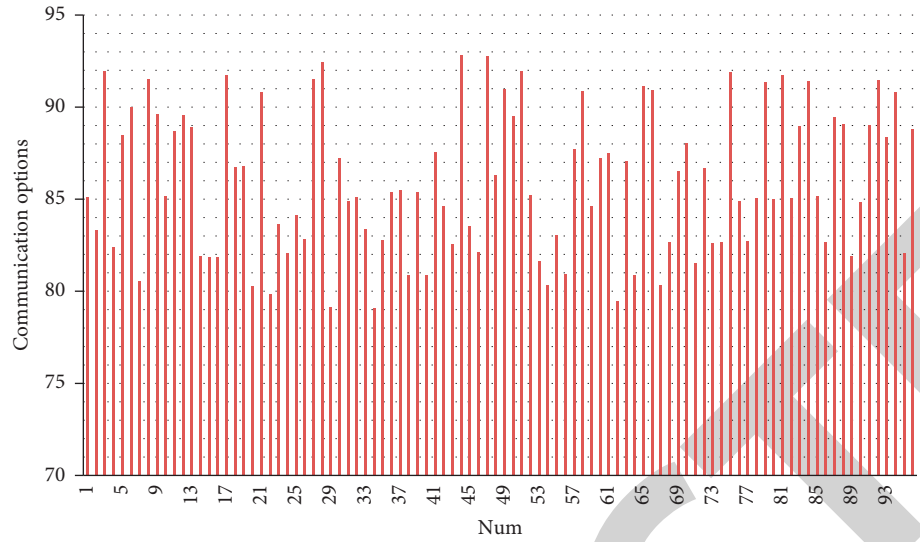


Figure 9: Path selection effect of communication network path selection system based on graph convolutional neural network.

It can be seen from the above research that the communication network path selection system based on graph convolutional neural network proposed in this paper can effectively improve the effect of multicommunication path selection.

5. Conclusion

The absence of a complete link between communicating nodes does not mean that the pair of nodes cannot communicate. Opportunistic routing can select the node closest to the target node to forward data, and adopts the "store-carry-forward" communication strategy. By utilizing the movement of nodes, the nodes can be brought into the mutual communication range to realize communication. This opportunistic routing mechanism can improve the efficiency, throughput and reliability of the network. A graph neural network is a mobile self-organizing network that uses an opportunistic routing mechanism. Moreover, the feature of opportunistic networks that do not require full network connectivity is more in line with the actual needs of ad hoc networks, so it has become a research hotspot in many fields in recent years. This paper combines the graph convolutional neural network to formulate the communication network path selection strategy and constructs an intelligent system. The research shows that the communication network path selection system based on graph convolutional neural network proposed in this paper can effectively improve the effect of multicommunication path selection.

Data Availability

The labeled dataset used to support the findings of this study is available from the corresponding author upon request.

Conflicts of Interest

The author declares no conflicts of interest.

Acknowledgments

This study was sponsored by Henan Finance University.

References

[1] J. Pan, Q. Xie, H. Chiang et al., ""From the nature for the nature": an eco-friendly antifouling coating consisting of poly(lactic acid)-based polyurethane and natural antifoulant," *ACS Sustainable Chemistry & Engineering*, vol. 8, no. 3, pp. 1671–1678, 2019.

[2] B. Behroozpour, P. A. M. Sandborn, M. C. Wu, and B. E. Boser, "Lidar system Architectures and circuits," *IEEE Communications Magazine*, vol. 55, no. 10, pp. 135–142, 2017.

[3] J. Barowski, M. Zimmermanns, and I. Rolfes, "Millimeter-Wave characterization of dielectric materials using calibrated FMCW transceivers," *IEEE Transactions on Microwave Theory and Techniques*, vol. 66, no. 8, pp. 3683–3689, 2018.

[4] Y. Jiang, S. Karpf, and B. Jalali, "Time-stretch LiDAR as a spectrally scanned time-of-flight ranging camera," *Nature Photonics*, vol. 14, no. 1, pp. 14–18, 2020.

[5] L. J. Xu, X. Lin, Q. He, M. Worku, and B. Ma, "Highly efficient eco-friendly X-ray scintillators based on an organic manganese halide[J]," *Nature Communications*, vol. 11, no. 1, pp. 1–7, 2020.

[6] Q. Y. Cheng, X. L. Zhao, Y. X. Weng, Y. D. Li, and J. B. Zeng, "Fully sustainable, nanoparticle-free, fluorine-free, and robust superhydrophobic cotton fabric fabricated via an eco-friendly method for efficient oil/water separation," *ACS Sustainable Chemistry & Engineering*, vol. 7, no. 18, pp. 15696–15705, 2019.

[7] N. Maring, P. Farrera, K. Kutluer, M. Mazzera, G. Heinze, and H. de Riedmatten, "Photonic quantum state transfer between a cold atomic gas and a crystal," *Nature*, vol. 551, no. 7681, pp. 485–488, 2017.

[8] H. Mohapatra and A. K. Rath, "Detection and avoidance of water loss through municipality taps in India by using smart taps and ICT," *IET Wireless Sensor Systems*, vol. 9, no. 6, pp. 447–457, 2019.

Hindawi
Security and Communication Networks
Volume 2024, Article ID 9818032, 1 page
https://doi.org/10.1155/2024/9818032

Retraction

Retracted: Enterprise Financial Risk Analysis Based on Improved Model *C*-Means Clustering Algorithm

Security and Communication Networks

Received 8 January 2024; Accepted 8 January 2024; Published 9 January 2024

This article has been retracted by Hindawi following an investigation undertaken by the publisher [1]. This investigation has uncovered evidence of one or more of the following indicators of systematic manipulation of the publication process:

(1) Discrepancies in scope

(2) Discrepancies in the description of the research reported

(3) Discrepancies between the availability of data and the research described

(4) Inappropriate citations

(5) Incoherent, meaningless and/or irrelevant content included in the article

(6) Manipulated or compromised peer review

The presence of these indicators undermines our confidence in the integrity of the article's content and we cannot, therefore, vouch for its reliability. Please note that this notice is intended solely to alert readers that the content of this article is unreliable. We have not investigated whether authors were aware of or involved in the systematic manipulation of the publication process.

Wiley and Hindawi regrets that the usual quality checks did not identify these issues before publication and have since put additional measures in place to safeguard research integrity.

We wish to credit our own Research Integrity and Research Publishing teams and anonymous and named external researchers and research integrity experts for contributing to this investigation.

The corresponding author, as the representative of all authors, has been given the opportunity to register their agreement or disagreement to this retraction. We have kept a record of any response received.

References

[1] J. Sun and Y. Jiao, "Enterprise Financial Risk Analysis Based on Improved Model *C*-Means Clustering Algorithm," *Security and Communication Networks*, vol. 2022, Article ID 1109813, 12 pages, 2022.

Hindawi
Security and Communication Networks
Volume 2022, Article ID 1109813, 12 pages
https://doi.org/10.1155/2022/1109813

Research Article

Enterprise Financial Risk Analysis Based on Improved Model *C*-Means Clustering Algorithm

Jia Sun[1] **and Yanrong Jiao**[2]

[1]*Department School of Finance & Economics, Chongqing City Management College, Chongqing 401331, China*
[2]*School of Construction Management, Chongqing College of Architecture and Technology, Chongqing 401331, China*

Correspondence should be addressed to Jia Sun; cswusunj@163.com

Received 16 March 2022; Revised 27 April 2022; Accepted 3 May 2022; Published 12 July 2022

Academic Editor: Zhiping Cai

As a provider of loans to SMEs, banks should prudently examine loan risks while ensuring that they provide loans to SMEs from the perspective of cooperating with policy implementation and controlling their own risks. The existing loan risk measurement tools include multiple discriminant analysis models, multiple regression models, and machine learning methods. Most machine learning methods have higher prediction accuracy than traditional models when using historical data for calculation, but the existence of problems such as overfitting seriously affects the robustness of machine learning methods. A similar method is introduced into the loan default risk prediction of SMEs, and the mean clustering method is used to preset penalty items to reduce overfitting and high accuracy to help banks effectively identify the default probability of SMEs during the loan period. This study will use the mean clustering method to iteratively train 900,000 SME credit records published by the US Small and Medium Business Administration, with 27 dimensions of data provided by Small Business Administration (SBA) to provide partial guarantees. A regression tree evaluates the data, combining the scores of multiple regression trees to produce a final prediction of the probability of credit default on the input data. The research results show that the mean clustering method can effectively improve the prediction accuracy of traditional machine learning methods and multiple linear regression in the scenario of SME loan default prediction and reduce the overfitting and black-box properties. As a supplementary loan default risk measurement tool, it can strengthen the ability of commercial banks to control the risk of loan business and can also promote the development of small- and medium-sized enterprises and the market economy to a certain extent.

1. Introduction

The measurement and evaluation of corporate credit default probability are the key content of the Basel Accord internal rating method, and it is also one of the main independent variables of credit risk evaluation. The calculation of expected loss and value at risk according to the background and conditions of different credit applicants is the core work of commercial banks to determine capital and carry out loan business. Therefore, the accuracy of the credit default probability measurement has a significant impact on the bank's credit.

Banks can use some innovative risk prediction tools according to business characteristics, such as after recording the accuracy and error of reused historical data, or before credit business, using these tools to predict new loan needs, and then pilot departments to deploy them to other businesses after confirming the effectiveness of this method [1]. Testing and gray of these offline and online data may last for a long time. For small- and medium-sized enterprises, they should also actively cooperate with the data audit and disclosure work of banks and use the cloud platform to update and upgrade their own data statistics. In this way, with the synchronous efforts of loan demand and supply

side, we can expect the extensive and active application of innovative risk prediction method in small- and medium-sized enterprise credit [2].

At present, machine learning-based methods have a good performance in classification and prediction and have a relatively mature application framework in search, advertising, recommendation, risk control, and other scenarios [3]. Compared with traditional linear models, machine learning algorithms such as neural network and support vector machine generally have high prediction accuracy, but these traditional machine learning methods lack economic intuition and interpretability and have serious overfitting problems, which have higher risks than linear regression methods in the financial field.

New machine learning methods such as mean clustering and LightGBM released in 2016 have received extensive attention from computer academia. After improvement, these methods have become the best algorithms in current machine learning research under structured data. As for the mean clustering algorithm, the average clustering method in the loss function increases the number of tree structure complexity and L2 regular penalty term of leaf node weight, which makes the model training result more smooth. Compared with the ordinary machine learning method, the degree of overfitting is reduced, and the leaf node weight and sample division condition of each tree are highly readable, which is conducive to further test the rationality after model training. These features make the mean clustering method have a more stable performance and intuitive model results than the traditional methods, and it is more suitable for applications in such strict scenarios as credit risk control [4].

This study uses the mean clustering method to iteratively train the credit records of some guaranteed small- and medium-sized enterprises of the U.S. SME administration and the Small Business Administration (SBA) from 27 dimensions, and generate multiple regression trees that can be used to evaluate loan data, so as to generate the input data for the final prediction of credit default probability through the comprehensive multiple regression tree [5]. Using and improving the average clustering method, the performance of credit default prediction model is better than the traditional linear regression, and other nonlinear machine learning methods can provide new tools for bank risk control and improve the current work effect of credit risk assessment of commercial banks. In the rapid development of artificial intelligence and the active pursuit of the landing of the current time point, it also provides a new direction for the research and application of machine learning algorithms.

2. State of the Art

For the problem of classification prediction of credit default probability, many different methods have been developed in academia and industry, such as linear regression and generalized linear model and machine learning methods. There are also some special empirical models for the financial fields, such as Z-score methods [6]. The linear assumption of ordinary linear regression models lacks practicality in many practical scenarios, and the model accuracy is generally not high. Over the past 20 years, generalized linear models (GLMs) have been commonly used in the fields of actuarial and credit analysis. According to Nelder et al., in summary the generalized linear model is a traditional method to analyze the probability of credit default, but Chen (2020) believes that there are several limitations: 1. when the variables in the model are too large, there may be multiple collinearity resulting in model estimation distortion [7]; 2. They are incapable to use shrinkage estimation to effectively contract too many variables in the model; and 3. the assumptions and limitations of the model are still too strong compared with machine learning models, resulting in the results of generalized linear models being inferior to nonlinear models. In machine learning methods, when conducting supervised learning of historical data, random forest, support vector machine, neural network, and other algorithms have been relatively mature, and the prediction accuracy can reach 80% and 90% after jumping the whole parameters. However, machine learning methods are not completely better than GLM [8]. When the noise data are relatively high or the training data are not representative, there may be serious overfitting problems. The model performance difference between the training set and the test set is too large, which cannot be applied to the actual scene at all. For models of decision tree types, overcomplex tree structure often means overfitting, so the degree of overfitting can be suppressed to some extent, but unfortunately effective pruning strategies are also difficult to find. In addition, due to its black-box characteristics, the machine learning method is difficult to explain its parameter significance. Even if they have good accuracy in both the training set and the test set, there are certain risks when actually using it [9].

However, the significant advantages of machine learning methods in accuracy have still attracted the attention of many foreign scholars, and some scholars have already applied machine learning methods to the financial field. Xie et al. through comparison found that BP neural network (BPNN), support vector machine (SVM), and AdaBoost methods have higher prediction accuracy and relatively small variance compared with traditional GLM. According to Zhou et al., at this stage, more advanced machine learning methods such as delta clustering have also been applied in the financial field. According to Yang et al., the composite Poisson model is applied to the risk control system of insurance companies, and the cutting-edge machine learning method performs better compared with the existing methods [10]. Son reviewed the existing large number of machine learning algorithm in credit default prediction, summarized the prediction of enterprise credit default probability scenario that shows good results of machine learning algorithm, such as regression tree model, bagged algorithm, random forest, and neural network, and provided the unsupervised learning methodology applied in credit default prediction. Chen also compared the performance of the modified version of LightGBM based on the gradient lifting tree model with other traditional methods in the probability prediction of auto insurance claims and found that the accuracy and AUC indicators of LightGBM were

significantly higher than SVM, neural network, and GLM, reaching more than 90%, and also improved than the ordinary gradient lifting tree model. These literature studies show that the high accuracy of machine learning algorithms helps solve the reverse selection problem in the credit default prediction scenario [11].

On the other hand, algorithms for cluster types are developing rapidly, and Breiman proposed the concept of bagging. Bagging is a model training method, namely random sampling to train the classifier, and then, it combines the classifier into a higher accuracy classifier, such as random forest, which is a typical algorithm based on the bagging training mode. Freund et al. proposed a clustering algorithm relatively different from bagging [12]. The clustering algorithm will adjust the weight of each sample on the classifier according to the classification results of the last round. The greater the classification error rate, the greater the weight. The observation that this weight was modified was used to train the next classifier. Finally, the different classifiers were merged into the more precise classifiers [13]. Friedman also proposed the gradient rise (gradient boosting) method based on the clustering method, which focuses on reducing the loss function value of the objective function, and the reduction process is determined by the derivative of the objective function. Chen et al. (2016) further strengthened the training method of gradient rise algorithm and proposed the mean clustering method. The algorithm often achieves the classification and prediction of nearly 90% accuracy in high-quality datasets and shows higher performance than LightGBM in a large number of experiments. We can expect its performance in the risk assessment scenario [14].

Many researchers are still conservative about the application of machine learning algorithms to production in the financial sector. Comparing the application of generalized linear model, neural network, decision tree, and other algorithms in enterprise default prediction, Goyal et al. found that the neural network algorithm has the highest accuracy, but there is an obvious overfitting problem. When applying machine learning algorithms to economic and financial scenarios, Wuthrich believes that the main problem is that the extracted features lack economic intuition and low interpretability, even if the accuracy is higher than linear models, and it is still not convincing [9]. Meanwhile, according to Wuthrich et al. single-value decomposition and bottleneck network are used to extract the features and replace the features in the PCA model, which improves the interpretability of the model [15]. However, the critical value problem of how to effectively determine the prediction probability after this treatment is still pending, but in fact the mean clustering method has effectively improved the two main defects of machine learning algorithms in the financial field mentioned by these scholars: Chen et al. point out that the clustering algorithm is almost better than the ordinary gradient lifting algorithm, and the regular term in the loss function can effectively reduce the variance of the model; on the other hand, the regular term also punished the complexity of the decision tree, effectively completed the pruning work, and make the mean clustering method avoid the overfitting problem in many experiments [16]. It also retains the advantages of the gradient lifting tree algorithm: the rules of the structure of the decision tree are easy to extract, and it can also help people understand its training results through many visual analysis tools.

Based on the literature, that the cutting-edge machine learning methods have high availability of credit default risk data, and the overall effect is better than generalized linear models, SVMs, neural networks, and neural network models, which have low explanatory power [17]. Classification trees can be directly understood by us. The interpretability of the model is increased, the requirements for the dataset are lowered, and the degree of overfitting to the training data is reduced, and at the same time, the error rate is lower and the accuracy rate is higher, which is feasible in the scenario of credit default risk prediction [18].

3. Model and Data Processing

3.1. Data Description and Processing. The reasons for credit defaults of SMEs mainly include five categories, including business processes and basic conditions. The overall classification and detailed factors are shown in Figure 1. We need to evaluate the basic data of mid-performance companies in terms of these aspects.

After accessing the original data, it is necessary to clean the data according to the characteristics of the clustering algorithm. Because the basic processing of variables in the mean clustering method is discrete, and continuous variables are supported by default, a thermal code is used as a noncontinuous variable of computer recognizable variables [19]. Finally, the numerical value can be normalized again.

The specific steps are as follows: first invalid records (because the mean clustering method is sensitive to missing values, 96% of the data used in this study are complete, so they are selected to eliminate the records with missing values) are removed, all data variables are converted into standard time format, and then the variables of amount type into digital format are converted. Then, for discrete variables, one-hot coding is converted into a binary vector; i.e., for discrete variables with n different values, a binary number of length n represents each value, i-value is i-bit 1, and the remaining bit is 0. In this way, the feature number will be very sparse, to avoid being too difficult for the algorithm to identify the feature [20]. Finally, the value is normalized and gradient descent algorithm is avoided in the multidimensional plane because the variable numerical range difference is too large and difficult to find a steady drop path. At the same time, the distance between some algorithm samples is also set as the calculation reference classifier, which can speed up the calculation speed while avoiding being misled by the too large sample range. This study uses the most common normalization method, with zero mean centralization with standard deviation and mean, as shown in Figure 2.

In this study, the data quality and numerical distribution after data preprocessing were tested by variable correlation. From Figures 3 and 4, in addition to the label, there are many variables whose distribution is uneven and does not conform

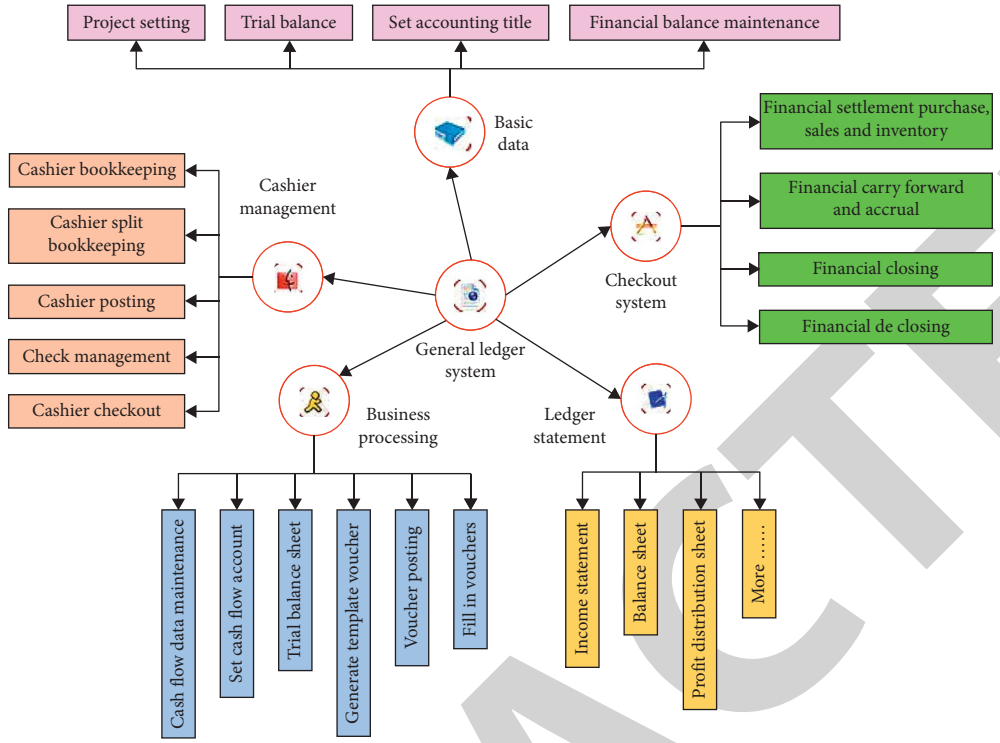


Figure 1: Overall classification and detailed factors for SMEs.

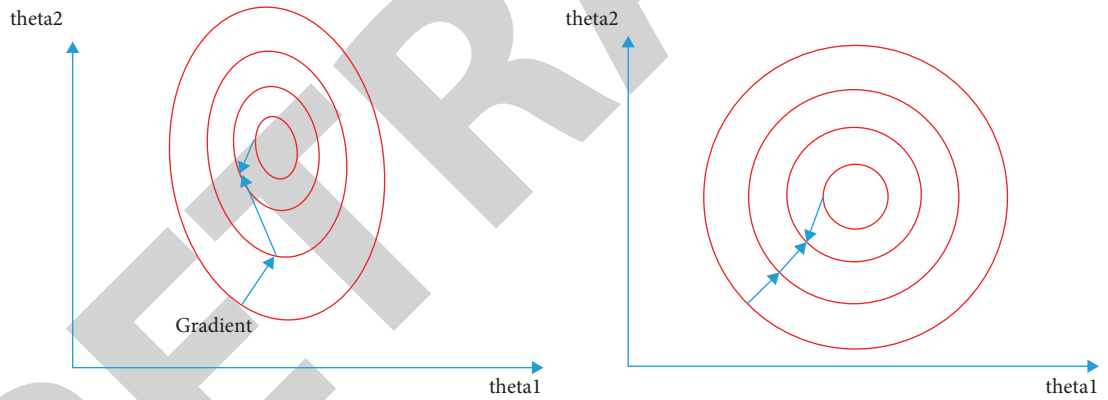


Figure 2: Effect of normalization on the model gradient descent process.

to the normal distribution, which is very unfriendly to many models, especially the linear regression model. For these biased distribution variables, this paper adopts the method of data processing to eliminate them. As can be seen from the correlation coefficient matrix (Figure 5), most variables are very weak (regional information is excluded from the variables, because there is too high correlation between this information, which may lead to some of the models used in this study). It can be judged that the now processed data quality can be applied to the empirical tests of multiple models.

3.2. Model Principle and Settings. The idea of clustering is to generate K regression trees through a certain training method, and then, the scores of these regression trees are added up to get an input final score. Under a certain weight value, the input samples are classified. If there are n samples, there are m features in total. q represents the structure of a regression tree, that is, the mapping of the sample to leaf nodes. T is the number of leaves of this tree.

$$\hat{y}_i = \phi(x_i) = \sum_{k=1}^{K} fk(x_i), f_k \in \Upsilon, \quad \text{where } T\Upsilon = \{f(x) = \omega_{q(x)}\}(q: R^m \longrightarrow T, \omega \in R^T). \tag{1}$$

We hope to find the optimal regression tree structure through a method, so we make the following constraints on the function in the above formula, so that it has the loss function L of regular penalty term. In addition, by minimizing the value of the loss function, the error between the predicted value and the actual value of the sample can be

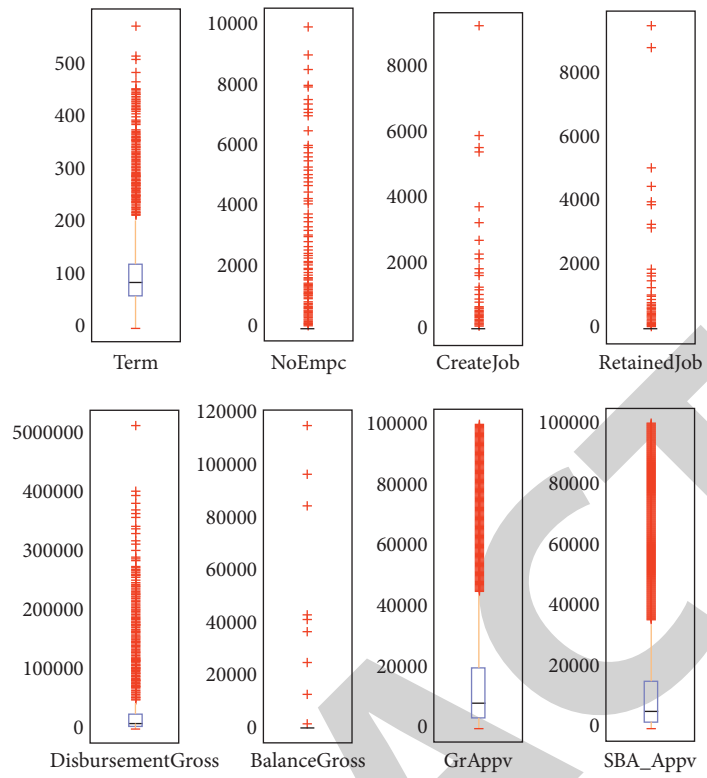


Figure 3: Box plots and violin plots of partial data distribution.

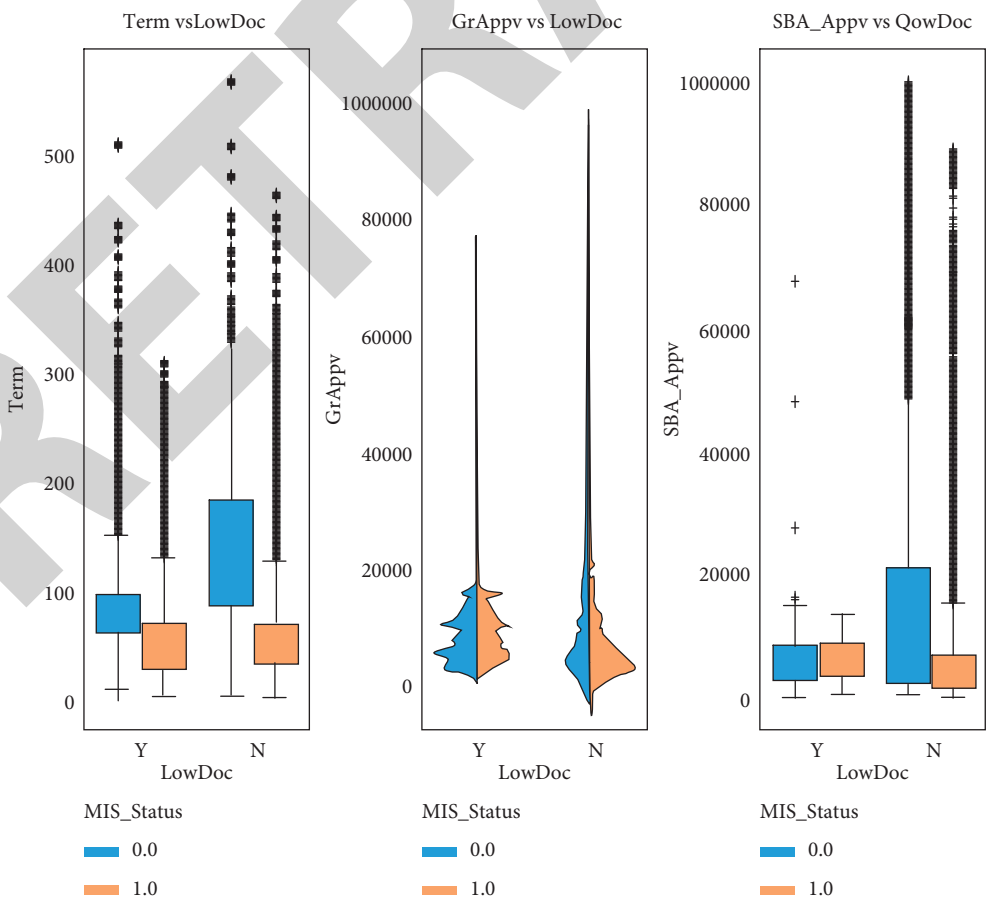


Figure 4: Box plots and violin plots of partial data distribution.

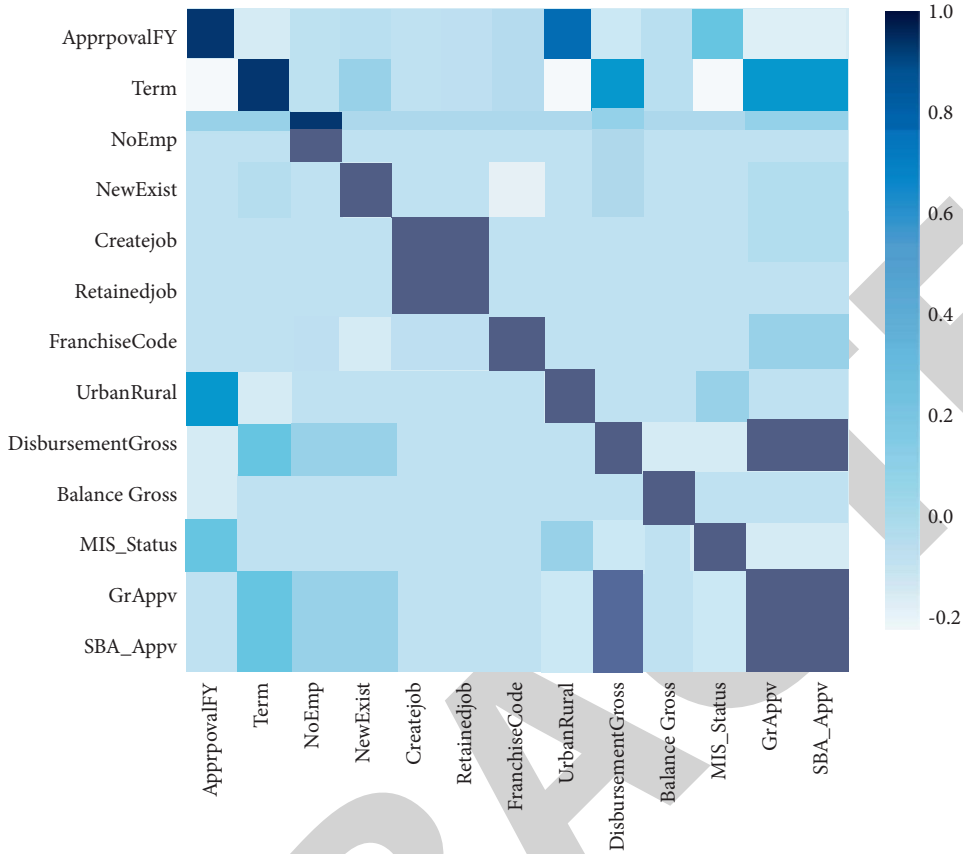


Figure 5: Correlation between the data variables.

continuously reduced, so as to find the optimal regression tree structure in theory.

$$L(\phi) = \sum_i l(\hat{y}_i, y_i) + \sum_k \Omega(f_k), \quad \text{where } \Omega(f_k) = \gamma T + \frac{1}{2}\lambda\|\omega\|^2. \tag{2}$$

In 2.2, tree integration model cannot be optimized by the traditional method, so the mean clustering method tries to optimize from the process of iterative accumulation of tree set, from the t tree to the tree set; to minimize the loss function after joining the t tree, we expand the loss function on the first i 1 tree set and discard the remaining term. The constant term is removed to simplify the objective function.

$$\begin{aligned} \mathscr{L}(t) &= \sum_{i=1}^{n} l(y_i, \hat{y}_i(t-1) + f_i(x_i)) + \Omega(f_t), \\ \mathscr{L}(t) &= \sum_{i=1}^{n}\left[l\left(yi, \hat{y}^{(t-1)}\right) + g_i f_t(xi) + \frac{1}{2}h_i f_t^2(x_i)\right] + \Omega(f_i), \\ \text{where } g_i &= \partial_{\hat{y}^{(i-1)}} l\left(y_i, \hat{y}^{(t-1)}\right), \\ h_i &= \partial^2_{\hat{y}(t-1)} l\left(y_i, \hat{y}^{(t-1)}\right) \\ \tilde{\mathscr{L}}(t) &= \sum_{i=1}^{n}\left[g_i f_t(x_i) + \frac{1}{2}h_i f_t^2(x_i)\right] + \Omega(f_t). \end{aligned} \tag{3}$$

Now, $I_j = \{i \mid q(x_i) = j\}$ is defined for all samples to fall on the set of the jth leaves so that we can rewrite the formula in 2.3,

$$\begin{aligned} \tilde{\mathscr{L}}(t) &= \sum_{i=1}^{n}\left[g_i f_t(x_i) + \frac{1}{2}h_i f_t^2(x_i)\right] + \gamma T + \frac{1}{2}\lambda\sum_{j=1}^{T}\omega_j^2 \\ &= \sum_{j=1}^{T}\left[\left(\sum_{i\in I_j} g_i\right)\omega_j + \frac{1}{2}\left(\sum_{i\in I_j} h_i + \lambda\right)\omega_j^2\right] + \gamma T. \end{aligned} \tag{4}$$

For any given tree structure q (x), we can compute the optimal weight w of the jth leaf node by the following below$_j$ and calculate the optimal loss value at this time.

$$\begin{aligned} \omega_j^* &= -\frac{\sum i \in I_j g_i}{\sum_{i\in I_j} h_i + \lambda}, \\ \tilde{\mathscr{L}}(t)(q) &= -\frac{1}{2}\sum_{j=1}^{T}\frac{\left(\sum_{i\in I_j} g_i\right)^2}{\sum_{i\in I_j} h_i + \lambda} + \gamma T, \\ \mathscr{L}_{split} &= \frac{1}{2}\left[\sum_{j=1}^{T}\frac{\left(\sum_{i\in I_L} g_i\right)^2}{\sum_{i\in I_L} h_i + \lambda} + \sum_{j=1}^{T}\frac{\left(\sum_{i\in I_R} g_i\right)^2}{\sum_{i\in I_R} h_i + \lambda} + \sum_{j=1}^{T}\frac{\left(\sum_{i\in I} g_i\right)^2}{\sum_{i\in I} h_i + \lambda}\right] - \gamma. \end{aligned} \tag{5}$$

2.6 can be used as an indicator to judge the current tree structure. As long as the above formula can be used in each

new tree, the global optimal tree structure set can be found, but because all the space of the possible tree structure space is infinite, so cannot really traverse to the optimal solution, so actually the mean clustering method uses a greedy strategy, let each tree split from a single node, each division as much as possible enum, compare when the tree structure split after 2.7 to judge whether the loss function value finally contraction, and choose the loss function value minimum, cannot find the tree structure when the iteration is completed. The empirical process of mean clustering method is the process of using sample data to continuously generate the tree structure in the above formula. After the training, the availability of the algorithm can be verified by detecting the accuracy and stability of the test set and checking the specific tree structure.

There are generally two approaches to find the approximate optimal splitting method from the mean clustering method: the feature number of splits based on all nodes and the feature-based total information gain.

The core of the method based on the number of feature divisions is used to calculate the total number of node divisions of each feature in the current node set of all the trees, and this number is used as the importance of this feature, defining the set of attributes in the data as $E = \{e_1, e_2, e_3, ...e_i\}^m$. The set of the regression trees is $F = \{f_1, f_2, f_3, ...f_i\}^k$, *Split* ($e_i$, f_j). For the number of times, the ith feature is divided on the jth tree. Then, the importance of this feature can be expressed as follows:

$$I_m(e_i) = \sum_{j=1}^{m} \text{Split}\left(e_i, f_j\right). \tag{6}$$

The key to the total information gain based on features is to calculate the sum of the information entropy of each feature in the set of nodes of all current trees and to judge the importance of the feature based on the sum of the information entropy. The greater the information entropy, the lower the information gain and importance of the feature. Set E = {e for all features1, e2, e3, ...ei}, for each feature, the value of ei. is contained in {ei 1, ei 2, ei 3, ...eij}. The probability of occurrence is the one of pij. According to the information entropy calculation formula, the information volume is as follows:

$$I\left(e_{ij}\right) = \log_2\left(\frac{1}{p_{ij}}\right) = -\log_2\left(p_{ij}\right). \tag{7}$$

$e_{i,}$ the information entropy, is as follows:

$$H\left(e_{ij}\right) = -\sum_{j=1}^{k} P_{ij}\log_2\left(P_{ij}\right). \tag{8}$$

X = (x) for datasets with a sample size of (ni, yi). Collection of values for different y is {y1, y2, y3, ...yi}. The proportion in the X is p_i. Then, the information entropy of dataset X is $I(X) = -)^{\sum k} p_i \log\ p_i$. If $k = 1$, the collection $X2$ will belong to only one category, and then, $I(X) = 0$. If the feature is e_iX was divided into k subsets $\{X_1, X_2, X_3, ...X_j\}^k$, among X_j, the number of samples included is n_j Then, the information entropy after the feature division is as follows:

$$E(e_i) = -\sum_{j=1}^{k} \frac{n_j}{n} I(X_i). \tag{9}$$

So, the feature ei on the regression tree fj is set. The information entropy on it can be expressed as follows:

$$\text{Gain}\left(e_i, f_j\right) = I(X) - E(e_i). \tag{10}$$

So, the importance of the feature ei can be expressed as follows:

$$\text{Gain}\left(e_i, f_j\right) = I(X) - E(e_i). \tag{11}$$

In this study, we will construct the mean clustering method model from the perspectives of information entropy and feature division number and analyze the economic meaning of variables according to the model's judgment of feature importance.

4. Model Demonstration and Analysis

4.1. Empirical of the Model

4.1.1. Comparison of the Results for the Multiple Models. After training these parameter set models on the dataset and repeating 5 cross-tests (the sample was randomly divided 5 times, of which 90% is the training set, and the rest was used to test the training model), the accuracy and AUC values of these models in the training set are shown in Figure 6.

The area under curve (AUC) value is to solve the problem that the accuracy of the model cannot truly reflect the model classification ability when the sample is extremely unbalanced. The two classification problem samples have positive and negative samples, and the judgment of the samples may be true or false, which constitutes the classification of true positive, true negative, false positive, and false negative. To truly reflect the accuracy of the model, two indicators of true-positive rate (TPRate) and false-positive rate (FPRate) are introduced.

$$\begin{aligned} \text{TPRate} &= \frac{\text{TP}}{\text{TP} + \text{FN}}, \\ \text{FPRate} &= \frac{\text{FP}}{\text{TN} + \text{FP}}. \end{aligned} \tag{12}$$

By constantly taking the classification threshold of the model, the corresponding TPRate and FPRate are obtained, and then, the above points in the two-dimensional coordinate axis form the receiver operating characteristic (ROC) curve. The area of the ROC curve and the X-axis is the AUC value.

4.1.2. Model Stability Test. The stability test of machine learning models mainly focuses on whether the model performance varies greatly on different datasets, and the test method used in this study is fivefold cross-validation. Through five repeated experiments, 90% of the data of the dataset was used to train the model parameters, and 10% of the data were used to test whether indicators such as contrast

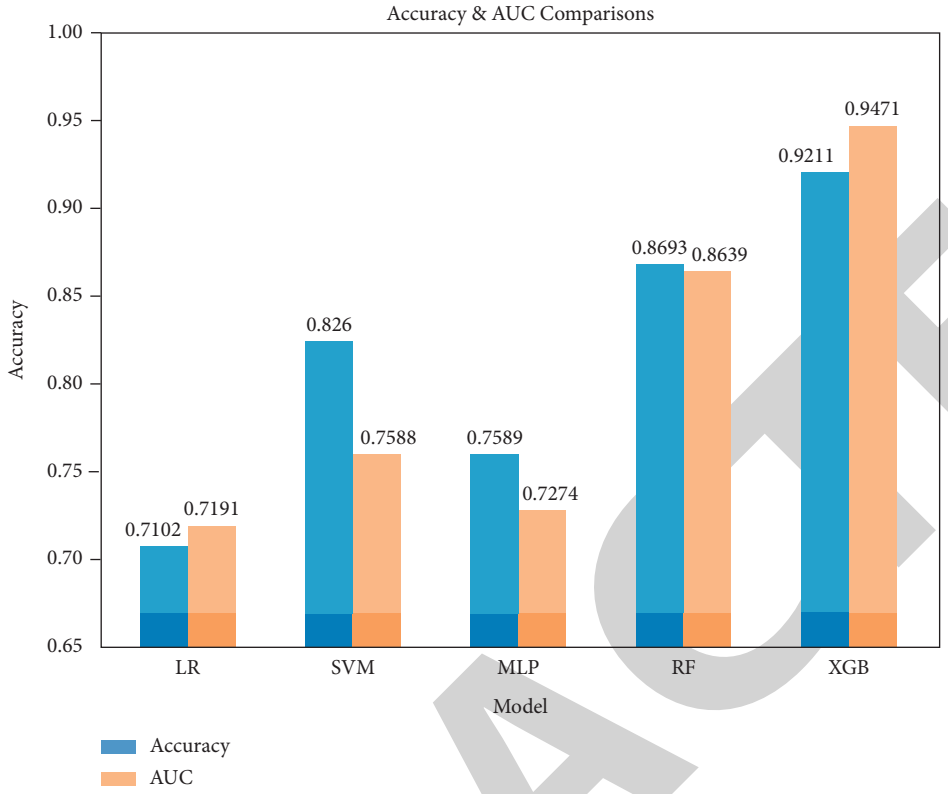


Figure 6: Model accuracy comparison.

Table 1: Cross-validation index of the mean clustering method.

Experimental number	Training set accuracy	Test set accuracy	Training set, AUC	Test set, AUC
1	0.929	0.9215	0.9689	0.9425
2	0.929	0.9093	0.9676	0.9507
3	0.9282	0.9169	0.969	0.9591
4	0.9258	0.925	0.966	0.9648
5	0.9323	0.9189	0.9708	0.9555

accuracy remained consistent. The results are shown in Table 1. Because the parameters of the model (the cluster-trained parameters are the base learner, or 100 regression trees) are completely determined by the training data, when the model is inconsistent in training data and test data, it is called overfitting. The indicator of the fivefold cross-validation conducted in this study can be considered stable and effective if the model does not show overfitting.

Five cross-validation ROC curve as shown below can be found that the ROC curve is very close to the line $y = 1$; although the test set prediction accuracy is about 2% lower than the training set, it still maintains above 90%, and the fluctuation range is small, the choice of data is not too big influence on the model, model stability is high, and the result is shown in Figure 7.

4.1.3. Optimization of the Classification Imbalance. As can be seen from the comparison of prediction accuracy and AUC values of different models, the mean clustering method is much higher than logistic regression and other methods of traditional machine learning methods. The average accuracy reached 94.71%, and the AUC value is close to the accuracy, and ROC curve is very close to $y = 1$, indicating that when processing these small- and medium-sized enterprise loan data samples, clustering method can have stable performance under different sample distribution, and from the perspective of prediction accuracy, average clustering method is the most suitable for predicting small- and medium-sized enterprise credit default risk studied in this study.

Lin et al. pointed out that in the model data sample category imbalance, even the ROC curve normal model has significant defects: the training process is not effective enough, most of the samples are unbalanced data samples, the proportion of the total loss function is too large, and such samples are generally easy to classify and did not provide enough useful signals for the model. Overall, simple positive samples can overwhelm the training, leading to model degradation. Only 20% of the sample in the loan data in this study is ultimately defaulted. The imbalance in the proportion of the loan sample and the default sample repaid on

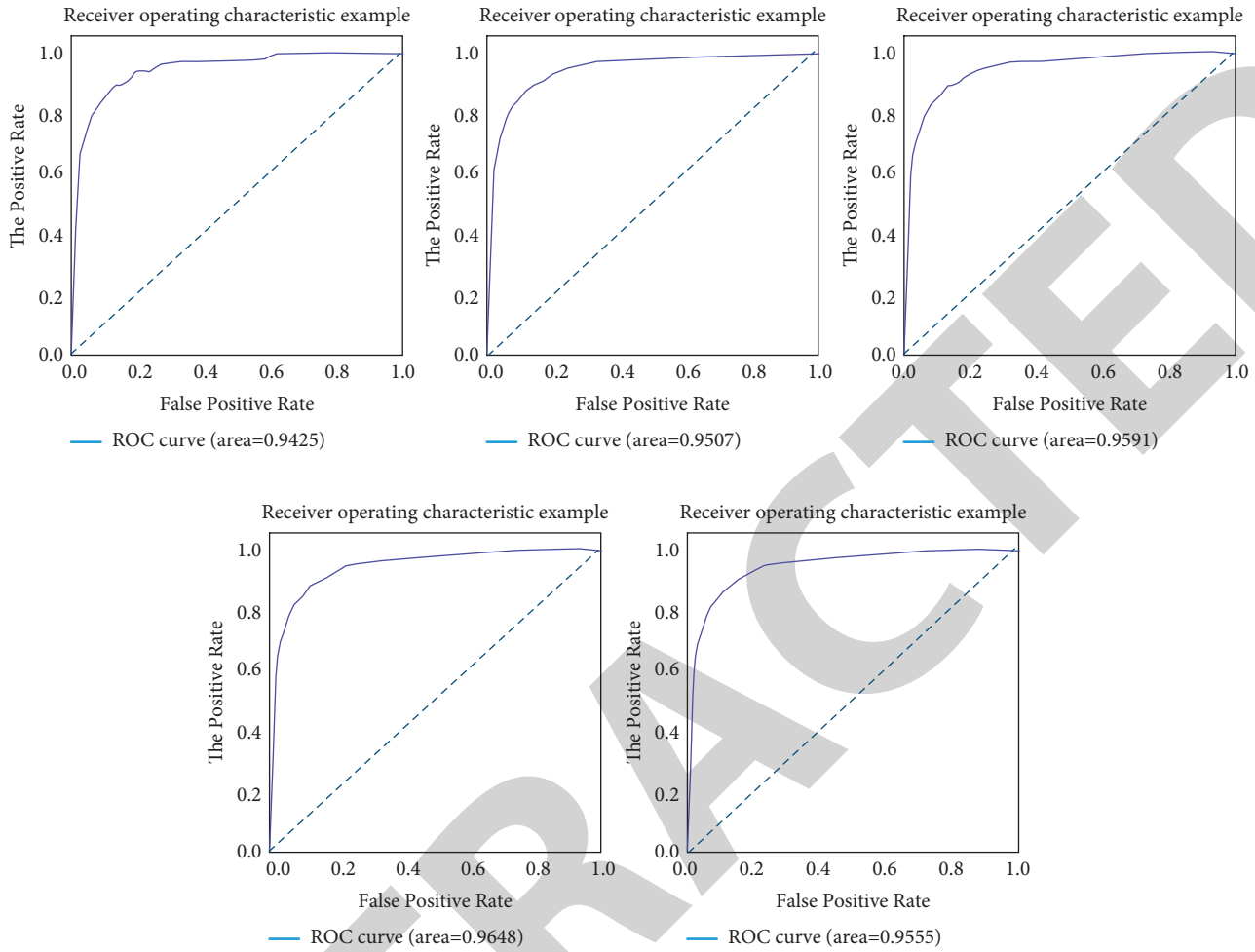


Figure 7: Fivefold cross-validation of the ROC curves.

time may limit the further improvement of the model performance, so this study will improve the ordinary clustering model from this aspect.

In past studies, the imbalance of data sample imbalance is relatively single. The mainstream approach is to increase a small number of samples in the dataset. The SMOTE method selects the nearest sample b for each small number of sample a. New samples were randomly generated between a and b. However, this approach is not applicable to the model shown in this study. Because, according to the empirical results of the model, certain important features such as term loan term volatility presents significantly different effects within different regions, then the samples generated by the SMOTE method may produce large amounts of noisy data. Another common treatment is online hard example mining (OHEM), which calculates the loss and then focuses on hard-to-classify data based on loss. Although the OHEM method increases the number of samples that are difficult to classify, on the other hand, it may cause the model to ignore the easily classified samples and may introduce new bias.

This article has decided to use Lin et al. after the comparison. The focal loss function is modified based on the ordinary cross-entropy loss function used on a single sample:

$$\begin{aligned}\text{Loss} &= -y_i \log f(x_i) - (1-y)\log 1 - f(x_i) \\ &= \begin{cases} -\log f(xi), & y = 1, \\ -\log(1 - f(xi)), & y = 0. \end{cases}\end{aligned} \tag{13}$$

In ordinary cross-entropy function, for each sample the weight is the same, in the classification imbalance data used are easy to ignore the influence of default samples, and focal loss function is to ordinary cross-entropy loss function increased a modulation coefficient, the size of the modulation coefficient depends on the parameter, when = 0. Focal loss function is ordinary cross-entropy function, but when more than 0, for easy to be classified samples, its f (xi). The value is large, which is controlled by the coefficient, the original loss is reduced, the impact on the overall loss is smaller, and the impact of samples that are not easily classified becomes larger. In this way, the processed loss function form can improve the identification ability of the average clustering method to identify a small amount of default data without changing the structure of the original data and introducing noisy data.

$$\text{FocalLoss} == \begin{cases} -(1 - f(xi))^{y} \log f(x_i), & y = 1, \\ -f(x_i)^{y} \log(1 - f(x_i)), & y = 0. \end{cases} \tag{14}$$

For the values of the parameters, Lin et al. found that with the increasing of the values, the importance of easily classified samples will gradually decrease, usually taking 2 to correct most data. After adding the mean clustering method of the focal loss function and comparing it with the previous model, it was found that the improved model had some improvement in the prediction accuracy and AUC value, indicating that the effect of the previous uneven sample distribution was indeed corrected by the modulation coefficient. Figure 8 shows the prediction results with different accuracies.

4.2. Analysis of Empirical Results. The data obtained here were fitted well by the mean clustering method. Although most machine learning algorithms have serious black-box properties, clustering can intuitively demonstrate its ability to analyze data features from two aspects. First, the model will calculate the ability to distinguish all features from samples in the process of generating the tree, and second, we can analyze the structural visualization results of the regression tree. The cluster method has two indicators to evaluate feature importance in dividing nodes: information gain and feature number. This study conducts experiments in these two ways and extracts the characteristic importance value accumulated during the calculation process. The results are compared as follows.

By observing the ranking results of two experiments, the absolute value of most variables is not high, and the ranking is relatively low. However, term, approval date, and disbursement date all showed a very high importance, especially because term was significantly higher than the other variables. This study will focus on the analysis of the term variables. In terms, they are called default and compliance variables.

Figure 9 shows the distribution in two cases. After observing the distribution in two cases (MIS_Status value is default), it is easy to find that the sample distribution of default is significantly concentrated in the short term, while the sample distribution of default is balanced in each time period. However, the term distribution under the two categories also coincides. If the classification is not considered, the term distribution of all samples is still more balanced.

This distribution suggests that the naive prior distribution is largely applicable to the analysis of term features and can only discuss its Bayesian probabilities after obtaining sample classification. The reason for the phenomenon of default samples concentrated in short-term loans may be related to the business model of small- and medium-sized enterprises. The capital demand of enterprises can be divided into long-term demand and short-term demand according to the length of time. These two demands are not only quite different in time but also have obviously different reasons for the demand.

For small- and medium-sized enterprises, long-term capital demand is more likely to come from the needs of fixed assets investment caused by the expansion of business development scale, while short-term capital demand is more likely to come from the shortage of funds needed for the operation of enterprises. In intuitive analysis of the enterprise operation and development information behind these two capital needs, the long-term capital demand is more related to the positive signal of the good development of the enterprise, while the short-term capital demand may be a sign that the enterprise fell into the predicament of poor management.

On the other hand, the interest rate of long-term loans will be higher than that of short-term loans under the same conditions. For enterprises with good operations that are less likely to default in the future, they will choose a reasonable loan cycle and amount according to their own needs. Enterprises with high uncertainty in the future are more likely to borrow from banks under the pressure of capital turnover and are more inclined to apply for short-term loans at high interest rates on long-term loans. Combined with long-term loans and short-term loans and the operating conditions of small- and medium-sized enterprises, the distribution of the data concentration loan cycle attribute is indeed in line with economic knowledge.

It can also be seen from the regression tree structure generated by the cluster training that the clustering gives a very high importance to the variable of term. In addition, the model is judged according to the different value range of term variables combined with other variables, rather than a simple linear simulation. Therefore, the scores of samples fluctuating within multiple intervals of term fluctuate, which also accords in line with the analysis of this study, so we cannot directly infer the default probability of loan application according to the size of term.

For the data variables used in this study, in addition to the attributes of the loan itself, it can basically be divided into macro-variables (time category) and enterprise characteristic variables. Judging from the model judgment and analysis of the importance of these variables, the importance of macro-variables is significantly higher than that of enterprise characteristic variables. The main reason for this distribution of importance is that the business scope of SMEs is relatively simple and the scale of capital is relatively small, resulting in low resistance to various risks. Not only large enterprises need to face this nonsystematic risk but also small- and medium-sized enterprises will encounter it under the influence of the economic cycle, because small- and medium-sized enterprises are vulnerable to the contraction of downstream demand and changes in upstream supply due to their small size. On the other hand, these loan applications have been reviewed by banks and SBA, and credit providers. The examiner reviewed the company's business and finances in advance and passed the sample. From a credit provider's perspective, detailed business information is more readily available when processing applications, while macroeconomic fluctuations are relatively unknown. These reasons make it easier to observe sample data.

Based on the empirical results of the above models, the clustering method has higher accuracy and consistent stability than other methods in predicting the credit default of small- and medium-sized enterprises, the error rate is lower, and the training method is simpler. For the data used in this study, the final cycle of loan default will have an impact, but the impact

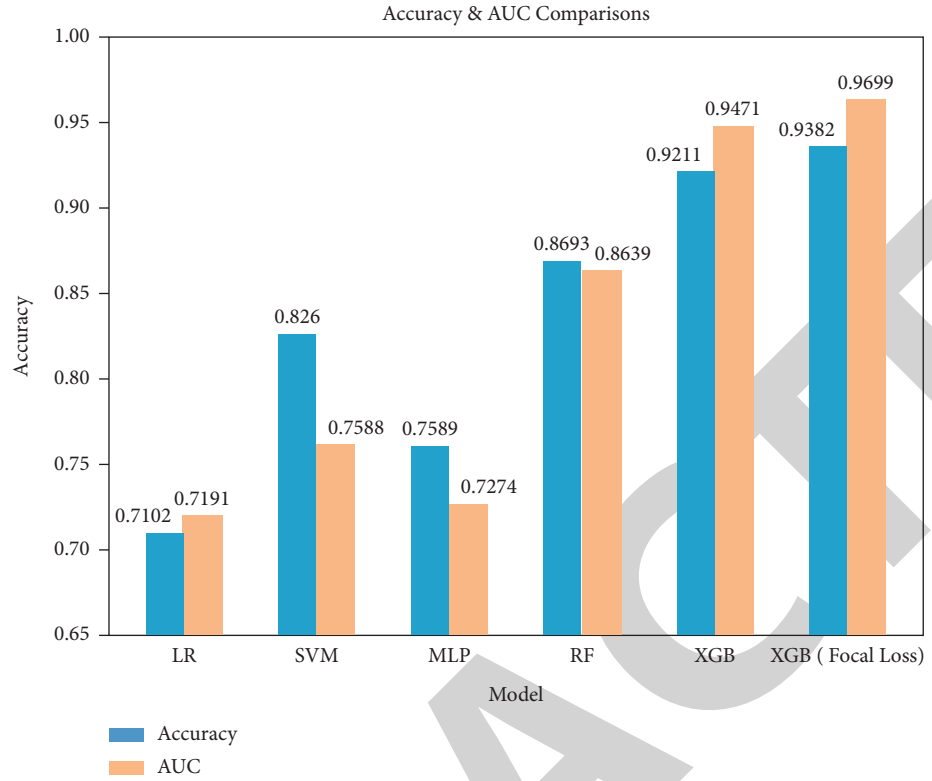


Figure 8: Comparison of prediction accuracy with the focal loss mean clustering method.

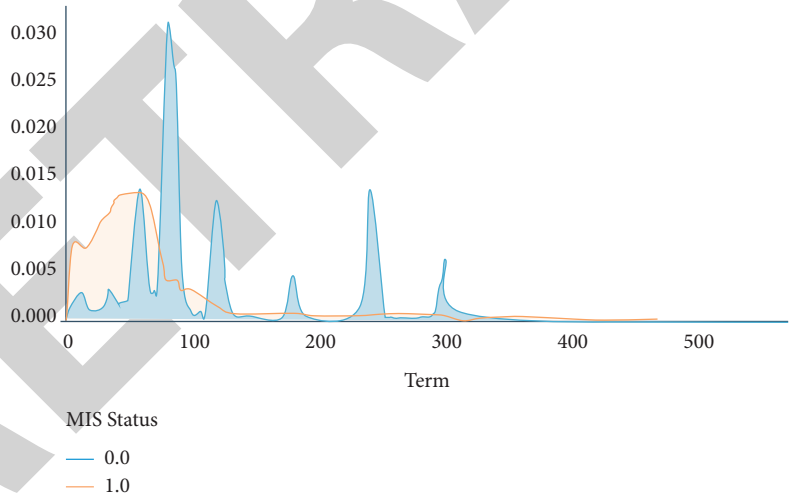


Figure 9: Scatterplot of the distribution of term variables in default and conservation cases.

is not linear, and it is still necessary to combine the characteristics of the macro- and company levels to effectively classify the sample. Combined with the historical background of the data, the model established in this study can further judge the loan default probability after analyzing and reviewing the loan, and the false reporting rate and false reporting rate are very low. As a supplementary means of bank credit risk control, the effect is very good. The downside is that while the models can more specifically analyze the impact of individual variables on defaults, they are not sufficiently powerful to explain how individual variables affect loan defaults.

5. Conclusion

This study analyzes and compares the credit records of SBA partially guaranteed by SVM, random forest, neural network, and logistic regression. The empirical results of the model show that the average clustering method has higher accuracy in predicting SME credit default scenarios than

Hindawi
Security and Communication Networks
Volume 2024, Article ID 9762740, 1 page
https://doi.org/10.1155/2024/9762740

Retraction

Retracted: Statistical Analysis of Employment Education in Colleges and Universities Based on Improved Clustering Algorithm

Security and Communication Networks

Received 8 January 2024; Accepted 8 January 2024; Published 9 January 2024

This article has been retracted by Hindawi following an investigation undertaken by the publisher [1]. This investigation has uncovered evidence of one or more of the following indicators of systematic manipulation of the publication process:

(1) Discrepancies in scope

(2) Discrepancies in the description of the research reported

(3) Discrepancies between the availability of data and the research described

(4) Inappropriate citations

(5) Incoherent, meaningless and/or irrelevant content included in the article

(6) Manipulated or compromised peer review

The presence of these indicators undermines our confidence in the integrity of the article's content and we cannot, therefore, vouch for its reliability. Please note that this notice is intended solely to alert readers that the content of this article is unreliable. We have not investigated whether authors were aware of or involved in the systematic manipulation of the publication process.

Wiley and Hindawi regrets that the usual quality checks did not identify these issues before publication and have since put additional measures in place to safeguard research integrity.

We wish to credit our own Research Integrity and Research Publishing teams and anonymous and named external researchers and research integrity experts for contributing to this investigation.

The corresponding author, as the representative of all authors, has been given the opportunity to register their agreement or disagreement to this retraction. We have kept a record of any response received.

References

[1] B. Liu, "Statistical Analysis of Employment Education in Colleges and Universities Based on Improved Clustering Algorithm," *Security and Communication Networks*, vol. 2022, Article ID 5776831, 12 pages, 2022.

Hindawi
Security and Communication Networks
Volume 2022, Article ID 5776831, 12 pages
https://doi.org/10.1155/2022/5776831

Research Article

Statistical Analysis of Employment Education in Colleges and Universities Based on Improved Clustering Algorithm

Bin Liu

Xinyang Vocational and Technical College, Xinyang 464000, China

Correspondence should be addressed to Bin Liu; liubin9027@xyvtc.edu.cn

Received 12 May 2022; Revised 6 June 2022; Accepted 10 June 2022; Published 11 July 2022

Academic Editor: Fang Liu

In order to improve the effect of employment education in colleges and universities, this study combines the improved clustering algorithm to carry out statistical analysis of employment education in colleges and universities and analyzes the current situation of employment education in colleges and universities. In cluster analysis, considering the complexity of the distribution of statistics after the reestimation of the sample size and the possible complex correlation between the series of statistics in the group sequential design, on the premise that the statistics used will not cause type I error expansion after sample size adjustment, some rules for reestimating the sample size can be formulated. Through the simulation analysis, it can be seen that the statistical analysis system of college employment education based on the improved clustering algorithm proposed in this study has a good effect in the clustering of employment education data and has a certain role in promoting the employment of college graduates.

1. Introduction

At present, under the guidance of "employment-oriented," some colleges and universities in China put students' professional skills training in a very prominent position, while students' quality education has been neglected. In addition to the two compulsory courses, foreign language, physical education, and other compulsory courses stipulated by the Ministry of Education, other humanistic quality education courses have been neglected, resulting in the disadvantaged position of humanistic quality education courses in colleges and universities. Humanistic quality education and vocational and technical education play an equally important role in the growth and success of college students, and they are in a position that cannot be ignored in the employment and career development of college students. However, at present, the quality of education for student development in China's colleges and universities is not in place, and quality education and practice are not enough. Moreover, education has not deeply analyzed the characteristics of college students, and the quality of talents demanded by the market needs to be improved, so that the problems existing in all aspects of students cannot be answered correctly and effectively. Second, quality education lacks pertinence. At present, the quality education of many colleges and universities is the traditional "big pot rice" education, which is the same as the education model of ordinary undergraduate colleges and does not educate students according to the actual situation of college students' love of outdoor activities and lack of learning motivation. Third, the effect of quality education is not good. Colleges and universities generally adopt various forms and methods to carry out quality education, but the effect is not obvious. Moreover, the ideological level, learning ability, and daily behavior of students have not been significantly improved and improved, and the content of quality education has not been truly implemented.

At present, under the guidance of "employment-oriented," some colleges and universities in our country have placed the professional skills training of students in a very prominent position, while the quality education of students has been neglected. In addition to the two compulsory courses, foreign language, physical education, and other compulsory courses stipulated by the Ministry of Education, other humanistic quality education courses have been neglected, resulting in the disadvantaged position of humanistic quality education courses in colleges and universities. Humanistic quality education and

vocational and technical education play an equally important role in the growth and success of college students, and they are in a position that cannot be ignored in the employment and career development of college students [1]. In order to achieve full employment, students in colleges and universities must shape themselves into an all-round development, with comprehensive quality and ability of senior professionals. The basic abilities it should have include the ability to adapt to society, practical ability, innovation ability and interpersonal communication ability, management ability, expression ability, core competitiveness, decision-making ability, team spirit, both ability and political integrity, and learning ability, in the final analysis, with the improvement of quality in all aspects [2]. However, at present, the quality of education for the development of students in various colleges and universities in our country is not in place, quality education and practice are not enough, there is no in-depth analysis of the characteristics of college students, and the quality of talents demanded by the market needs to be improved. Correct and effective answer: Second, quality education lacks pertinence. At present, many colleges and universities develop quality education, which is a traditional "big pot rice" education, which is the same as the education model of ordinary undergraduate colleges and is not aimed at college students. If students lack learning motivation due to their love of outdoor activities, they should be educated according to the actual situation [3]; third, the effect of quality education is not good; colleges and universities generally adopt various forms and methods to carry out quality education, but the effect is not obvious; students' ideological level, learning ability, and daily behavior have not been significantly improved and improved, and the content of quality education has not been truly implemented [4].

According to the research content of Western employment theory by Chinese and Western scholars, it is generally believed that Keynes' previous employment theory (i.e., Western traditional employment theory) includes automatic employment equilibrium theory, equilibrium wage employment theory, and employment cycle fluctuation theory. The theory of automatic equilibrium emphasizes that the government should not intervene in the economy, because according to the spontaneous adjustment of the price mechanism, the commodity market and the production factor market will gradually tend to the equilibrium of supply and demand, which will lead to full employment. The unbalanced state of supply and demand is only temporary, and the self-regulation of the market will automatically restore it to an equilibrium state [5]. What the government can do is best limited to the role of encouraging production. The core content of the equilibrium wage employment theory is that the wage of labor is determined by demand and supply, while the amount of employment is determined by the equilibrium wage. The employment cycle fluctuation theory refers to the cyclical fluctuations of employment caused by the cyclical fluctuations of the economy, such as insufficient consumption, and the social demand for consumer goods cannot keep up with the growth of consumer goods supply; then the surplus of labor will lead to underemployment. Austrian economist Hayek believes that excessive investment will cause the supply of money to fail to meet the demand for money in real economic life. It will also lead to the phenomenon of underemployment [6]. Tavani and Zamparelli [7] pointed out that the old equilibrium caused by innovation is broken, and when transitioning to the new equilibrium, the labor force whose skills cannot keep up with the pace of innovation is eliminated, and unemployment becomes a helpless necessity. And society progresses in the process of breaking the old equilibrium from the new equilibrium, and unemployment caused by technological innovation will be inevitable. With Keynesian employment theory (i.e., modern employment theory), through Keynesian theoretical analysis, full employment can only appear when the total social supply and total demand are in the best state [8]. However, in the actual operation of the market economy, in order to achieve a balance between total social supply and total demand, we can only hope for economic contraction, which is contrary to the law of social progress. Portella-Carbó [9] believed that the realization of full employment must be done by vigorously stimulating demand and carrying out demand management. The lack of effective demand is the irreconcilable product of the market mechanism itself. In order to break through this practical bottleneck and expand the functions of the government, implementing the means of government intervention in the economy is an effective way to solve the problem. Keynes therefore also extended the macroeconomic policy proposition on solving the unemployment problem. Its main contents include tax policy, monetary policy, fiscal policy, and foreign trade policy. The core of Keynes's policy proposition on solving the unemployment problem is to change laissez-faire and implement the policy of government intervention in the economy to increase the effective demand of the society and achieve full employment. The emergence of modern employment theory is due to the fact that the contradictions inherent in capitalist society have not been fundamentally eliminated by the Keynesian policy, and although the state intervention promoted by this policy has stimulated production to a certain extent, it has also contributed to a more serious crisis. Condition [10] is provided. In order to solve the inflation problem plaguing the capitalist economy, various new theories and theories have emerged one after another. The more important theoretical schools after Keynes are supply school, monetary school, rational expectation school, development economics, and new Keynesian school. In employment theory [11], the point of [12] is that the most convenient way to stimulate economic growth and expand employment can be achieved through tax cuts; any practice that increases the cost of labor use will hinder the expansion of employment. Clarkson [13] proposed the monetarist policy of "market unemployment rate" and "natural rate of unemployment." By envisioning the formulation of a single monetary policy rule, the money supply will increase at a fixed rate, so as to achieve the goal of maintaining the stability of the capitalist economy, and under such an economic environment, the employment problem will be gradually solved.

Promoting the employment of engineering students in colleges and universities is of great significance to the country, schools, and individuals. In addition, as colleges continue to expand enrollment and it is difficult for college students to find employment, it is particularly important to carry out employment promotion work to enhance the competitiveness of advanced engineering students in the job market and increase their employment rate [14].

With the continuous expansion of the enrollment scale, the pressure of the oversupply of labor force across the country is increasing, and the graduates of colleges and universities have also encountered unprecedented employment pressure. In the face of the lack of sophisticated technical talents in high-end industries and the saturated supply of talents in low-end industries, the embarrassing situation of college graduates can be imagined. Explore scientific and reasonable employment education countermeasures for students in colleges and universities, while increasing students' employment skills, guide students to establish correct employment values, improve students' income chips, open up ideas for students' employment, and help students pursue life goals and achieve life value which has become the driving force behind the reform of employment education.

This study combines the improved clustering algorithm to conduct statistical analysis of employment education in colleges and universities to analyze the current situation of employment education in colleges and universities, which provides a reference for better development of employment education in the future.

2. Improved Clustering Algorithm

2.1. Adaptive Design. Considering the complexity of the statistic distribution after the reestimation of the sample size and the possible complex correlations between the statistic series in the group sequential design, Bauer and Kohne [15] proposed to carry out hypothesis test analysis on the stage data between each two analyses separately and finally merge the P values obtained by each hypothesis test in a certain form. Figure 1 shows an example of a two-stage adaptive sequential design. That is, first calculate the P_1 of the first stage; if $P_1 > \beta_1$, the null hypothesis H_0 is not rejected in the early stage. If $P_1 < \alpha_1$, the null hypothesis H_0 is rejected early. If $\alpha_1 \le P_1 \le \beta_1$, we continue to enroll subjects in the second stage, and after the enrollment is completed, the hypothesis test probability P_2 of the second-stage samples is calculated separately, and P_1 and P_2 are combined into $C(P_1, P_2)$ in a certain form. If $C(P_1, P_2) < \beta_2$, the null hypothesis H_0 is rejected; otherwise, the null hypothesis H_0 is not rejected.

There are many ways to combine P_1 and P_2. In fact, it can be shown that the MSP statistic is the general form of the Cui-Hung-Wang statistic, the latter were combined using the standard normal distribution statistic Z_i, and the parameters $w_1' w_2$ were specified as the square root of the two-stage sample size percentage before sample size adjustment, the reason why a statistic is defined as a function of probability P. On the one hand, the probability P is simply distributed under the null hypothesis H_0 and obeys the uniform distribution $U(0, 1)$ on $[0, 1]$. On the other hand, it is due to the fact that the t-statistic is considered to be complicated in the correlation between the statistic series in the traditional group sequential design. When the probability P is used to construct the statistic and the sample size is readjusted, the conditional distribution $P_2|P_1 = p_1 \sim U(0, 1)$ under the null hypothesis H_0 is the same as the case where the variance is known.

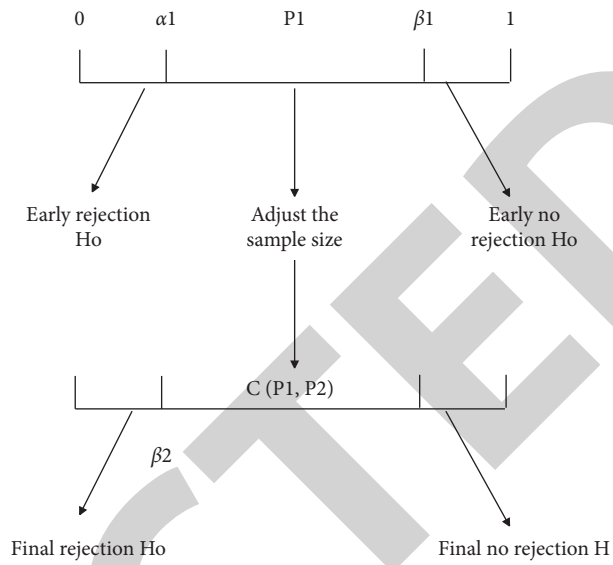


Figure 1: Two-stage adaptive sequential design diagram.

Although the above two statistics can accurately control the type I error at the preset α level, they also have certain defects. When $P_1 \longrightarrow \alpha_1$ or β_2, the MPP statistic can almost 100% reject the null hypothesis H_0 at the end of the period analysis. The MSP statistic is more prone to type II errors in interim analysis than the former. Based on the above two points, this study deduces a new statistic—MCP statistic.

For brevity, the following assumes that the population variance is known and uses a two-stage adaptive sequential design as an example. In fact, based on the theory of two-stage adaptive design, it can be generalized to multistage adaptive design, and the generalization method will be introduced in the sample size adjustment based on conditional type I error.

2.2. Construction of MCP Statistics. Based on the probability P value of each stage, the MCP statistic is constructed: $T_1 = P_1, T_2 = (w_1\sqrt{P_1} + w_2\sqrt{P_2})^2$, and the rules for early termination of the experiment similar to the traditional group sequential design are specified:

$$\begin{cases} \text{If } T_1 \le \alpha_1, & \text{Terminate the test in advance and reject the null hypothesis } H_0, \\ \text{If } T_1 \ge \beta_1, & \text{Terminate the test in advance and do not reject the invalid hypothesis } H_0, \\ \text{If } \alpha_1 < T_1 < \beta_1, & \text{Continue the second stage test.} \end{cases} \quad (1)$$

In the final analysis, if $T_2 \geq \beta_2$, the null hypothesis H_0 is not rejected, and if $T_2 < \beta_2$, the null hypothesis H_0 is rejected. $\alpha_1, \beta_1, \beta_2$ are the preset boundaries of the rejection domain or the accepted domain, respectively.

The properties of this statistic are derived as follows:

We assume a continuous variable X, and its distribution function is F(x). Obviously, the function F and its inverse function F^{-1} are both monotonically increasing functions.

For one-sided hypothesis testing, the probability $P = 1 - F(X)$, and then the distribution function of P is

$$\begin{aligned} P(P \leq p) &= P(1 - F(X) \leq p) = P\left(X \geq F^{-1}(1-p)\right) \\ &= 1 - \mathrm{P}\left(X \leq F^{-1}(1-p)\right) = 1 - F\left(F^{-1}(1-p)\right) \\ &= p(p \in [0,1]). \end{aligned} \tag{2}$$

For the two-sided hypothesis test, the probability $P = 2(1 - F(|X|))$, we assume that the statistic obeys a symmetrical distribution, and then the distribution function of P is

$$\begin{aligned} P(P \leq p) &= P(2 - 2F(|X|) \leq p) = 2P\left(X \geq F^{-1}\left(1 - \frac{p}{2}\right)\right) \\ &= 2\left(1 - P\left(X \leq F^{-1}\left(1 - \frac{p}{2}\right)\right)\right) \\ &= 2\left(1 - F\left(F^{-1}\left(1 - \frac{p}{2}\right)\right)\right) \\ &= pp \in [0,1]. \end{aligned} \tag{3}$$

From the above, it can be proved that the random variable P obeys a uniform distribution on [0, 1]; that is, T_1 of the MCP statistic obeys a uniform distribution on [0, 1] under the null hypothesis.

Since $P_1 = 1 - F(Z_1)$, the sample size of the second stage after the reestimation of the sample size is $\tilde{n}_2 = \tilde{N} - n_1 = g(Z_1) = h(P_1)$, and the conditional probability density function is $f(p_2|p_1) = f(p_2|\tilde{n}_2) = 1$, so the joint distribution of P_1 and P_2 is $f(p_1, p_2) = f(p_2|p_1)^* f(p_1) = 1$.

It is easy to find the Jacobian determinant from (P_1, P_2) to (T_1, T_2) as

$$\begin{aligned} J &= \begin{bmatrix} 1 & 0 \\ h(T_1, T_2) & \dfrac{1}{w_2^2} - \dfrac{w_1}{w_2^2}\sqrt{\dfrac{T_1}{T_2}} \end{bmatrix} \\ &= \frac{1}{w_2^2} - \frac{w_1}{w_2^2}\sqrt{\frac{T_1}{T_2}}. \end{aligned} \tag{4}$$

Then the joint probability density function of (T_1, T_2) is $f(t_1, t_2) = J * f(p_1, p_2) = (1/w_2^2) - (w_1/w_2^2)\sqrt{(t_1/t_2)}$. The subprobability density function of T_2 is $f(t_2) = \int_{\alpha_1}^{\beta_1} f(t_1, t_2)\mathrm{d}t_2\mathrm{d}t_1$.

If the results of the interim analysis meet the conditions for rejecting H_0 and early termination of the experiment under the premise that H_0 is true, then the probability of making a type I error at this time is $P_{\mathrm{rob}} = \alpha_1$. Conversely, if the results of the interim analysis do not meet the conditions for early termination of the trial, further phase II trials are required. From the definition of T_2, we know that $T_2 \geq w_1^2 T_1$. When $w_1^2\beta_1 \geq \beta_2$, there is $T_1 > \beta_2/w_1^2$, at this time $T_2 = (w_1\sqrt{T_1} + w_2\sqrt{P_2})^2 > \beta_2$, and H_0 can be accepted without a second-stage test. Therefore, when $w_1\sqrt{\beta_1} \geq \sqrt{\beta_2}$, the probability of making a type I error in the end-of-period analysis is

$$\begin{aligned} \mathrm{Prob}_2 &= \int_{\alpha_1}^{(\beta_2/w_1^2)} \int_{w_1^2 t_1}^{\beta_2} f(t_1, t_2)\mathrm{d}t_2\mathrm{d}t_1 \\ &= \int_{\alpha_1}^{(\beta_2/w_1^2)} \int_{w_1^2 t_1}^{\beta_2} \left(\frac{1}{w_2^2} - \frac{w_1}{w_2^2}\sqrt{\frac{t_1}{t_2}}\right)\mathrm{d}t_2\mathrm{d}t_1 \\ &= \cdots\cdots = \frac{\beta_2^2}{6w_1^2w_2^2} + \frac{4w_1\alpha_1\sqrt{\alpha_1\beta_2}}{3w_2^2} - \frac{w_1^2\alpha_1^2}{2w_2^2} - \frac{\alpha_1\beta_2}{w_2^2}. \end{aligned} \tag{5}$$

When $w_1\sqrt{\beta_1} < \sqrt{\beta_2}$, similar to the above calculation process, the probability of making a Type I error in the end-of-period analysis is

$$\begin{aligned} \mathrm{Prob}_2 &= \int_{\alpha_1}^{\beta_1} \int_{w_1^2 t_1}^{\beta_2} f(t_1, t_2)\mathrm{d}t_2\mathrm{d}t_1 \\ &= \int_{\alpha_1}^{\beta_1} \int_{w_1^2 t_1}^{\beta_2} \left(\frac{1}{w_2^2} - \frac{w_1}{w_2^2}\sqrt{\frac{t_1}{t_2}}\right)\mathrm{d}t_2\mathrm{d}t_1 \\ &= \cdots\cdots = \frac{6\beta_2(\beta_1 - \alpha_1) + 3w_1^2\left(\beta_1^2 - \alpha_1^2\right) + 8w_1\alpha_1\sqrt{\alpha_1\beta_2} - 8w_1\beta_1\sqrt{\beta_1\beta_2}}{6w_2^2}. \end{aligned} \tag{6}$$

The rejection of the null hypothesis H_0 at the interim analysis and the rejection of the null hypothesis H_{0} at the end of the period are two mutually exclusive and independent events. Therefore, in order to control the overall type I error to the preset inspection level α, it is necessary to satisfy

$$\text{Prob}_1 + \text{Prob}_2 = \alpha. \tag{7}$$

If the early termination of the experiment due to rejection of the null hypothesis H_0 is not allowed in the interim analysis, the experiment will no longer make type I errors in the interim analysis, and $\alpha_1 = 0$ in equations (5) and (6). When $w_1\sqrt{\beta_1} \geq \sqrt{\beta_2}$, the probability of making a type I error in the end-of-period analysis is

$$\text{Prob}_2 = \frac{\beta_2^2}{6w_1^2w_2^2}. \tag{8}$$

When $w_1\sqrt{\beta_1} < \sqrt{\beta_2}$, the probability of making a Type I error in the end-of-period analysis is

$$\text{Prob}_2 = \frac{6\beta_1\beta_2 + 3w_1^2{\beta_1}^2 - 8w_1\beta_1\sqrt{\beta_1\beta_2}}{6w_2^2}. \tag{9}$$

Furthermore, it satisfies

$$\text{Prob}_2 = \alpha. \tag{10}$$

Under this constraint, the boundary values α_1 and β_1 can be selected according to the experimental design requirements and relevant regulations, and the boundary value β_2 at the end of the period can be calculated.

Since the joint distribution of (T_1, T_2) is not affected by the readjustment of the sample size, the MCP statistic can accurately control the total type I error of the trial at the preset α level.

In a simulation of employment data that allows for sample size reestimation, it is not enough for a statistic to draw conclusions about whether to reject the null hypothesis. However, if the probability P value of hypothesis testing can be obtained, it will make this statistic more useful. In hypothesis testing, the P value is defined as the probability of the current situation and more extreme situations when the null hypothesis $H0$ is true. The smaller the P value, the stronger the reason for rejecting the null hypothesis $H0$. The probability P value of the traditional design is easily obtained according to the monotonicity of the likelihood ratio, while the adaptive design no longer has a monotonic likelihood ratio in the sample space due to the different number of subjects in different analysis stages. Therefore, a number of different definitions for "extreme" have been proposed, including stagewise ordering, maximum likelihood estimation order (MLE ordering), likelihood ratio order, and score test order, among which stage order is the most commonly used.

For the MCP statistic, the P values based on the order of stages are

$$P(k) = \begin{cases} T_1 \quad (k = 1), \\ \alpha_1 + \dfrac{T_2^2}{6w_1^2w_2^2} + \dfrac{4w_1\alpha_1\sqrt{\alpha_1 T_2}}{3w_2^2} - \dfrac{w_1^2\alpha_1^2}{2w_2^2} - \dfrac{\alpha_1 T_2}{w_2^2} \quad \left(k = 2, w_1\sqrt{\beta_1} \geq \sqrt{\beta_2}\right), \\ \alpha_1 + \dfrac{6T_2(\beta_1 - \alpha_1) + 3w_1^2\left(\beta_1^2 - \alpha_1^2\right) + 8w_1\alpha_1\sqrt{\alpha_1 T_2} - 8w_1\beta_1\sqrt{\beta_1 T_2}}{6w_2^2}, \\ \left(k = 2, w_1\sqrt{\beta_1} < \sqrt{\beta_2}\right). \end{cases} \tag{11}$$

One of the advantages of using the sequence of stages is that the results of the probability $P(k)$ are guaranteed to be consistent with the hypothesis testing results. That is, if the null hypothesis is rejected at any stage at the α level, then $P(k) < \alpha$. Otherwise, $P(k) \geq \alpha$.

Noninferiority test and bioequivalence test are commonly used test methods in the simulation of new drug employment data. Compared with the traditional hypothesis testing, the confidence interval method has obvious advantages. The MCP statistic can also be used to estimate confidence intervals. Still taking the employment data simulation of the difference test between groups as an example, we assume that the actual difference between the group means is θ. Then, the confidence interval of the parameter to be tested refers to the interval composed of all possible values of θ calculated according to the current sample when the null hypothesis H_0 is established. It is easy to obtain $P_k' = 1 - F(F^{-1}(1 - P_k) - \theta\sqrt{n_k}/\sqrt{2}\,\sigma)$, $(k = 1, 2)$, $F(\cdot\cdot)$ is the cumulative probability function of the normal distribution, $F^{-1}(..)$ is its inverse function, P_k' is the probability P value when the actual difference is θ, and P_k is the probability P value when the actual difference is equal to the H_0 test value. If the trial is terminated at the interim analysis, the confidence interval for θ is the set

$$\left\{\theta | 1 - F\left(F^{-1}(1 - p_1) - \frac{\theta\sqrt{n_1}}{\sqrt{2}\,\sigma} \geq \alpha_1\right)\right\}. \tag{12}$$

If the trial is terminated at the end-of-period analysis, the confidence interval for θ is the set

$$\left\{\theta\middle|\left(w_1\sqrt{1-F\left(F^{-1}(1-p_1)-\frac{\theta\sqrt{n_1}}{\sqrt{2}\,\sigma}\right)}+w_2\sqrt{1-F\left(F^{-1}(1-p_2)-\frac{\theta\sqrt{n_2}}{\sqrt{2}\,\sigma}\right)^2}\geq\beta_2\right\}. \tag{13}$$

2.3. Reestimation of Sample Size. On the premise of ensuring that the statistics used will not cause type I error expansion after sample size adjustment, some rules for sample size reestimation can be formulated. From the derivation process of the statistic distribution, as long as the conditional probability density function $f(p_2|p_1) = 1$ of P_2 is guaranteed, that is, when the sample size in the second stage is a function of the variable P_1, the sample size can be adjusted "arbitrarily." The commonly used adjustment rules are as follows:

As mentioned earlier, the sample size estimation formula is $N = 2\sigma^2[Z_{1-\alpha} + Z_{1-\beta}]^2/\theta^2$. We assume that the initial estimated sample size of an experiment is N_0 and the effect size is $E_0 = \theta/\sigma$. Then, the effect size estimated from the sample of n_1 cases in the interim analysis is $\widetilde{E} = \widetilde{\theta}/\widetilde{\sigma}$. The total sample size can be reestimated intuitively to be $\widetilde{N} = (E_0/\widetilde{E})^2 N_0$, so that the sample size of the second phase trial is $\widetilde{n}_2 = \widetilde{N} - n_1$. Generally, a minimum value $n_{2\min}$ and a maximum value $n_{2\max}$ are specified for $\widetilde{n}_2$, so the second-stage sample size of reestimation is $\widetilde{n}_{2re} = \min(\max(\widetilde{n}_2, n_{2\min}), n_{2\max})$.

In an adaptively designed experiment, the conditional power is often more important than the total power. Based on conditional test power, it is possible not only to compare different experimental designs and statistical methods, but also to make decisions such as sample size reestimation. The so-called conditional test power refers to the probability of rejection of the null hypothesis H_0 at the end of the period analysis after obtaining the results of the interim analysis under the alternative hypothesis H_1, that is, the probability of $T_2|P_1 = p_1, H_1 < \beta_2$. For the MCP statistic, conditional test power refers to the probability that $P_2|P_1 = p_1, H_1 < ((\sqrt{\beta_2} - w_1\sqrt{p_1})^2/w_2^2)$.

Taking the simulation of employment data comparing the means of the two groups as an example, we assume that, under the alternative hypothesis H_1, θ is the actual difference between the means of the two groups, the variance of the variable is known as σ^2, F is the standard normal distribution function, the sample size of each group in the second stage is n_2, and then, the conditional distribution of P_2 is $D(p_2|p_1) = P(P_2 \leq p_2|p_1) = P(1 - F(Z_2) \leq p_2|p_1) = P(Z_2 \geq F^{-1}(1 - p_2)|p_1) = 1 - F(F^{-1}(1-p_2) - (\theta\sqrt{n_2}/\sqrt{2}\sigma))$; therefore, the conditional test power of the MCP statistic is

$$cP = 1 - F\left(F^{-1}\left(1 - \frac{\left(\sqrt{\beta_2} - w_1\sqrt{p_1}\right)^2}{w_2^2}\right) - \frac{\theta\sqrt{n_2}}{\sqrt{2}\,\sigma}\right), \tag{14}$$

$$\widetilde{n}_2 = \frac{2\sigma^2}{\theta^2}\left(F^{-1}\left(1 - \frac{\left(\sqrt{\beta_2} - w_1\sqrt{p_1}\right)^2}{w_2^2}\right) - F^{-1}(1-cP)\right)^2. \tag{15}$$

The sample size n_2 of the second stage can be estimated by specifying the conditional test power cP. Since σ and θ are often unknown, they can be replaced by the corresponding estimated values obtained from the interim analysis.

Due to the constraints of human, financial, and material resources, a maximum sample size $n_{2\max}$ is specified for the second stage. At the same time, in order to make the sample size of the second stage not too small, a minimum sample size $n_{2\min}$ is specified. We assume that the reestimated sample size calculated according to equation (15) is $\widetilde{n}_2$; then the sample size of the second stage is $\widetilde{n}_{2re} = \min(\max(\widetilde{n}_2, n_{2\min}), n_{2\max})$. According to equation (14), the probability density function of conditional test power cP can be obtained as $f(cP)$. If the trial is terminated early, the expected sample size in the second stage is

$$E\left(\widetilde{n}_{2\,\text{stage}}\right) = \int_0^1 \min\left(\max\left(\widetilde{n}_2, n_{2\min}\right), n_{2\max}\right) f(cP)\,dcP. \tag{16}$$

The probability of terminating the experiment early because the data is valid is $p_e = \phi((\theta_R\sqrt{n_1}/\sqrt{2}\sigma) - \phi^{-1}(1-\alpha_1))$. And the probability of terminating the experiment early due to invalid data is $p_f = \phi(\phi^{-1}(1-\beta_1) - (\theta_R\sqrt{n_1}/\sqrt{2}\sigma))$. Then, the expected total sample size is

$$E(\widetilde{n}) = \left(p_e + p_f\right) * n_1 + \left(1 - p_e - p_f\right) * E\left(\widetilde{n}_{2\text{stage}}\right). \tag{17}$$

It is worth mentioning that when the conditional test power is very low, it is possible that the sample size obtained by reestimating is larger than the sample size of starting a new simulation of employment data. At this point, it is necessary to discuss whether to continue the employment data simulation.

Based on this idea, we can make

$$\frac{2\widetilde{\sigma}^2}{\widetilde{\theta}^2}\left(\phi^{-1}\left(1 - \frac{\left(\sqrt{\beta_2} - w_1\sqrt{p_1}\right)^2}{w_2^2}\right) - \phi^{-1}(1-cP)\right)^2 \leq \frac{2\widetilde{\sigma}^2\left[\phi^{-1}(1-\alpha) + \phi^{-1}(1-\beta)\right]^2}{\widetilde{\theta}^2}. \tag{18}$$

We assume that the conditional test power is $cP = 1 - \beta$ and then simplify the above formula to get

$$p_1 \leq \left(\frac{\sqrt{\beta_2} - w_2\sqrt{\alpha}}{w_1}\right)^2. \tag{19}$$

That is, when $p_1 > (\sqrt{\beta_2} - w_2\sqrt{\alpha}/w_1)^2$, it would be a better choice to abandon the current experiment and start a new experiment purely from the point of view of saving the sample size statistically. Of course, researchers generally prefer to keep the employment data simulation intact. At the same time, it must be taken into account that the preparation of a new employment data simulation is also a rather

complicated process. Therefore, this study proposes to set a multiple upper limit Δ, and when the reestimated sample size is greater than Δ times the sample size of a new employment data simulation, comprehensively consider various factors to decide whether to stop the current employment data simulation.

The so-called conditional type I error refers to the probability of rejection of the null hypothesis H_0 at the end of the period analysis after obtaining the results of the interim analysis under the null hypothesis H_0, that is, the probability of $T_2|P_1 = p_1, H_0 < \beta_2$. For the MCP statistic, that is the probability of $P_2|P_1 = p_1$, $H_0 < ((\sqrt{\beta_2} - w_1\sqrt{p_1})^2/w_2^2)$. Since the conditional distribution of P_2 is $F(p_2|p_1) = p_2$ under the H_0 condition, the conditional type I error is $A(p_1) = (\sqrt{\beta_2} - w_1\sqrt{p_1})^2/w_2^2$. In fact, if $\theta = 0$ in the conditional test efficiency formula, the above formula can also be obtained. It is easy to know from the definition that the unconditional type I error of the second stage is $\int_{\alpha_1}^{\beta_1} A(p_1)\mathrm{d}p_1$, and it satisfies $\alpha_1 + \int_{\alpha_1}^{\beta_1} A(p_1)\mathrm{d}p_1 = \alpha$; this formula is equation (14).

The reason why it is called "staged" sample size readjustment is that the conditional type I error is mainly used to adjust the number of experimental stages compared to the conditional test power mainly used for sample size readjustment. Consider adding another interim analysis to the current design. We assume that, after adding a new experimental stage, the conditional type I error based on p_1 becomes $A^*(p_1)$, which is sufficient to keep the total type I error at the α level. Considering the following interim analysis and final analysis as a new two-stage adaptive sequential design experiment, the total type I error of these two stages needs to be controlled at the $A(p_1)$ level. We assume that the boundary values of the rejection domain and the acceptance domain are α_2, β_2', respectively, in the second interim analysis, and the boundary value in the end-of-period analysis is β_3. As before, when $w_1\sqrt{\beta_2'} \geq \sqrt{\beta_3}$, it needs to satisfy

$$A(p_1) = \frac{{\beta_3}^2}{6w_1^2w_2^2} + \frac{4w_1\alpha_2\sqrt{\alpha_2\beta_3}}{3w_2^2} - \frac{w_1^2\alpha_2^2}{2w_2^2} - \frac{\alpha_2\beta_3}{w_2^2} + \alpha_2. \tag{20}$$

When $Q = 1$, it needs to satisfy

$$A(p_1) = \frac{6\beta_3(\beta_2' - \alpha_2) + 3w_1^2\left(\beta_2'^2 - \alpha_2^2\right) + 8w_1\alpha_2\sqrt{\alpha_2\beta_3} - 8w_1\beta_2'\sqrt{\beta_2'\beta_3}}{6w_2^2} + \alpha_2, \tag{21}$$

α_2, β_2', and β_3 can be calculated.

If the experimental stage is added in the above manner during the interim analysis, the corresponding parameters should also be adjusted in the reestimation of the sample size based on the conditional test power or the total test power. Referring to this idea, in the second interim analysis, we can also calculate the conditional type I error and continue to increase the analysis stage and make a reasonable sample size adjustment under the premise of controlling the conditional type I error.

The MCP statistic $T_1 = P_1, T_2 = (\sqrt{P_1} + \sqrt{2P_2})^2$ is used. After the interim analysis results are obtained, the sample size is reestimated, and the reestimation formula is

$$\widetilde{n}_2 = \frac{\widetilde{S}^2}{\widetilde{\theta}^2}\left(\phi^{-1}\left(1 - \frac{\left(\sqrt{\beta_2} - \sqrt{p_1}\right)^2}{2}\right) - \phi^{-1}(1 - cP)\right)^2. \tag{22}$$

Among them, $\widetilde{S}^2$ is the combined variance obtained from the interim analysis, $\widetilde{\theta}^2 = (\widetilde{\mu}_{\text{experience group}} - \widetilde{\mu}_{\text{control group}} + 1)^2$, $\widetilde{\mu}_{\text{control group}}\,\widetilde{\mu}_{\text{experience group}}$ is the mean of the control group and the experimental group in the interim analysis, respectively.

3. Statistical Analysis of Employment Education in Colleges and Universities Based on Improved Clustering Algorithm

Referring to the existing website and the actual needs of users, the employment distance education platform for graduates is divided into three types of users, namely, the student end, the training lecturer end, and the administrator. Each type of user corresponds to corresponding functional modules, and in the form of mobile applications, it can meet the needs of students to study anytime and anywhere and effectively solve the problem of employment difficulties for college graduates in the computer industry. The overall functional structure is shown in Figure 2.

By establishing a conceptual model, it is convenient to design the database table structure. According to the overall function diagram, the E-R diagram describing the entity is shown in Figure 3.

The shared intelligent warehouse leasing platform uniformly uploads the intelligent warehouse operation data to the enterprise big data platform for classification and screening, aggregation, extraction, mining, and analysis of scattered and repeated data to form valuable big data in logistics and warehousing. After that, the data can be applied to the coordination, management, collaboration, and decision-making of the whole process of enterprise control and management. The big data platform architecture is shown in Figure 4 which is divided into four layers: data source, big data acquisition, big data processing, and big data service.

The intelligent employment service of colleges and universities based on big data needs to contact various departments of the school. It needs to be based on big data thinking and technology to build an intelligent employment service model for colleges and universities that is oriented by

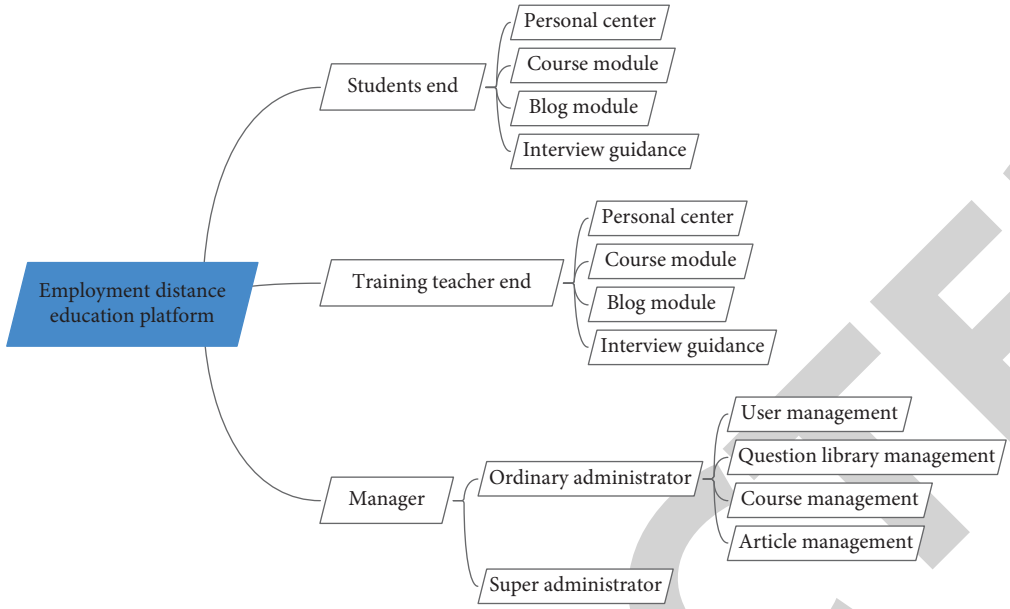


Figure 2: The overall functional structure of the employment education platform.

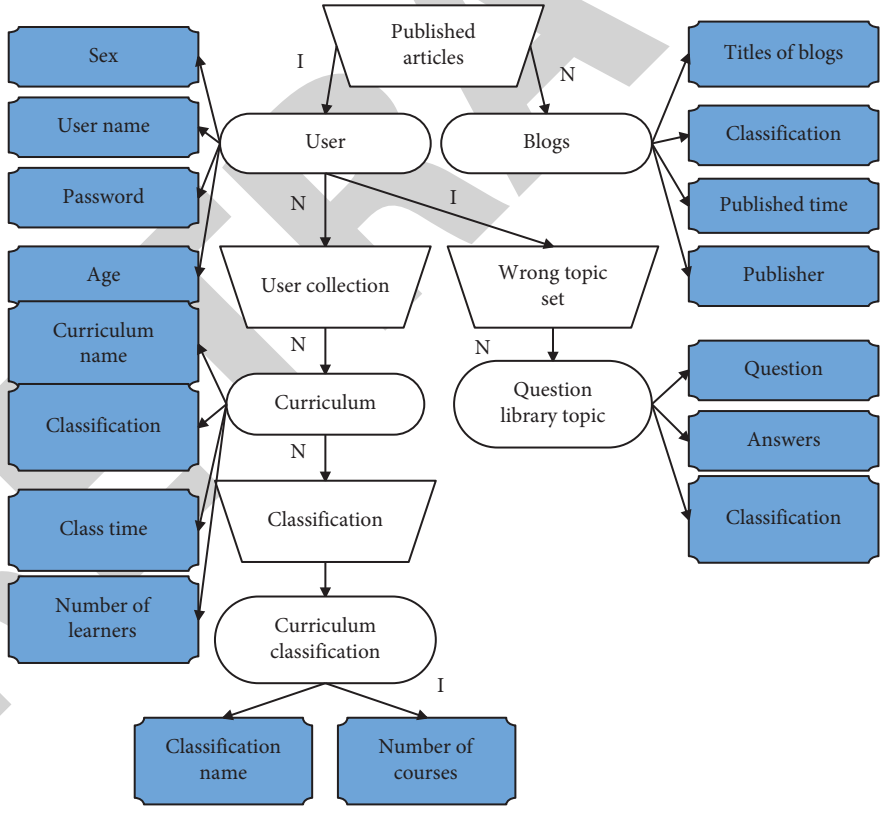


Figure 3: E-R diagram.

student training and centered on the precise employment of college students, integrating recruitment, education, evaluation, monitoring, and research and judgment, as shown in Figure 5.

Based on the intelligent employment service model, this research combines the front-end demand analysis to design the overall architecture of the intelligent employment platform based on the principle of "data consistency and on-demand sharing." The main contents and the logical relationship between them are shown in Figure 6.

This study integrates personal information, college career guidance information, and enterprise recruitment

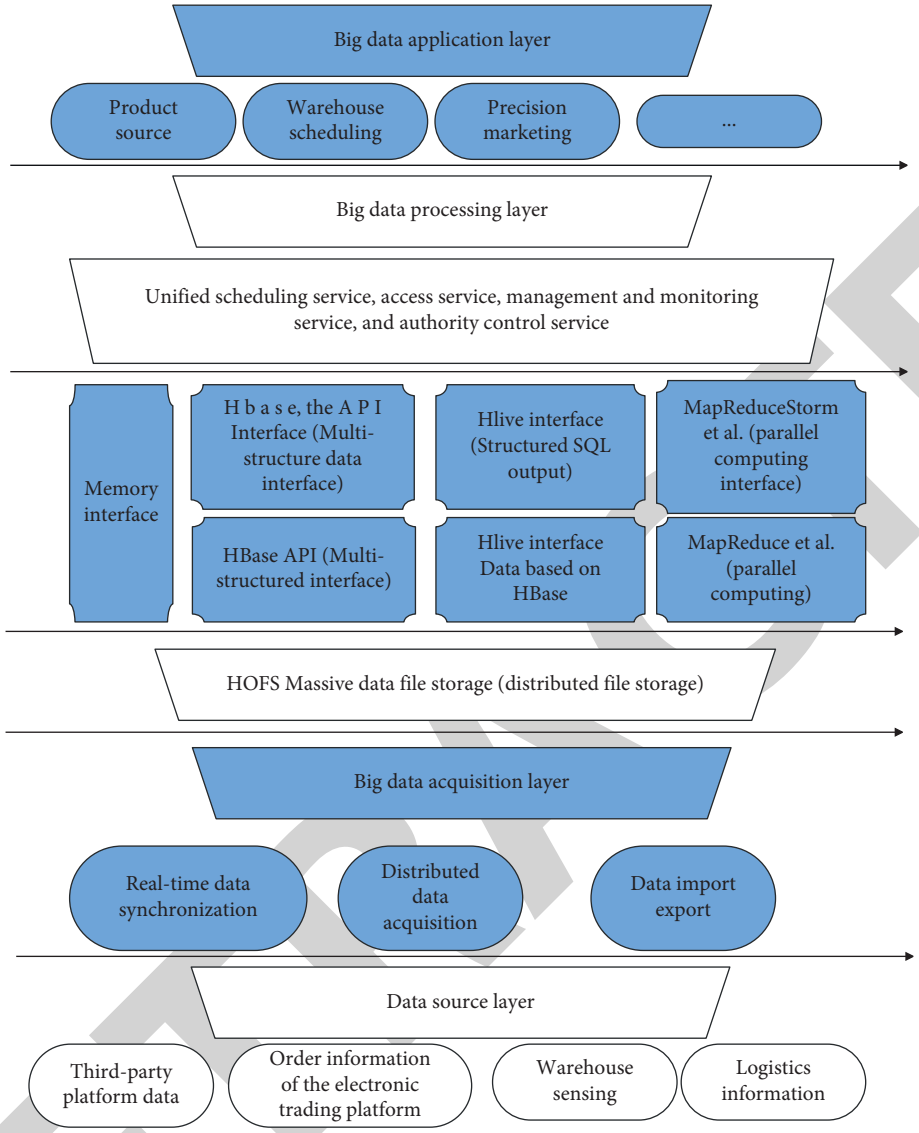


Figure 4: Warehouse big data application.

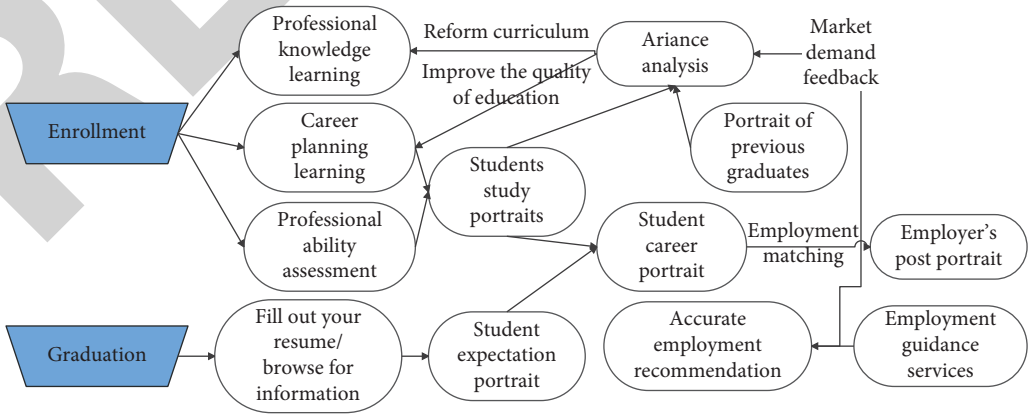


Figure 5: Intelligent employment service model in colleges and universities based on big data.

information in the three aspects of individual-college-enterprise to increase the communication between units and graduates, provide reliable recruitment channels, and solve the problem of graduate employment difficulties. Figure 7 shows an example of college employment information interaction.

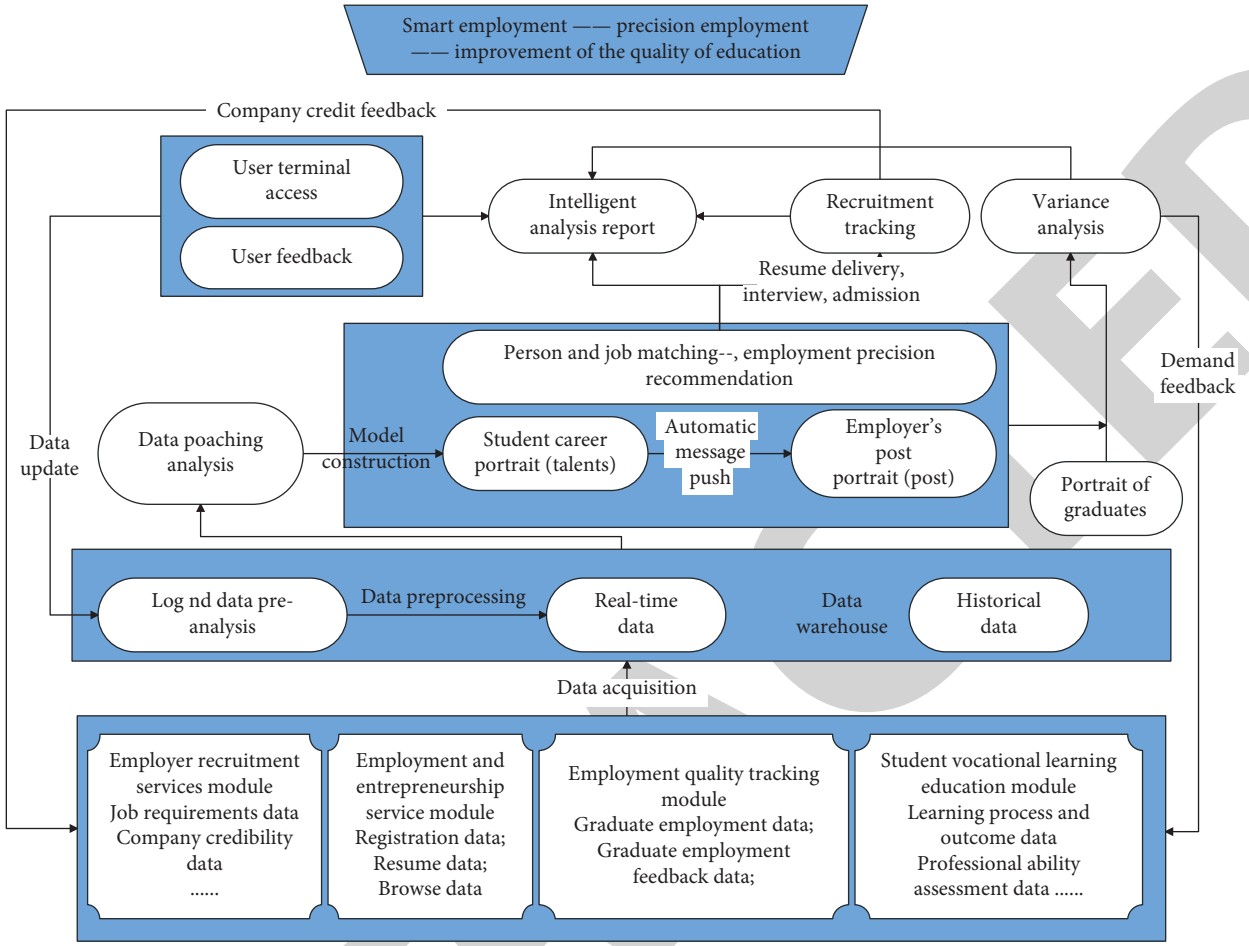


Figure 6: The overall architecture of the college intelligent employment platform based on big data.

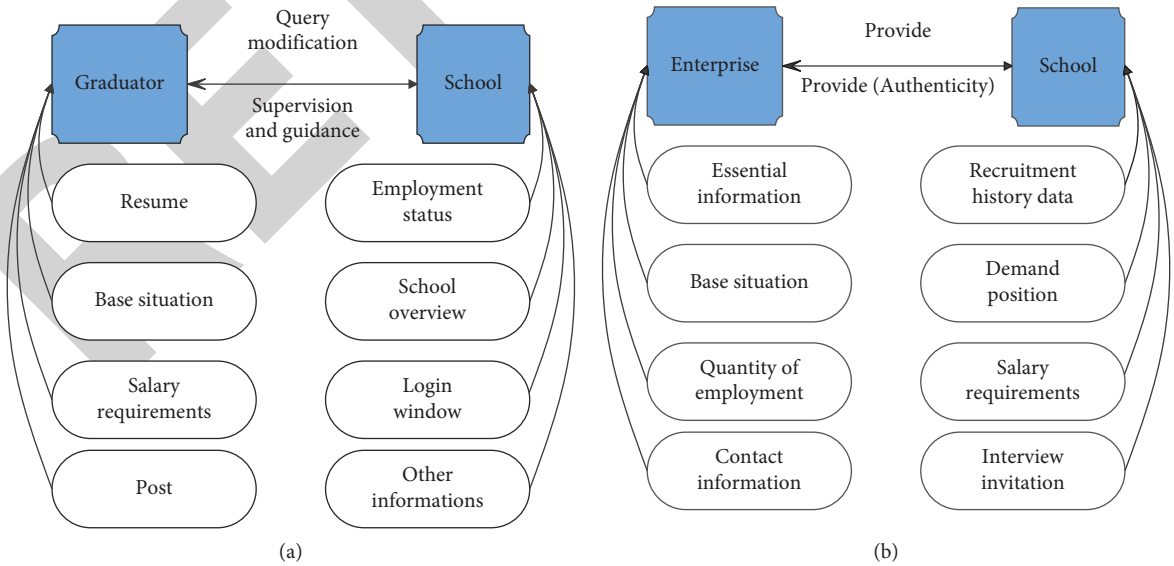


Figure 7: Continued.

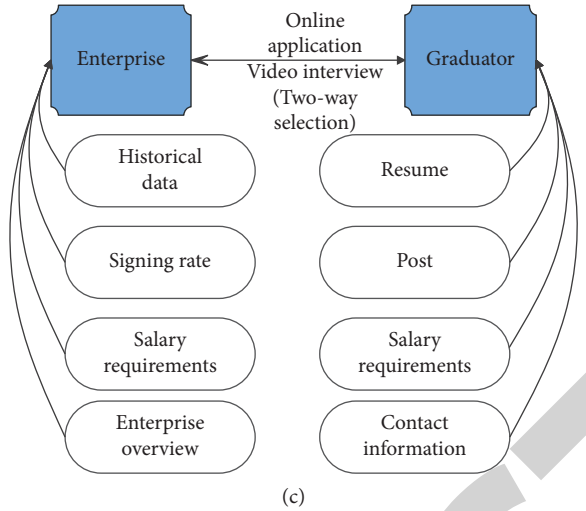


Figure 7: Example of college employment information interaction. (a) Information exchange between graduates and schools. (b) Information exchange between schools and enterprises. (c) Information exchange between graduates and enterprises.

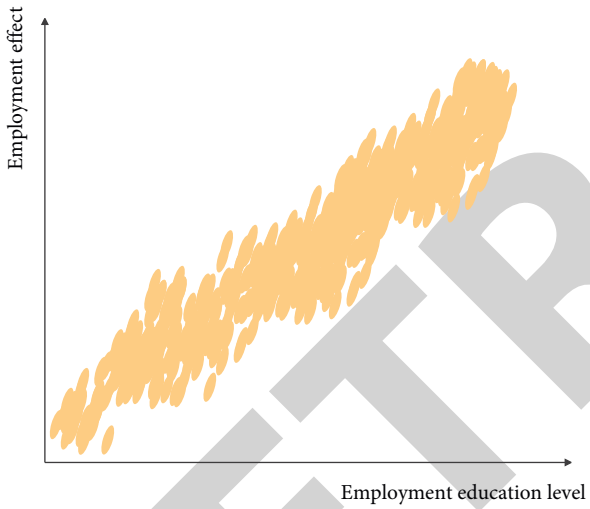


Figure 8: Simulation analysis of the clustering effect.

This study analyzes the effect of the improved clustering algorithm proposed in this study in the statistics of employment education in colleges and universities. The results of the statistical simulation test are shown in Figure 8.

Through the simulation analysis, it can be seen that the statistical analysis system of college employment education based on the improved clustering algorithm proposed in this study has a good effect in the clustering of employment education data. After that, this study analyzes the effect of the statistical analysis system of employment education in colleges and universities based on the improved clustering algorithm and obtains the results given in Table 1.

Through the above analysis, it can be seen that the statistical analysis system of college employment education based on the improved clustering algorithm proposed in this study can effectively improve the effect of employment education and has a certain role in promoting the employment of college graduates.

Table 1: Analysis of the effect of the statistical analysis system of employment education in colleges and universities based on the improved clustering algorithm.

Num	Employment education	Num	Employment education	Num	Employment education
1	82.55	9	77.52	17	78.36
2	78.69	10	79.55	18	80.07
3	80.60	11	76.97	19	82.96
4	82.36	12	83.66	20	76.20
5	77.38	13	76.36	21	82.98
6	83.14	14	78.71	22	80.48
7	83.79	15	77.66	23	80.29
8	81.00	16	80.05	24	79.02

4. Conclusion

In order to achieve full employment, students in colleges and universities must shape themselves into a high-level professional talent with all-round development and comprehensive quality and ability. The basic abilities they should have include the ability to adapt to the society, practical ability, innovation ability and interpersonal communication ability, management ability, expression ability, core competitiveness, decision-making ability, team spirit, both ability and political integrity, and learning ability. This study combines the improved clustering algorithm to conduct statistical analysis of employment education in colleges and universities to analyze the current situation of employment education in colleges and universities. Through the simulation analysis, it can be seen that the statistical analysis system of college employment education based on the improved clustering algorithm proposed in this study has a

Hindawi
Security and Communication Networks
Volume 2023, Article ID 9892320, 1 page
https://doi.org/10.1155/2023/9892320

Retraction

Retracted: Construction of University English Informatization Learning Environment Based on ESP Teaching Mode

Security and Communication Networks

Received 19 September 2023; Accepted 19 September 2023; Published 20 September 2023

This article has been retracted by Hindawi following an investigation undertaken by the publisher [1]. This investigation has uncovered evidence of one or more of the following indicators of systematic manipulation of the publication process:

(1) Discrepancies in scope

(2) Discrepancies in the description of the research reported

(3) Discrepancies between the availability of data and the research described

(4) Inappropriate citations

(5) Incoherent, meaningless and/or irrelevant content included in the article

(6) Peer-review manipulation

The presence of these indicators undermines our confidence in the integrity of the article's content and we cannot, therefore, vouch for its reliability. Please note that this notice is intended solely to alert readers that the content of this article is unreliable. We have not investigated whether authors were aware of or involved in the systematic manipulation of the publication process.

Wiley and Hindawi regrets that the usual quality checks did not identify these issues before publication and have since put additional measures in place to safeguard research integrity.

We wish to credit our own Research Integrity and Research Publishing teams and anonymous and named external researchers and research integrity experts for contributing to this investigation.

The corresponding author, as the representative of all authors, has been given the opportunity to register their agreement or disagreement to this retraction. We have kept a record of any response received.

References

[1] L. Feng, "Construction of University English Informatization Learning Environment Based on ESP Teaching Mode," *Security and Communication Networks*, vol. 2022, Article ID 5462618, 12 pages, 2022.

Hindawi
Security and Communication Networks
Volume 2022, Article ID 5462618, 12 pages
https://doi.org/10.1155/2022/5462618

Research Article

Construction of University English Informatization Learning Environment Based on ESP Teaching Mode

Ling Feng

Department of Public Foreign Language Teaching, Henan Finance University, Zhengzhou 450046, Henan, China

Correspondence should be addressed to Ling Feng; fengling@hafu.edu.cn

Received 28 May 2022; Accepted 23 June 2022; Published 11 July 2022

Academic Editor: Fang Liu

To further improve university students' English comprehensive quality and knowledge level, a kind of information analysis and evaluation system based on the English course was put forward and designed. The construction of the informatization learning environment was explored from the perspective of ESP theory, combining with the existing problems of English informatization teaching in universities. It aimed at promoting the transformation and development of the targeting of English teaching, the application of the curriculum system, the specialization of the teaching content, and the multidimensional evaluation mechanism. The results showed that the application of ESP teaching theory in the construction of an informatization learning environment could provide the system and resource guarantee for the innovative development of the English teaching model and further optimize the English teaching method. Through a semester of The Foundation of University Information Technology MOOC study and practice in the practical operation of the evaluation system, the pass rate of each college was over 80%. And 91% of the students scored more than 60 in the final exam and 35% of the students scored more than 90.

1. Introduction

With the deepening of national education system reform, an adjustment must be made timely and innovation is required for the modernization of teaching in colleges and universities. And with the continuous development of network technology and mobile communication technology, the new technology based on modern information technology begins to gradually fuse into the field of university English teaching and learning environment [1]. Both the network teaching mode based on multimedia and the independent learning platform have been widely used in university English teaching and other related information technologies have gradually been integrated into university English teaching. It can be said that the informatization development of modern education has become the inevitable choice of educational innovation and development in the new era. Under the informatization environment, the construction of university English teaching mode and informatization learning environment is also the inevitable trend of English teaching reform and innovation in the future. Therefore, how to apply information technology to university English teaching and innovate the existing English teaching environment is the current focus of university English research [2].

2. Literature Review

Shamsudin and Majid believed that social environment, predictive factors, process factors, and learning effects jointly affected English teaching in the process model of English teaching. Some scholars believed that the course goal was to meet the actual job demand for employment and the core of the course content was to develop vocational skills in this teaching model, with teachers and students playing the most important roles [3]. According to the language requirements, cultural background, English proficiency, and career goals of vocational students, it was divided into several different models by Lee. The second language mode was the language training for employment and job environment. Vocation mode referred to the training of language skills related to a specific occupation or the occupation through the simulation of occupational scenarios. Work experience

mode combined experience of workplace and VESL classroom teaching so as to train. The field mode was the training of language skills related to specific work areas, which were carried out in the context of a specific workplace [4].

Foreign scholars created a system to help people learn foreign languages for free. It was found by Veselov et al. that when Spanish native speakers just started to learn English pronouns such as "he," "she" and "it," the word "it" tended to cause confusion and anxiety in learners. Because it was difficult to translate into corresponding Spanish. Therefore, he tried many times to get the best way for Spanish people to learn English, which was that "he" and "she" were only taught at first and then "it" was taught a few weeks later when the number of people who insisted on learning increased significantly, thus improving the number of people who insisted on learning significantly [5]. Baram et al. believed that the teaching method presented us with a way of big data reshaping education, which reflected that big data technology could effectively analyze and intervene in learning. The mechanism of how to collect behavioral data of learners and obtain information from it was designed [6]. Ruge and Mackintosh believed that with these learning behavior data, big data analysis could solve those problems that were difficult to solve in the past. For example, which questions did learners spend more time answering, right questions or wrong questions? The reason for learners' wrong answers is their insufficient understanding of the content or physical and mental exhaustion [7]. Gan et al. believed that the most suitable learning path for learners could be planned through data analysis. Teachers and parents could also obtain learners' learning progress reports through the digital panel, so that learners could play an active role in learning. This teaching method highlighted the changes in teaching and learning in the era of big data and the analysis results of learners' learning behaviors could be used for teaching improvement [8]. The structured system proposed and constructed by Han and Chen provided learners with the freedom to choose the content they were interested in as much as possible. And he studied the data that learners searched and learned on the Internet and the data that learners communicated and exchanged with each other, so that teachers could master learners' learning behaviors [9]. According to the actual learning behavior based on the situation, Huang provided advice and counseling to students and the proposed and designed system had functional modules related to the study of learners' behavior and evaluation, mainly studying learners' learning behavior data and learners' feedback to the learning system so as to evaluate learners' learning behavior [10].

Based on the present research, a kind of information analysis and evaluation system based on the English course was put forward and designed. The construction of the informatization learning environment was explored from the perspective of ESP theory, combining with the existing problems of English informatization teaching in universities. It aimed at promoting the transformation and development of the targeting of English teaching, the application of the curriculum system, the specialization of the teaching content, and the multidimensional evaluation mechanism.

3. English Course Information Analysis and Evaluation System

3.1. Course Learning Platform

3.1.1. Learning Platform. The rapid rise of Massive Open Online Courses (MOOC) and other large-scale open online courses has prompted the reform of traditional teaching mode and management system, which bring new opportunities and challenges to the teaching reform of colleges and universities. Facing the "digital tsunami" in the history of education, in order to participate in, explore and innovate college computer basic education suitable for the Internet era actively, several colleges and universities in Fujian province jointly produce the MOOC quality teaching video of The Foundation of University Information Technology, which has been released on the MOOC cloud platform [11]. The MOOC resource is fully open and accessible to learners at any time. Supported by The Foundation of University Information Technology, various universities can carry out mixed a teaching mode including classroom teaching, online learning, SPOC, and Flipped Classroom (Learners complete knowledge learning after class, and classroom becomes a place for the interaction between teachers and students and between students). There are 39 videos and 8 chapter tests. So the points of the video task account for $39/(39+8) = 82.98\%$ and the points of the chapter test task account for $8/(39+8) = 17.02\%$. As shown in Figure 1.

3.1.2. Comprehensive Evaluation Method of Theoretical Courses. The comprehensive means of a process evaluation method and a summative evaluation method were adopted in the MOOC of The Foundation of University Information Technology. The purpose of the comprehensive evaluation was to encourage learners to pay more attention to the learning process [12].

3.1.3. Analysis of Overall Learning Behavior

(1) Statistics of Access Times in Each Period. From November 1, 2019 to January 6, 2020, a day not on school holidays from Monday to Friday was randomly selected and a total of 20 days were randomly selected for the statistics of learners' active time period within 24 hours of a day. As shown in Figure 2.

It can be seen that learners' access to the platform improves significantly from 20 o'clock and the number of clicks drops sharply after 21 o'clock. The active trend of learners on the platform is also consistent with their learning rules in school life.

(2) Statistics of Learners' Accessing Learning Way. According to the statistics of learners' access to MOOC on the platform, it is found that most learners use mobile clients to access courses. As shown in Figure 3.

It can be seen that most learners use mobile clients to access the MOOC of The Foundation of University Information Technology. When teachers assign teaching tasks or

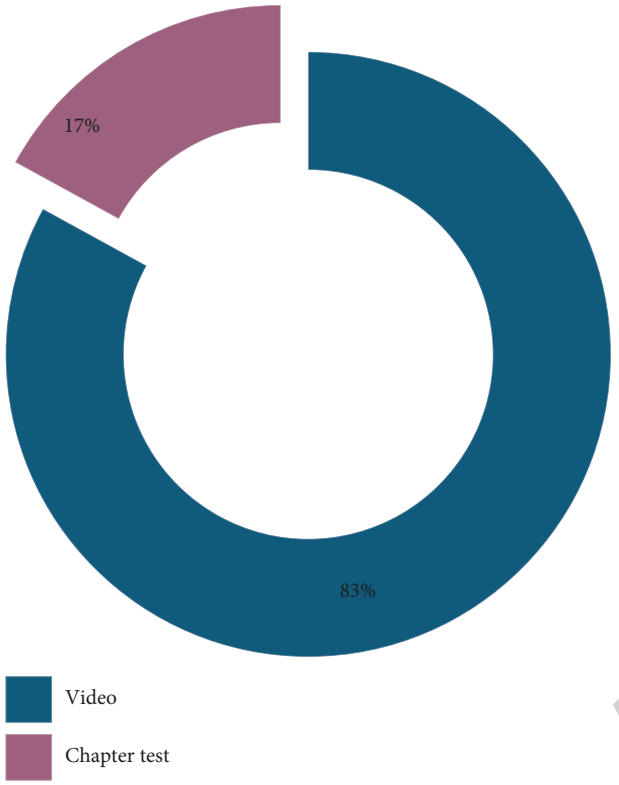


Figure 1: Distribution of the course task points.

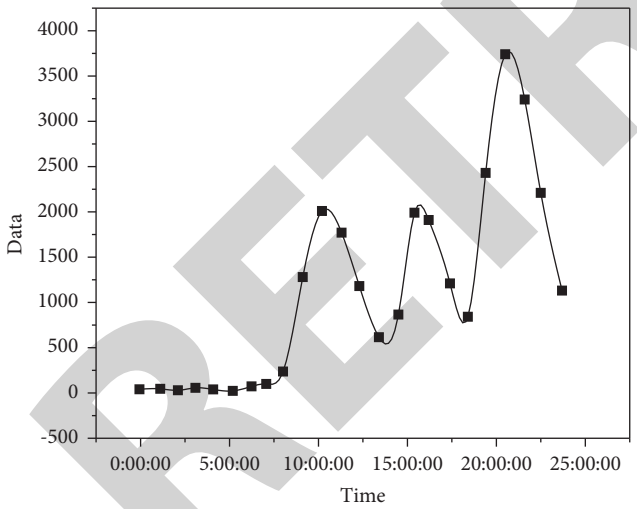


Figure 2: Statistics of access times in each time period.

ask questions online, they should give full consideration to the operations that can be completed on mobile terminals [13].

3.2. Cluster Analysis of Learning Behavior. In order to understand the relationship between the behavior of each type of learners watching videos in the chapter and the learning effect (chapter test), the learning behavior of each video in MOOC of The Foundation of University Information

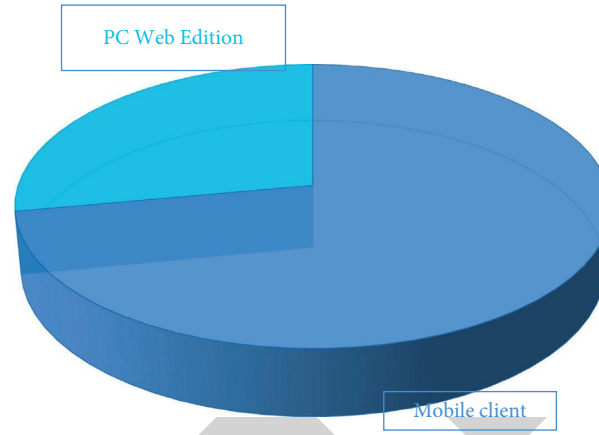


Figure 3: Statistics of learners' accessing learning way.

Technology was combined respectively according to eight chapters and the percentage of learners watching videos in each chapter was counted, as shown in formula.

$$N = \frac{\sum_{p=1}^{k}\left(m_p * L_p\right)}{\sum_{p=1}^{k} L_p}. \quad (1)$$

In formula (1), N is the viewing rate of a video in a chapter. k is the number of videos in the chapter. m_p is the viewing rate of the pth video in the chapter and L_p is the length of the pth video in the chapter. Therefore, the correlation analysis between "learning behaviors of watching chapter videos" and "learning effects of chapter tests" can be carried out.

After the mean clustering of learning behaviors was carried out, learners were divided into 4 cluster members. And the average score of theoretical scores of these 4 cluster members was counted. It was found that cluster member 1 had the highest score and cluster member 3 had the lowest score.

3.2.1. Comparative Analysis of Watching Videos. The behavior data log of watching videos in learners' learning behaviors was extracted and analyzed. To compare the differences of learning behaviors of watching course videos in four clusters, the average value of watching duration ratio from video 1 to video 8 of four clusters was drawn here, as shown in Figure 4.

As shown in Figure 4, the frequency of watching videos of learners of different groups varied greatly. The progress of watching videos of samples in different clusters varied widely, indicating that the overall situation of learners in different clusters was not stable. Because the frequency of watching videos of some learners differed greatly from that of other learners [14].

3.2.2. Comparative Analysis of Chapter Test. The submitting time of eight tests for the learners in cluster 0 is shown in Figure 5. It could be found that there were almost no existed learners not submitting test in the cluster 0. By and large, the completeness degree was higher for cluster 0 learners in

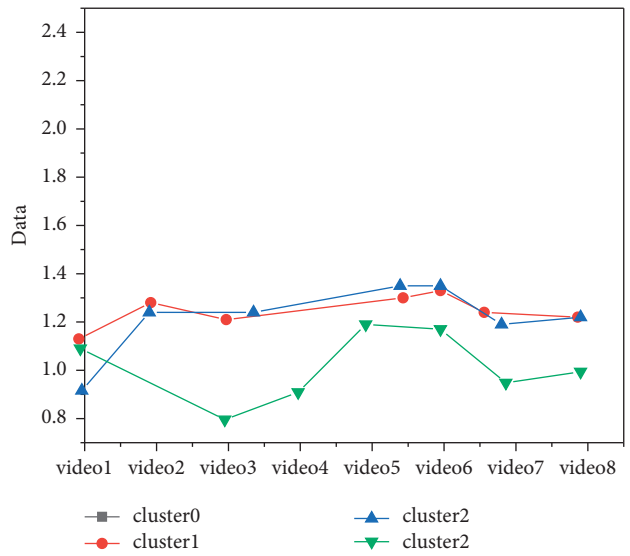


Figure 4: Video duration of watching 8 chapters by four clusters.

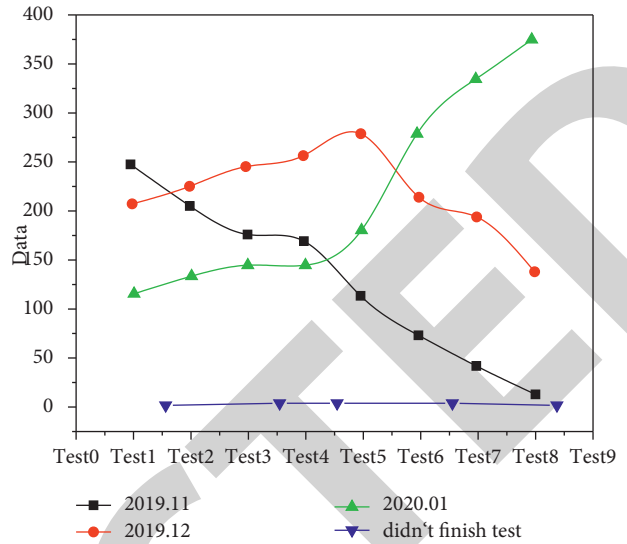


Figure 6: Learners' eight tests submission time in cluster 1.

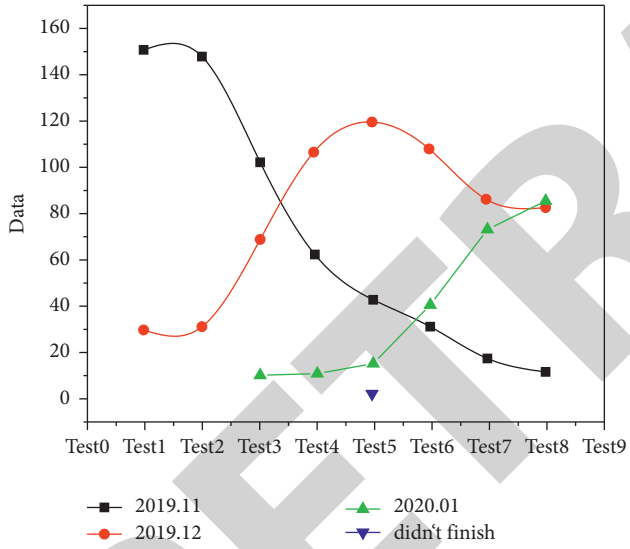


Figure 5: Learners' eight tests submission time in cluster 0.

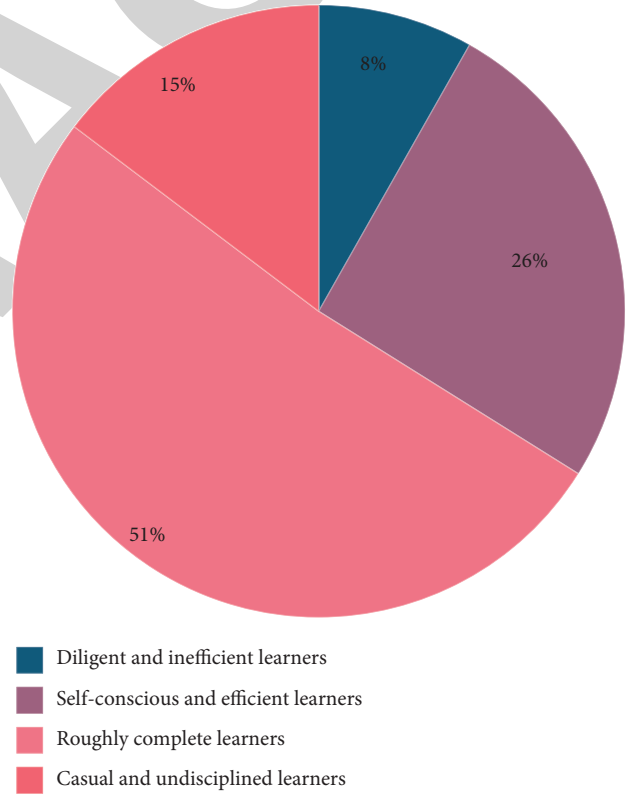


Figure 7: Proportion of the four types of learners.

online test, indicating that they had a more serious learning attitude. A part of learners in cluster 0 submitted the homework before January. The cluster 1 learners' learning habit was worse than the cluster 0 learners' learning habit. It could be seen from Figure 6 that some cluster 1 learners finished the test of each chapter in January 2019. A small number of learners could review and test what they learned through the chapter test timely to ensure the learning time. All the learners in cluster 1 almost submitted all tests. And most of these learners were science and engineering majors and had a certain theoretical basis.

3.2.3. Learning Model Summary and Suggestions. As can be seen from Figure 7, the roughly completing learners accounted for a majority in the four types of learners. They had good study habits and finished the chapter test immediately after learning the teaching video at the beginning, but the learners' enthusiasm on completing the test declined over time. And the value of chapter test were not valued. They just took the test as a mandatory task, so their final score was not the highest. These learners mainly learned knowledge through the course videos and could pass the course.

For different types of learners, teachers can adopt different personalized methods to assist learners to improve their scores. The roughly completing learners account for a majority in the four types of learners. For such learners, teachers should encourage them to keep their good learning habits at the beginning and remind them to pay attention to the teaching video knowledge and chapter tests in daily life, using chapter tests to consolidate what they have learned instead of cramming before exams [15].

3.3. Analysis of Learning Behavior Characteristics Effectiveness

3.3.1. The Engineering of Learning Behavior Characteristics. The unit tests in the MOOC of The Foundation of University Information Technology were graded. Those whose scores were greater than or equal to 0 and less than 10 were divided into level 1. Those whose scores were greater than or equal to 10 and less than 20 were divided into level 2. As shown in formula (2), where K is grade and G is score. Set a failing grade below level 6. The calculation formula is as follows.

$$K = \text{int}\left(\frac{G}{10}\right). \tag{2}$$

3.3.2. Gini Index Analysis. Gini index can be used as a measure of feature weight and is widely used in feature selection of decision trees. The Gini index is also used to measure the "impure degree" of data. When the data comes from the same category, the Gini index is 0. When the data comes from two categories with half of each, the Gini index reaches the maximum value of 0.5 [16]. The smaller the Gini index is, the lower the probability that the selected samples in the set are misclassified. That is to say, the higher the purity of the set is, the less pure the set is. Gini index is defined as formula.

$$Gini(P) = \sum_{c=1}^{N} P_c\left(1 - P_c\right) = 1 - \sum_{c=1}^{N} P_c^2. \tag{3}$$

Description of Gini index analysis algorithm:

(1) For sample D in set D, Pc represents the probability that sample D belongs to category C, so the probability of wrong selection is (1-Pc).

(2) There are C categories in the sample set and a sample randomly selected can be assigned to any of these C categories.

(3) When it is dichotomous

$$Gini(D) = 2P_c\left(1 - P_c\right). \tag{4}$$

(4) When it is C category

$$Gini(D) = 1 - \sum_{c=1}^{C} P_c^2. \tag{5}$$

Suppose that there are 15 samples in the current training set S, among which 5 are positive classes and the other 10 are negative classes. The Gini index corresponding to the training set can be calculated as follows:

$$P_+ = \frac{5}{15} = \frac{1}{3},$$

$$P_- = \frac{10}{15} = \frac{2}{3}, \tag{6}$$

$$Gini(S) = 1 - \left(\frac{1}{3}\right)^2 - \left(\frac{2}{3}\right)^2 = 0.44.$$

(5) The Gini index can be used to select the optimal feature in the classification tree. If sample set D is divided into D1 and D2 according to the value a of feature A, then under the condition of feature A, the Gini index of set D is as follows:

$$Gini(D, A) = \frac{|D_1|}{|D|} Gini(D_1) + \frac{|D_2|}{|D|} Gini(D_2). \tag{7}$$

Suppose there is such a set of performance dataset. The sample set has nine samples and each sample has three characteristics (Test1, Test2, Test3). One sample has the result of a pass or a fail.

In this sample, the set of values of Test 1 = {6, 7, 8};

In this sample, the set of values of Test 2 = {5, 6, 7};

In this sample, the set of values of Test 3 = {5, 7, 8};

In this sample, the set of the final grade values = {pass, fail};

Test1:

$$D1(\text{Test1} = 6), D2(\text{Test1} = 7), D3(\text{Test1} = 8),$$

$$|D| = 9, |D1| = 4, |D2| = 93, |D3| = 2,$$

$$Gini(D, \text{Test}) = \frac{|D^1|}{|D|} Gini\left(D^1\right) + \frac{|D^2|}{|D|} Gini\left(D^2\right) + \frac{|D^2|}{|D|} Gini\left(D^3\right). \tag{8}$$

$|D^1| = 4$. The pass number is 1 and the number of fail is 3.

$$Gini\left(D^1\right) = 1 - \left(\frac{1}{4}\right)^2 - \left(\frac{3}{4}\right)^2 = 0.375. \tag{9}$$

$|D^2| = 3$. The pass number is 2 and the number of fail is 1.

$$Gini\left(D^2\right) = 1 - \left(\frac{1}{3}\right)^2 - \left(\frac{2}{3}\right)^2 = 0.444. \tag{10}$$

$|D^3| = 2$. The pass number is 1 and the number of fail is 1.

$$Gini\left(D^3\right) = 1 - \left(\frac{1}{2}\right)^2 - \left(\frac{1}{2}\right)^2 = 0.5,$$

$$Gini(D, \text{Test}) = \frac{4}{9} * 0.375 + \frac{3}{9} * 0.444 + \frac{2}{9} * 0.5 = 0.425. \tag{11}$$

By using this method, the values of Gini (D, Test2) and Gini (D, Test3) can be calculated. It can be seen that which feature has the greatest impact on the final grade. By using Gini coefficient method to analyze learning behavior feature weights, it is found that timely submission of chapter tests has the greatest impact on grades. Teachers should set the chapter test submission time in the Mooc platform chapters and monitor learners to complete the test timely after class to consolidate their knowledge of learning. Learners are urged to watch videos carefully.

3.4. System Function Requirements. System design is C/S architecture. To reduce the size of the installation package, the installation program is divided into server installation package, client installation package, and teacher installation package. Different users log in on different software interfaces. After successful login of legitimate users, they can enter corresponding modules and perform related operations.

3.4.1. System Function Requirements. The system users are divided into three kinds of users including administrators, teachers and students. The three kinds of users must be authorized by the system to use the related system resources. The system resources used by authorized users are determined by user identities. Administrators are mainly responsible for subject management, program management, question bank management, student management, task management, parameter management, monitoring management, connection management, statistics management, software update, authority management, log management, etc. See Figure 8. Teachers mainly have the authority of invigilation management and other permissions are determined by the administrator [17].

Through the system, students can change the password, conduct online practice, view the results, view risk evaluation, online test, and so on. See Figure 9.

3.4.2. System Function Analysis. Based on the needs of various users of the system, the system should have basic functions closely related to the evaluation system, including the following routine function operations, as shown in Figure 10:

The main purpose of this system is to improve the work efficiency of teachers in our school and to facilitate teachers to supervise the learning state of learners. In this learning process, learners can also be encouraged to learn regularly so that learners can have the most fundamental learning pressure at any time, preventing the interruption of learning due to the loss of learning interest. At the same time, in the learning process of learners, teachers can correct learners' learning style timely, promote learners to study according to their learning objectives, and strive to achieve learning tasks [18].

The practical operation evaluation system platform has complex functions. Due to the limited space of the article, only part of the function structure is shown in Figure 11.

(1) Program Management Function. The program management provides all the functions related to the practice operation and examination, including creating, editing, browsing and deleting examination paper program, generating, editing, deleting, and printing examination paper, etc. For learners to practice and take tests on the client, administrators or authorized teachers need to set up a plan first.

(2) Learning Behavior Risk Evaluation. First of all, the score of each learner who takes this course is counted and the average score of each learner is obtained. The ranking is calculated according to the evaluation score of each learner and the percentage of ranking is obtained. Then it is compared with the percentages of excellent, good, medium, pass, and fail in the final exam of the learners in the last semester to get the corresponding risk level. The system will present the corresponding risk evaluation to learners according to the corresponding risk level [19].

The system compares the ranking percentage of the average score of learners in all tasks with the percentages of excellent, good, medium, pass, and fail in the practical operation final exam of learners in the last semester to get the corresponding risk level.

4. Construction of English Informatization Learning Environment Based on ESP Theory

4.1. Teaching Characteristics and Feasibility Analysis

4.1.1. Characteristics of ESP Theory Teaching. For ESP teaching, different teaching situations are set up for students and communicative tasks are simulated in specific situations. All communicative tasks are carried out around the application of relevant professional knowledge. For example, in the English course teaching of architecture major, students can simulate the communication of work site projects, describe the specific accident site, explain the use of equipment and prepare for work meetings, etc. After class, students can contact front-line construction workers and understand the details of the process or work link at the work site. Teachers' teaching also focuses on how students use English in relevant working environments [20].

In addition, ESP theory has the following characteristics. As shown in Table 1.

4.1.2. The Feasibility of ESP Theory in Higher Vocational English Teaching. Closely integrated with majors, ESP teaching is practicability-oriented, which focuses on the combination of English teaching and majors to cultivate students' pragmatic competence. A high level of professional English skills should be mastered. The idea that the ability to use English and professional skills are the same is emphasized. The starting point and central point of setting ESP teaching objectives is the demand analysis, extracting English applications that are suitable for the profession or academic field and then integrating words, syntax, and other factors in teaching to make the teaching path more relevant and practical. The goal of English teaching in higher

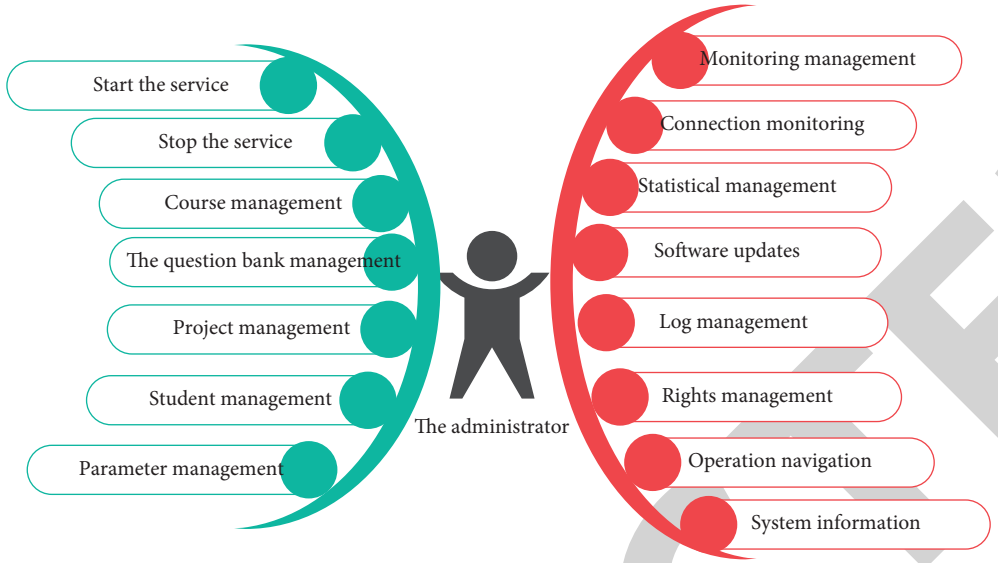


Figure 8: Administrator use case diagram.

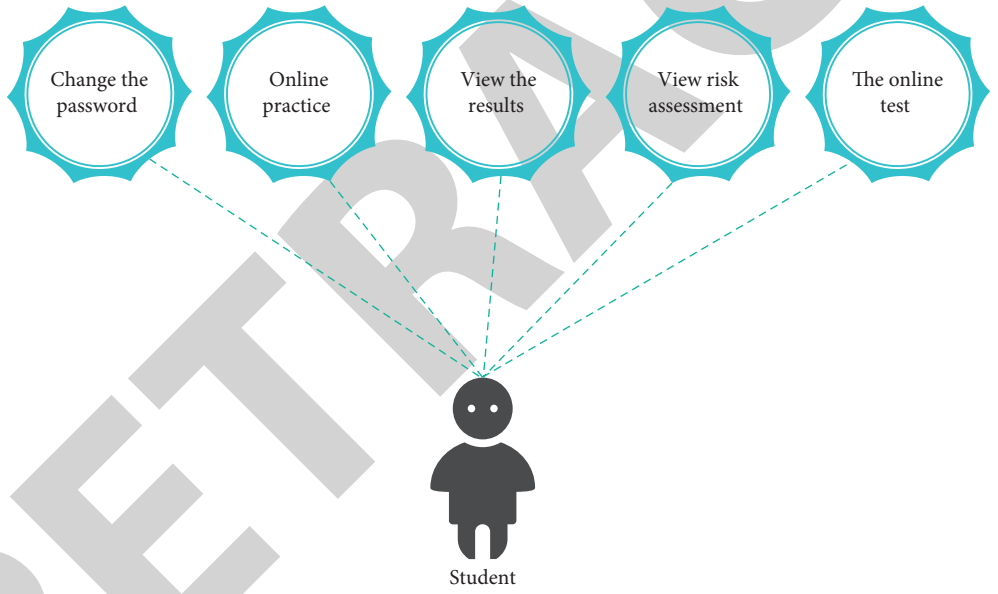


Figure 9: Student user use case diagram.

vocational colleges is to train students to complete their future job tasks with the help of English. It can be seen that ESP teaching objectives are consistent with higher vocational English.

4.2. Mode Construction. Through the combination of quantitative analysis and qualitative analysis, a higher vocational college in Qinhuangdao is taken as an example and its English teaching mode is analyzed. And the problems existing in the current teaching mode are pointed out. To solve these problems fundamentally, we must reform the teaching mode. In the author's opinion, only under the guidance of ESP theory can the current situation of "learning English cannot be applied" in higher vocational colleges be solved and basic English can be combined with professional English, so that students can consolidate their English foundation, enlarge their vocabulary and reading ability of professional English and meet the needs of future work [21]. Under the guidance of ESP theory, feasible solutions are put forward.

As shown in Figure 12, ESP courses should be based on demand analysis. Skills training in listening, speaking, reading, writing, and translation are implemented, covering all aspects of skills and knowledge in students' professional fields to meet their professional needs.

4.2.1. Contextualization of English Teaching Materials. When compiling ESP textbooks, teachers should spend more time on the training of students' language output skills. Centering on teaching objectives, combining students'

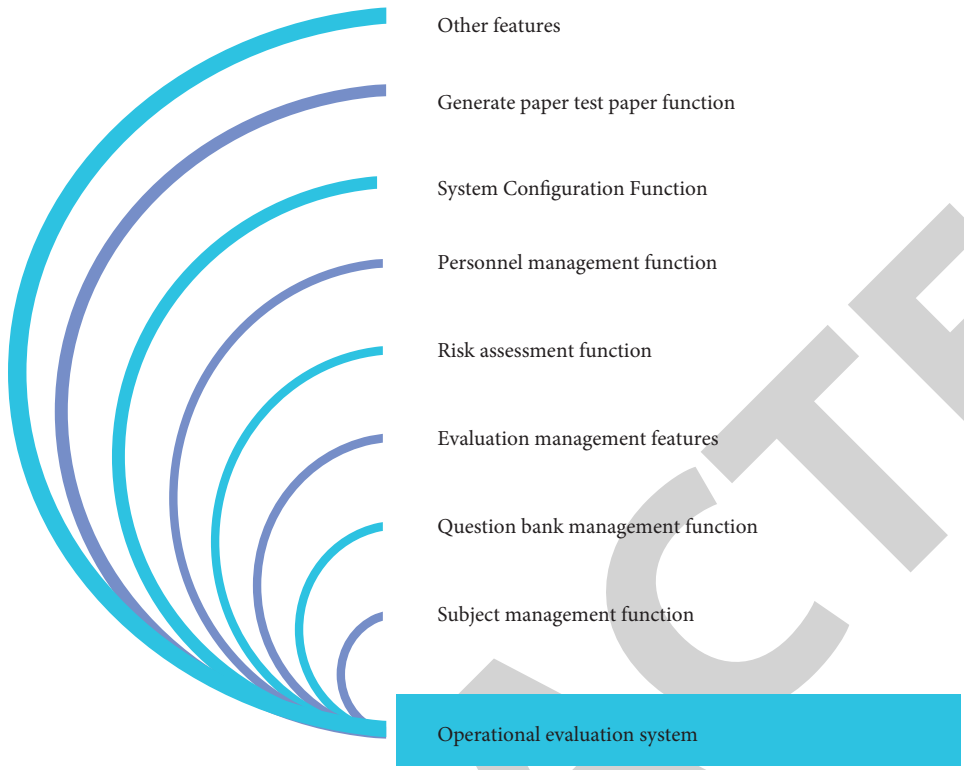


Figure 10: System function module diagram.

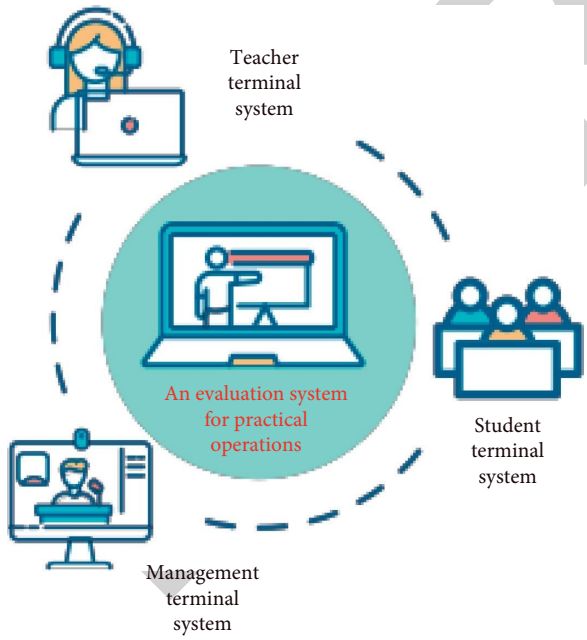


Figure 11: Partial function structure of the practical operation evaluation system.

majors and students' different learning demands and knowledge levels, teachers should design simulated situational tasks imitating real professional situations to cultivate students' English application ability. Teachers should ensure that students are fully and truly taught English for specific purposes. At the same time, combined with the real context and case analysis, the after-class exercises are designed so that students really can apply what they have learned.

4.2.2. Practicability of Teaching Methods. Teaching methods can also use heuristic method, case analysis method, situational performance method, role simulation method, communicative contrast method to encourage students to participate in interaction and mobilize their enthusiasm of students. At the same time, with the help of multimedia network resources, teachers can create a real language environment for teaching and practice. The competition method can be adopted after class to encourage students to participate in various English competitions and improve their English level. Teachers can also strengthen school-enterprise cooperation, bringing students to the enterprise to observe and learn or even combining some practical operation links of the enterprise to let students use English to realize the use of the ESP teaching method. For English major teaching in automobile parts, teachers can guide students into the university training building and the form of interactive question and answer in English can be adopted. ESP teaching methods are diversified, which are easy to arouse students' interest. There is a large independent learning space for students to choose. Students can learn English and use English in a relaxed and efficient learning atmosphere so as to achieve a good learning effect.

4.2.3. The Multidimensional Evaluation Mechanism. Scientific and reasonable evaluation is a strong guarantee of teaching reform. Teachers should change the traditional

Table 1: Absolute and variable characteristics of ESP.

Absolute characteristics	Variable characteristics
(1) The curriculum of ESP is learners' specific requirement	(1) ESP teaching is not limited to language learning
(2) The teaching content of ESP is related to the specific subject, occupation, and activity	(2) ESP teaching methods are flexible and varied
(3) ESP teaching should be carried out with the help of teaching activities of relevant majors	(3) ESP teaching objects are not limited to learners with no foundation, but apply to elementary, middle, and advanced learners

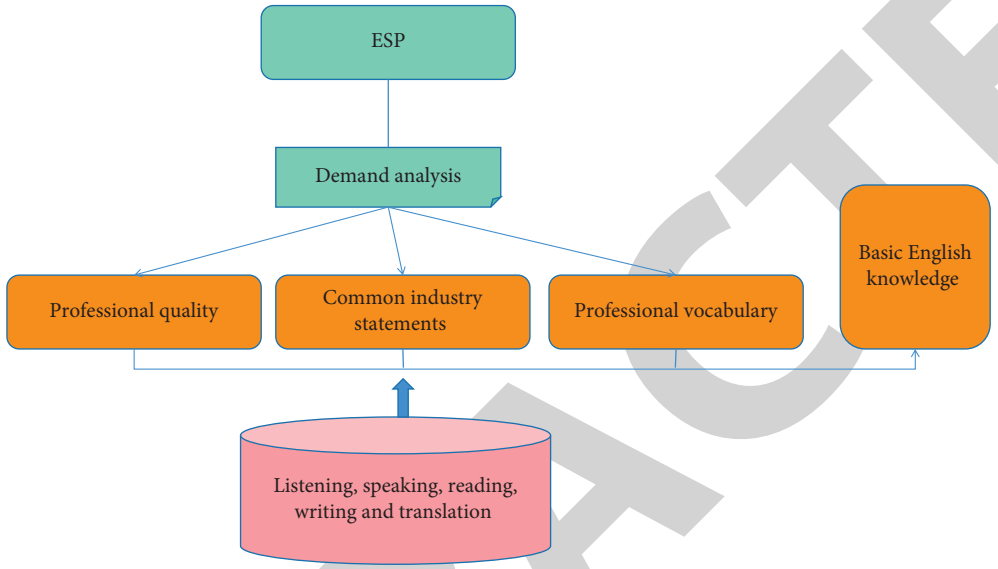


Figure 12: Demand analysis.

single evaluation method, pay more attention to the application and context of English language skills and value the ability to use English to solve problems related to the major. A multi-level evaluation system is established from pure language knowledge evaluation to professional English ability evaluation. At the same time, teachers should pay attention to the evaluation of practical ability and the evaluation of students' learning ability in the learning process, constructing the combination of the evaluation mechanism of "knowledge and ability, school and enterprise, curriculum and certificate." In addition, the evaluation has also formed a variety of forms, such as the students' mutual evaluation panel reports and the learning process programs evaluation certificate, so that students have the practical application ability required by the target position.

4.3. Comparison of Final Score between the Theoretical Learning Behavior Clustering and the Practical Operation

4.3.1. Comparison of Teaching Effects before and after Using the Evaluation System. Before the use of the evaluation system, the usual exercises are manually changed by the teacher and the final exam will be taken as the result of the practice final exam. The learning effect of learners before using the system with that after using the system is compared. It is found that the teaching effect improved significantly after using this system. The statistical distribution of each score segment is shown in Figure 13.

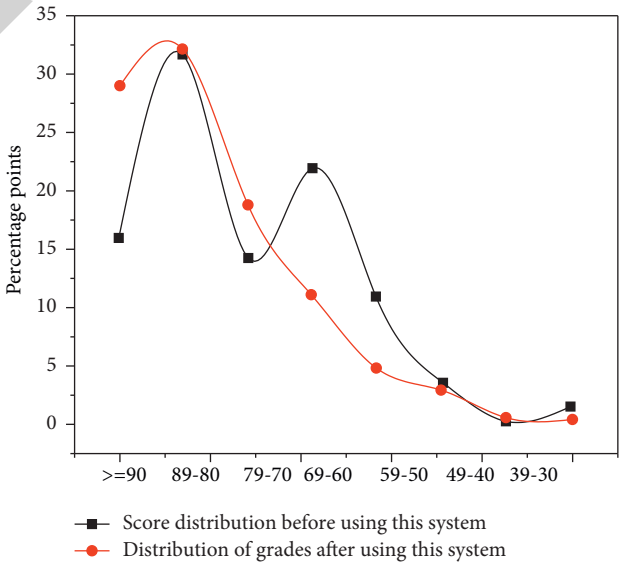


Figure 13: Semester score distribution before and after using the system.

In Figure 13, the pass rate increased by nearly 7 percentage points and those with scores above 90 increased by 13 percentage points.

4.3.2. Analysis of the Entrance Test and the Final Examination Results. To know how well students have mastered

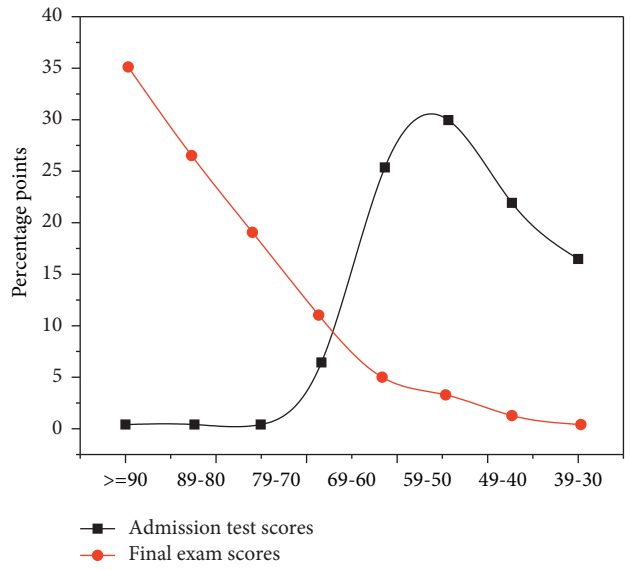


Figure 14: Statistics of scores in the entrance examination and the final examination.

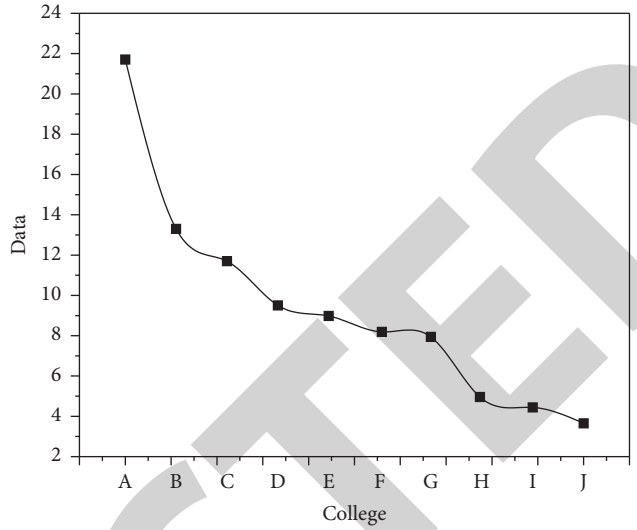


Figure 15: Entrance test of each college.

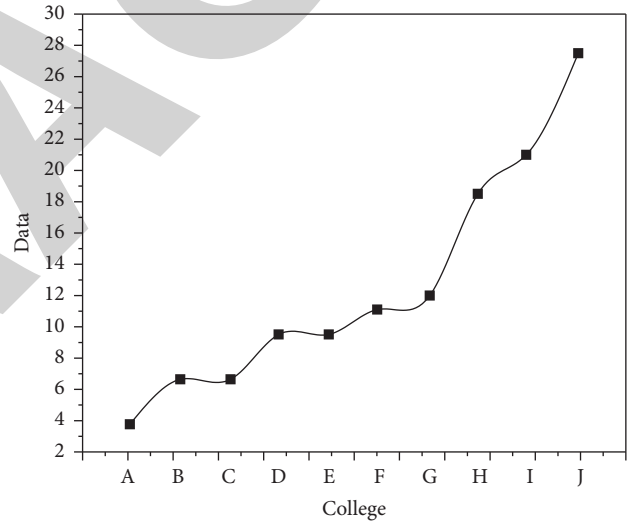


Figure 16: Pass improvement rate of each school in the final examination and the entrance test.

the course The Foundation of University Information Technology before entering the university, an entrance examination was organized for freshmen at the beginning of the first semester in 2018-2019, the results of which was compared with in the results of the final examination.

(1) Statistical Analysis of Each Score Segment. As shown in Figure 14, the proportion of students who scored more than 60 points in the entrance examination was 7.4%. Most of them were in the 60–70 area, accounting for 6.7%. It could be seen that more than 90% of the students did not meet the requirements of The Foundation of University Information Technology. The proportion of students with more than 80 points was 0.1%, indicating a very low excellent rate. The total score of the students was mainly concentrated in the range of 50–60 and 40–50. The sum of the two segments accounted for 55% of the total number of students, indicating that more than half of the students had the basic ability of computer application, but their grasp was not solid enough and their level needed to be improved.

After a semester of The Foundation of University Information Technology MOOC study and practice in the practical operation of the evaluation system, 91% of the students scored more than 60 in the final exam and 35% of the students scored more than 90. It could be seen that 91% of the students met the requirements of the course and a considerable proportion of students had a very solid grasp of knowledge.

(2) Pass Statistics of Each College. As could be seen from Figure 15, College A had the highest pass rate of 21.7%, while College J had the lowest pass rate of 3.3%. With the exception of College A, College B and College C, the remaining seven colleges had a pass rate of less than 10%.

From the statistical results of the entrance examination, we could find several interesting phenomena. The level of computer basic application ability of students in College A was higher than that of students in other colleges. The new media major of College A and digital media major of College B ranked first and second in pass rate respectively, indicating that the students of these two majors had received solid training of basic computer application ability in high school. The basic computer application ability of engineering majors was lower than that of other majors. The students in College J, College I, and Materials Science and Engineering all had a pass rate of less than 5%. This result was beyond the judgment of many teachers and the specific reasons remained to be further explored. However, according to past experience, the computer application ability of engineering students was generally lower than that of students majoring

in economics, management and language. After a semester of MOOC and practice on the evaluation system of practical operation, the pass rate of all colleges was above 80%, but the highest improvement was no longer in liberal arts majors and the computer application ability of engineering students had been rapidly improved [22].

As could be seen from Figure 16, the higher improvement rates for the final examination and the entrance test were College G, College I, and College H. The reason for the high rate of improvement was that the basic computer application ability of engineering students was relatively weak at the time of admission, but the basic computer application ability of engineering students had rapidly improved after learning. It could be seen that engineering majors had certain disciplinary advantages.

5. Conclusion

Students' learning motivation and confidence are affected by the teaching evaluation greatly. It has been accepted by English teachers to change the mode of final evaluation based on single test scores and attach importance to process evaluation in the whole learning process of students. But in teaching practice, teachers often rely too much on personal formative evaluation and students are short of self-evaluation and mutual evaluation. Information in the context of the learning process is more diversified, so the teaching evaluation should pay attention to students' learning link performance. The cooperative learning group is advocated. Based on teachers' personal evaluation, students' self-evaluation, group evaluation, and peer mutual evaluation should be developed. Students' emotional factors should be given full consideration. Through diversified evaluation mechanism, affirmation and encouragement are given to the students, which helps them to recognize their shortcomings, so as to mobilize their enthusiasm of students. After a semester of The Foundation of University Information Technology MOOC study and practice in the practical operation of the evaluation system, the pass rate of each college was over 80%. And 91% of the students scored more than 60 in the final exam and 35% of the students scored more than 90. It could be seen that 91% of the students met the requirements of the course and a considerable proportion of students had a very solid grasp of knowledge.

ESP English teaching mode has made a detailed discussion on English teaching content, textbook selection, teaching methods, teaching staff, and evaluation methods and feasible countermeasures are put forward. The teaching content reflects the principles of practicality, proficiency, professionalism, and comprehensiveness. Practical courses should be increased and practical teaching links should be strengthened. According to the content of practice, practice should be connected with related teaching courses and teaching content as far as possible. The selection of teaching materials caters to the characteristics of higher vocational colleges and adheres to the principle of "giving priority to practical use and giving priority to sufficient use" based on students' language. For teaching methods, oral English, reading and translation should be attached great importance to, especially to skills which are closely related to students' ability to use English in their future jobs. The teaching and training of English language skills should be focused on. It should be emphasized that English language skills must be combined with professional knowledge. English teachers should not only know and understand professional knowledge, but also have the comprehensive teaching ability of "profession + English." English teachers should must have some business experience. For the universities, relevant training system and incentive mechanism should be established to encourage teachers to conduct further research. The teachers should be organized to practice in the school-enterprise cooperation department. Case teaching should be introduced into the classroom. And a strong and "double-qualified" teacher team forms gradually. In a word, ESP theory requires that the English teaching model should pay attention to the combination and penetration of professional English and basic English, which is employment-oriented. It emphasizes students' application ability of professional English so as to achieve the effect of applying what they have learned to practice.

Data Availability

The labeled dataset used to support the findings of this study are available from the author upon request.

Conflicts of Interest

The author declares that there are no conflicts of interest.

References

[1] Asiyah, J. Sapri, N. Novitasari et al., "Construction ethnoscience-based learning environment material in scientific knowledge," *Journal of Physics: Conference Series*, vol. 1796, no. 1, Article ID 012034 8 pages, 2021.

[2] B. Gan and C. Zhang, "Research on the design and construction of university informationized learning environment under the tpack framework," *Journal of Physics: Conference Series*, vol. 1550, no. 3, Article ID 032064 5 pages, 2020.

[3] N. M. Shamsudin and F. A. Majid, "Effectiveness of construction safety hazards identification in virtual reality learning environment," *Environment-Behaviour Proceedings Journal*, vol. 4, no. 12, p. 375, 2019.

[4] N. Balakrishnan, A. Rajendran, and P. Ajay, "Deep embedded median clustering for routing misbehaviour and attacks detection in ad-hoc networks," *Ad Hoc Networks*, vol. 126, Article ID 102757, 2021.

[5] G. Veselov, A. Tselykh, A. Sharma, and R. Huang, "Special issue on "applications of artificial intelligence in evolution of smart cities and societies," *Informatica*, vol. 45, no. 5, p. 603, 2021.

[6] T. Z. Baram, F. Donato, and G. L. Holmes, "Construction and disruption of spatial memory networks during development," *Learning & Memory*, vol. 26, no. 7, pp. 206–218, 2019.

[7] G. Ruge and L. Mackintosh, "Facilitating reflective practice: developing built environment educators' capacity for teaching and learning," *Construction Economics and Building*, vol. 20, no. 3, pp. 160–174, 2020.

[8] B. Gan, C. Zhang, and H. Meng, "Construction of experiential learning space model based on virtual reality technology,"

Hindawi
Security and Communication Networks
Volume 2024, Article ID 9815745, 1 page
https://doi.org/10.1155/2024/9815745

Retraction

Retracted: Decision Model of Wireless Communication Scheme Evaluation via Interval Number

Security and Communication Networks

Received 8 January 2024; Accepted 8 January 2024; Published 9 January 2024

This article has been retracted by Hindawi following an investigation undertaken by the publisher [1]. This investigation has uncovered evidence of one or more of the following indicators of systematic manipulation of the publication process:

(1) Discrepancies in scope

(2) Discrepancies in the description of the research reported

(3) Discrepancies between the availability of data and the research described

(4) Inappropriate citations

(5) Incoherent, meaningless and/or irrelevant content included in the article

(6) Manipulated or compromised peer review

The presence of these indicators undermines our confidence in the integrity of the article's content and we cannot, therefore, vouch for its reliability. Please note that this notice is intended solely to alert readers that the content of this article is unreliable. We have not investigated whether authors were aware of or involved in the systematic manipulation of the publication process.

Wiley and Hindawi regrets that the usual quality checks did not identify these issues before publication and have since put additional measures in place to safeguard research integrity.

We wish to credit our own Research Integrity and Research Publishing teams and anonymous and named external researchers and research integrity experts for contributing to this investigation.

The corresponding author, as the representative of all authors, has been given the opportunity to register their agreement or disagreement to this retraction. We have kept a record of any response received.

References

[1] M. Li, Y. Ouyang, W. Kang, X. Che, and R. Ye, "Decision Model of Wireless Communication Scheme Evaluation via Interval Number," *Security and Communication Networks*, vol. 2022, Article ID 5916061, 10 pages, 2022.

Hindawi
Security and Communication Networks
Volume 2022, Article ID 5916061, 10 pages
https://doi.org/10.1155/2022/5916061

Research Article

Decision Model of Wireless Communication Scheme Evaluation via Interval Number

Man Li, Yuhong Ouyang, Wenqian Kang, Xiangbei Che, and Ruixian Ye

Senior Engineer, Shenzhen Power Supply Bureau Co., Ltd., Shenzhen 518000, Guangdong, China

Correspondence should be addressed to Man Li; wanglemima10@163.com

Received 20 April 2022; Revised 20 May 2022; Accepted 30 May 2022; Published 28 June 2022

Academic Editor: Zhiping Cai

This study aims to evaluate the communication schemes of wireless communication systems to make reasonable decisions. Firstly, the wireless communication scheme is assessed based on the interval number technology, and the primary evaluation process and evaluation index system are described. Secondly, the analytic hierarchy process of interval numbers is studied. Besides, a decision model has been established for wireless communication scheme evaluation. Thirdly, the evaluation index of the wireless communication scheme is determined through the simulation analysis of the model. Finally, experiments verify the decision model for evaluating wireless communication schemes based on interval numbers. Channel encoding can be adjusted automatically and can effectively track electrical signals. The results demonstrate that under the same high signal-to-noise ratio (SNR), the error rate in the 16 quadrature amplitude modulation (QAM) mode decreases faster than that in the 2 frequency shift keying (FSK) mode, so the 16QAM mode is better than the 2FSK mode. Under a low SNR, the binary phase shift keying mode is superior to the 2FSK mode, and the 2FSK mode is superior to the 16QAM mode. The bit error rate of the communication signal in the additive white Gaussian noise channel is the lowest. These findings provide a solid foundation for a universal and scalable wireless communication system. This research has practical application value for scheme evaluation and model decision-making in the wireless communication field. Models need to be tested and evaluated based on large amounts of statistical data in future studies.

1. Introduction

The progress of information technology has promoted the rapid development of society and modern science and technology. This fast dynamic progress is inseparable from the support of communication technology and wireless communication technology. Mainly based on digital wireless communication technology, wireless communication technology plays an increasingly important role in communication, the army, daily life, and society [1]. The wireless communication system must achieve more functions and applications because of the need for service expansion and resource sharing [2]. The operating environment is increasingly complex for the wireless communication system, the requirements are continuously higher, and the system composition is even more complicated. In addition, the research of wireless communication technology and the development of communication-related products requires a shorter time, lower cost, and higher level [3]. Under this situation, engineers need more time and energy to analyze and study system problems, improve the cognitive level of the system, and evaluate the practical application of the system [4]. In the evaluation of wireless communication systems, the method used by national evaluators still has the characteristics of equipment-type tests. Evaluation tests are usually limited to the requirements of system development. In other words, system performance tests should be carried out under established and ideal test conditions [5]. This evaluation method has the deficiencies of single means, single purpose, low resource utilization rate, and poor experimental conditions. Besides, the evaluation results only stay at the test level, so it is difficult to evaluate the system's adaptability to the actual environment and system requirements. Therefore, it is essential to adopt more reasonable and effective evaluation methods based on a preliminary systematic evaluation to meet the growing

evaluation needs. Consequently, the utility originating from western economics is applied to the assessment of equipment systems and becomes an important concept of equipment system research [6].

Western economics first introduced the concept of utility to describe consumer satisfaction with commodities. The idea of the effectiveness of the equipment system comes from the concept of utility, which corresponds to performance [7]. It describes the performance values of devices and procedures and the ability to implement one or more target tasks. It is an abstract expression of the difference between supply and demand in the system. Compared with the traditional performance test evaluation method, the evaluation of system effectiveness is higher in evaluation level and more practical [8]. However, the evaluation of the effectiveness of a wireless communication system through field tests often faces a limited field test environment, which still cannot meet the requirements of the evaluation environment. Meanwhile, the field test has apparent defects such as long-time consumption, high test cost, low safety, and unreproducible test results [9]. Although the evaluation results obtained through field tests are very real, the entire evaluation process is arduous and expensive, so conducting a comprehensive evaluation test [10].

On this basis, this study expounds on the basic principles of wireless communication scheme evaluation and decision-making and conducts the corresponding modeling and simulation experiments. The efforts reported here lay a foundation for evaluating wireless communication systems and decision-making methods based on interval numbers. In Section 2, the performance index of wireless communication is analyzed. In Section 3, an index system for assessing the effectiveness of wireless communication systems is established. In section 4, the research innovation is to combine interval numbers with wireless communication to study the decision-making model of wireless communication scheme evaluation. The advantage of interval numbers is that they can sort out all the sets within the closed interval and optimize the uncertainty of the system after being introduced into the model.

2. Relevant Theories of Decision-Making of Wireless Communication Scheme Evaluation Based on Interval Numbers

2.1. Wireless Communication Technology. Wireless communication technology has many advantages and traits. In terms of information exchange, the wireless communication mode is supplemented by electromagnetic wave signals, while the traditional communication mode uses cables to complete the transmission of signals [11]. This transmission mode may have significant limitations, but the transmission mode of electromagnetic wave signals is not limited by time and place. Meanwhile, it has the characteristics of long transmission distance and flexible and reliable transmission [12]. Wireless communication is widely used in various fields of life and work and plays greatly important functions and roles [13]. However, there are still some problems and shortcomings in the practical application of wireless communication technology, impacting the use range and performance of wireless communication technology. With the rapid development of modern science and technology, wireless communication technology has made major breakthroughs and attained new features [14]. With regard to the access form of wireless communication technology, the wireless connection can ensure the efficiency, flexibility, and speed of information transmission without being affected by time and place [15]. With the help of these advantages, international information exchange and economic and cultural development are more frequent, and communication technology has entered a new stage of development. Moreover, the access method of wireless communication technology adopts wireless communication and wireless access methods, with the characteristics of high reliability and high liquidity, which can break through the limitations of time and space factors and transmit information effectively, stably, and reliably [16]. Compared with wireless communication, wireless communication devices are smaller and have more ingenious information transmission, which significantly increases the scope and field of wireless communication technology.

2.2. Concept of Scheme Evaluation. Generally, schemes can be divided into personal, business, and system. The effectiveness of a single element represents the extent to which a single goal is achieved when using a device or system [17]. Operational efficiency, or troop efficiency, denotes the extent to which operational objectives are achieved throughout military operations under the synergy of forces, equipment, and operational command. There is no uniform definition of the system scheme. The definition proposed by the United States industry is currently used a single system or a system-wide system to achieve the mission's objectives under established operating conditions [18]. The system scheme contains task planning and deployment, system operation mode, and other factors according to the circumstances of the operating conditions. The specific and designated task that is described qualitatively and quantitatively set up according to different times, spaces, and quantities. The efficiency scale can be expressed by probability, completion rate, and other physical quantities, which clarifies the basic concept of system effectiveness [19].

2.3. Basic Process of Wireless Communication Scheme Evaluation. The evaluation of a wireless communication system must be practical. Therefore, the reasonable establishment process of the effectiveness evaluation is essential, which can be divided into the following stages: analyzing the effectiveness of the evaluation system, including analyzing the structure, environment, and objectives of the evaluation system; clarifying the technical and financial constraints of the evaluation system; establishing evaluation index system of wireless communication system efficiently; qualitative analysis of each index of the impact index system; and evaluating the effectiveness and efficiency of the evaluation system by the index system. An appropriate valuation

algorithm should be determined to quantitatively calculate the system efficiency values, check the accuracy of the results, and make a comprehensive evaluation system [20]. Figure 1 reveals the specific process.

2.4. Evaluation Index System. Wireless communication scheme analysis is the basis of establishing an efficiency evaluation index system. It is necessary to use the system analysis method to analyze the functions and relationships of each system structure module, the goals and standards to be achieved by the system, and the environment that is interdependent with the system. The effectiveness evaluation index system is established based on the comprehensive collection of the relevant information of the system [21]. Generally, there are many factors that affect the evaluation results of the evaluation system, among which no one can be reflected in the effectiveness evaluation. In addition, some factors are extremely random while other factors are not easy for quantitative analysis, so evaluators must optimize the measurement metrics frequently under the foundation of qualitative analysis [22]. Therefore, the effectiveness of the evaluation index system should consider the following points: the institutional principle, the concision principle, the objectivity principle, the timeliness principle, the measurability principle, the integrity principle, the independence principle, and the consistency principle [23].

It is worth noting that there are inevitable contradictions in the establishment of an effectiveness evaluation index system based on the above principles. At this stage, evaluators should take complete account of the effectiveness of the evaluation index system and make appropriate changes to the index system in the evaluation process [24]. For example, the integrity principles and the concision principle of the evaluation index system are contradictory. Therefore, some indexes with little impact should be eliminated to minimize the number of evaluation indexes and make evaluation easier. The system effectiveness index reflects the essence of the system and the most basic understanding of the system function [25]. Combined with the analysis of the effectiveness of the system, the effectiveness indexes that can reflect the same function of the system are summarized and synthesized. In contrast, the effectiveness evaluation indexes that can reflect the various objectives and standards of the system are extracted. The selected effectiveness evaluation indexes and each index weight are the specific content and focus of system user requirements. Combined with an efficiency evaluation algorithm, system effectiveness evaluation reflects the degree to which the system's working ability meets users' needs [26].

2.5. Establishment of Wireless Communication Index. The efficiency analysis is the basis for establishing an effectiveness evaluation index system. It is necessary to use system analysis methods to analyze the functions and relationships of each system structural module, the goals and standards that the system must achieve, and the environment interdependent with the system. The effectiveness evaluation index system is established based on the comprehensive collection of the relevant information of the system [27]. In terms of systematic evaluation of effectiveness, generally speaking, there are still many factors that affect the evaluation results, which cannot be reflected in the effectiveness evaluation. Therefore, the evaluator must always choose excellent measurement metrics based on qualitative analysis [28]. The goal of the wireless communication system task is to complete the communication between the sender and the receiver. Correspondingly, the communication capability of the wireless communication system is considered to be the objective of evaluating the effectiveness of the system. Seven indicator elements of wireless communication are established: quality, service, survivability, anti-interference ability, coverage, speed, and delay [29].

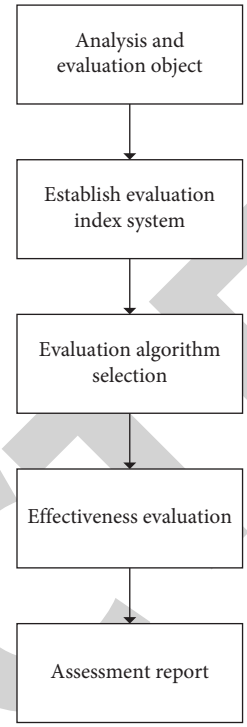


Figure 1: Basic process of wireless communication scheme evaluation.

3. Evaluation Algorithm of Wireless Communication Scheme

3.1. Interval Number Analytic Hierarchy Process. As the most commonly used efficiency scheme evaluation method, the analytic hierarchy process (AHP) of interval numbers, combines the interval number theory with the AHP theory. The specific implementation is as follows. In the index classification of wireless communication systems, the "weight" value of different levels of decision-making is calculated according to the relevant theoretical knowledge of interval numbers. Then, the effectiveness of the system is evaluated using AHP [30].

Firstly, the effectiveness of the comprehensive AHP evaluation system is analyzed, and the objectives that must be prioritized are defined in a unique way. The overall goal of

AHP effectiveness evaluation is to meet the needs of users. Secondly, the criteria as part of the general aim of effectiveness evaluation are considered to be the low level of the goal. There are many standards in the general evaluation system. Thus, it is essential to distinguish the foremost standard and substandard. If necessary, the standards that have little impact on the evaluation system can be deleted to reduce the complexity of the evaluation according to the method of establishing the evaluation index system. Third, it is essential to analyze these standards' factors and their relationship. The upper and lower structures need to be built for the elements with adhesion to reflect the domination of the upper elements over the lower parts. In addition, a group relationship is set for the factors that have similar attributes and impact the upper piece, in which the upper element is subordinate. In this way, the efficiency evaluation index system is established [31]. The steps of the national health plan are as follows.

Step 1. Evaluate the system scheme based on in-depth analysis, the principal analysis level of the evaluation object and process is used to determine the target to be achieved by the evaluation object. Then, the influencing factors are decomposed from one layer to another to ensure that the elements of the same layer and the same group do not intersect. The elements of the upper layer and the lower layer form a tree relationship. The basic element is the evaluation index.

Step 2. Calculate the weight of lower elements relative to higher elements in the evaluation index system. Experts or evaluators subjectively judge the importance of the lower part relative to the higher part. Finally, the judgment matrix A is obtained:

$$\mathrm{A} = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix}, \tag{1}$$

where a_{mn} represents the evaluation value given by the mth evaluation expert for the nth evaluation index. Then, each row element of matrix A is standardized to obtain the weight value θ, which can be expressed as follows:

$$\theta = [\, \theta_1 \;\; \theta_2 \;\; \ldots \;\; \theta_n \,]^T, \tag{2}$$

where

$$\theta_n > 0, \tag{3}$$

$$\theta_1 + \theta_2 \ldots + \theta_n = 1. \tag{4}$$

According to the effectiveness evaluation, the importance of each element needs to be compared, and a_{ij} is assigned:

$$a_{ij} = \frac{\theta_j}{\theta_i}. \tag{5}$$

Step 3. Calculate the scheme evaluation matrix B_{ji}, as shown in the following equation:

$$\mathrm{B}_{ji} = \begin{bmatrix} b_{11} & b_{12} & \cdots & b_{1i} \\ b_{21} & b_{22} & \cdots & b_{2i} \\ \cdots & \cdots & \cdots & \cdots \\ b_{j1} & b_{j2} & \cdots & b_{ji} \end{bmatrix}. \tag{6}$$

In equation (6), b_{ji} denotes the evaluation value given by the ith evaluation expert to the jth evaluation index.

Step 4. Determine the evaluation of the grey class. Here, the class function describes an uncertain interval range, where whitening means improving certainty. The Whitening weight function of the grey class means quantifying the degree of grey class. There are three common whitening weight functions, as shown in the following equations:

$$g\left(b_{ji}\right) = \begin{cases} 0, \\ \dfrac{b_{ji} - b_1}{b_2 - b_1}, \\ 1, \end{cases} \tag{7}$$

$$g\left(b_{ji}\right) = \begin{cases} \dfrac{b_{ji} - b_1}{b_2 - b_1}, \\ \dfrac{b_3 - b_{ji}}{b_3 - b_2}, \\ 0, \end{cases} \tag{8}$$

$$g\left(b_{ji}\right) = \begin{cases} 0, \\ \dfrac{b_2 - b_{ji}}{b_2 - b_1}, \\ 1. \end{cases} \tag{9}$$

Step 5. Calculate the grey evaluation coefficient. The grey evaluation coefficient c_k^j is obtained according to the evaluation matrix B_{ji} and the whitening weight function $g_k(b_{ji})$.

$$c_k^j = \sum_{i=1}^{n} g_k\left(b_{ji}\right). \tag{10}$$

In equation (10), c_k^j refers to the kth grey evaluation coefficient of index element j.

Correspondingly, the total grey evaluation coefficient c^j can be written as the following equation:

$$c^j = \sum_{i=1}^{n} c_k^j. \tag{11}$$

The input layer is denoted as a_i, the hidden layer is denoted as b_j, and the output layer is denoted as c_k. Moreover, the connection weight between the input layer and the hidden layer is denoted as f_{ij}, and the connection

weight between the hidden layer and the output layer is denoted as g_{jk}. Furthermore, the thresholds of the output and the hidden layer are denoted as d_l and e_m, respectively, and the predicted output value of the output layer is denoted as h_n. The neuron is regarded as net, then

$$net_j = \sum_{i=0}^{n} p_{ij} a_i. \tag{12}$$

The output from the hidden layer to the output layer can be expressed as the following equation:

$$c_k = f(net_k) = f\left(\sum_{i=1}^{n} g_{ik} b_j - d_l\right). \tag{13}$$

For the convenience of calculation, let

$$net_k = \sum_{j=0}^{n} g_{ij} b_j. \tag{14}$$

The signal error backpropagation process is as follows. The error function

$$E = \frac{1}{2} \sum_{k=1}^{n} e_k^2. \tag{15}$$

The error function of the hidden layer

$$E = \frac{1}{2} \sum_{k=1}^{n} \left[h_n - f\left(\sum_{j=0}^{n} g_{ij} b_j\right)\right]^2. \tag{16}$$

The error function of the input layer

$$E = \frac{1}{2} \sum_{k=1}^{n} \left[h_n - f\left(\sum_{j=0}^{n} g_{ij} p \sum_{i=0}^{n} p_{ij} a_i\right)\right]^2. \tag{17}$$

Among them, the error function is the function of the connection weight f_{ij}. The connection weight g_{jk} between the hidden and output layers, and reducing the error function value e can be realized by changing the connection weight. Next, the error signal δ_{jk} is defined, and then the corresponding weights and thresholds are adjusted to make them present the same gradient changes.

$$\delta_{jk} = \sum_{k=1}^{k} (h_k - c_k) c_k (1 - c_k), \tag{18}$$

$$\delta_{jk} = \delta_{jk} g_{jk} b_j (1 - b_j). \tag{19}$$

The weight of the hidden layer is adjusted according to the following equation:

$$\Delta p_{ij} = \eta \delta_{ij} a_i. \tag{20}$$

The weight of the output layer is adjusted according to the following equation:

$$\Delta g_{jk} = \eta \delta_{jk} b_i. \tag{21}$$

The threshold is adjusted according to the following equations:

$$\Delta d_l = -\eta \delta_{ij}, \tag{22}$$

$$\Delta e_m = -\eta \delta_{jk}. \tag{23}$$

Step 6. Calculate the grey evaluation weight matrix D and the weight vector e.

$$e_k^j = \frac{c_k^j}{c^j}, \tag{24}$$

$$D = \left[e^1 \;\; e^2 \;\; \ldots \;\; e^n \right]^T. \tag{25}$$

Step 7. Calculate the comprehensive scheme evaluation vector F according to the full matrix.

$$F = G^t D. \tag{26}$$

The total efficiency can be expressed as

$$E = F \; D. \tag{27}$$

Thus, the total efficiency value is obtained.

3.2. Construction of the Decision Model of Wireless Communication Scheme Evaluation. The main task of the overall modeling of the effectiveness evaluation scheme of wireless communication systems based on interval numbers is to model the wireless communication system. The basic structure modules of the system are similar to the general model of digital communication systems, as shown in Figure 2.

Accordingly, the overall decision model of wireless communication scheme evaluation is built, as presented in Figure 3.

The model is divided into four parts: signal input, simulation parameter configuration, wireless communication system simulation, and performance evaluation. The signal input part provides digital signals, voice input signals, and other external signals. In simulation parameter configuration, the evaluator must provide various types of parameters, including system simulation method, source and method of parameter encoding and decoding, parameters and methods of channel encoding and decoding, parameter modulation and demodulation mode, spread spectrum parameters, and simulation module controlling communication environment parameters of the wireless communication system. The wireless communication system simulation part consists of system simulation structure modules, which can be added or deleted according to the actual structure of the system to be evaluated. The performance evaluation includes the input signal, output signal, and relevant parameters of simulation parameter configuration of the wireless communication system. Meanwhile, the performance evaluation part can modify the stimulation parameters according to the evaluation results, and the simulation is repeated until getting satisfactory results.

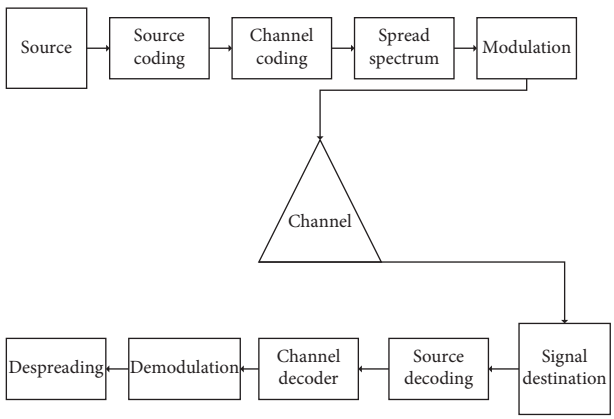


Figure 2: Wireless communication evaluation model.

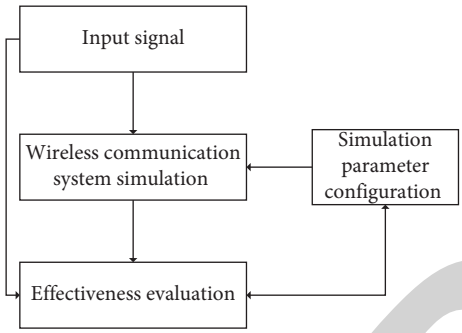


Figure 3: Decision model of wireless communication scheme evaluation.

3.3. Decision Simulation Process of Wireless Communication Scheme Evaluation. The wireless communication system is simulated according to the actual needs based on analyzing its characteristics and objectives. Meanwhile, the corresponding mathematical expression is put forward. This mathematical expression, combined with the relevant principles of the system, is also known as the mathematical model of the system. The factors that have little impact on the system in the process of establishing the system's simulation model are often ignored to improve the effectiveness of the simulation. For example, in the process of signal transmission, the error of relative delay and signal bandwidth is very small, which will significantly change when the signal strength is affected by the time-varying channel gain. Therefore, the signal bandwidth is approximately replaced by the relative delay. Next, the simulation is carried out. It is essential to select the appropriate simulation algorithm, software, and hardware platform combined with the system simulation model programming. The general sub-functions or modules of the system simulation model can be encapsulated and saved to reuse programming and simplify the programming process. The simulation program requiring observation and analysis of the change of system response usually needs to run many times, to modify the analog input signal data. Then, the simulation analysis is as follows. After the simulation operation stage, the user obtains sufficient simulation data information to be analyzed and processed for the subsequent system evaluation and result display. The above three aspects often need a running cycle to achieve satisfactory optimization and improvement results of the wireless communication system and provide a performance evaluation module. Finally, the information is transmitted to the actual system as a reference for optimization and reconstruction.

4. Simulation Analysis of the Decision-Making of Wireless Communication Scheme Evaluation

4.1. Simulation Analysis of Channel Coding, Decoding, and Common Digital Modulation. The voice signal of 25 seconds is selected according to the simulation process of channel coding. The result is shown in Figure 4, in which the channel coding data can be adjusted automatically and effectively track the electrical signal. It can be seen that when the signal data are 0–15 seconds, the tracking voltage of the circuit is about 0 V, and the fluctuation range is extensive. When the signal data are 15–25 seconds, the tracking voltage of the system circuit basically tends to be stable. After that, the above speech signal is intercepted for another simulation experiment, which produces the same result.

Simulink is used to debug 16 quadrature amplitude modulation (QAM), 2 frequency shift keying (FSK), and binary phase shift keying (BPSK). Figure 5 shows the experimental results. The bit error rate (BER) in the 16QAM mode and 2FSK mode is significantly lower than that in the BPSK mode. Under the same high signal-to-noise ratio(SNR) condition, the BER in the 16QAM mode decreases faster than that in the 2FSK mode, indicating that the modulation effect of the 16QAM mode is better than that of the 2FSK mode. Under the condition of low SNR, the BPSK mode is better than the 2FSK mode, while the 2FSK mode is better than the 16QAM mode.

4.2. Wireless Communication Channel Transmission. The propagation characteristics of radio waves in any wireless communication system depend on the radio wave propagation environment, namely the wireless communication channel. These environments include the ground state, building coverage, weather conditions, and the use of frequency bands, which limit the communication ability of both sides. Therefore, research on wireless communication channels is necessary and vital, providing key theoretical support for the simulation and evaluation of wireless communication systems. The research on the fading effect of different scales is critical in evaluating wireless communication schemes, as shown in Figure 6. From Figure 6, the large-scale disk refers to the slow change of signal level with distance in the environment of transmitting electromagnetic waves between transceivers. This attenuation signal refers to the attenuation of the electromagnetic wave transmission signal in the disk. Under the influence of scattering, refraction, and reflection of various substances in the channel, the signals arrive at the receiver along different paths and overlaps, resulting in large fluctuations in the received signal

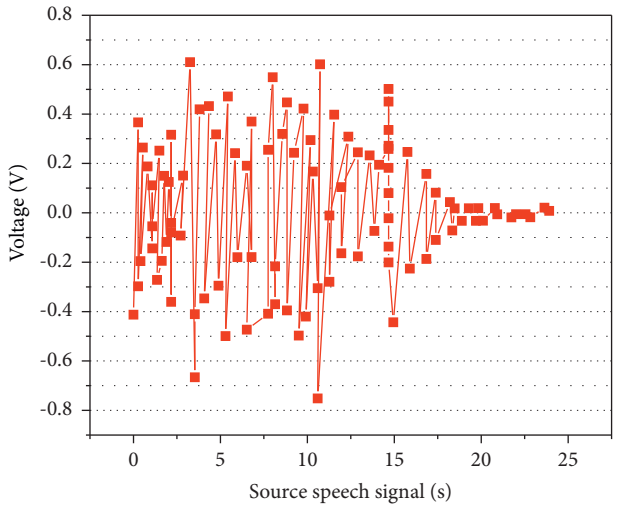


Figure 4: Source trace.

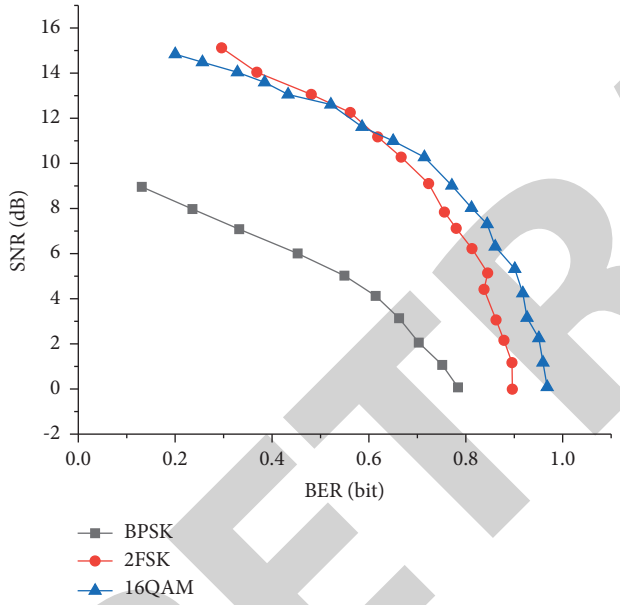


Figure 5: BER curves under three modulation modes.

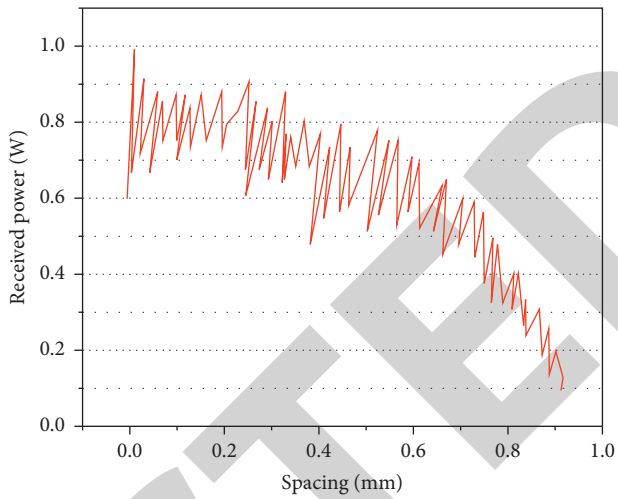


Figure 6: Fading effect of different scales.

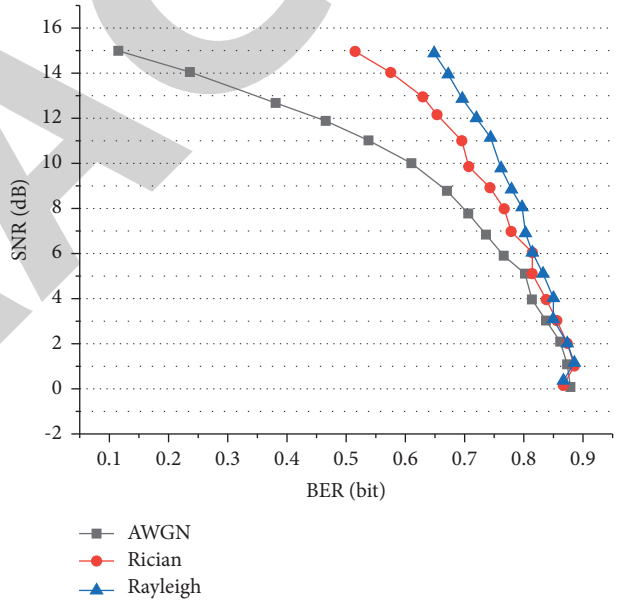


Figure 7: BER curves under three types of channels.

level. The average variation of the reception level in the short-term range is always tiny, which is also called the superposition of dozens of short-term fading levels. The main influencing factors are multichannel propagation and spectrum spread caused by the relative motion between transmitter and receiver caused by time delay spread.

4.3. Simulation Analysis of Wireless Communication Channel under Line-of-Sight Transmission. The 2FSK signal is simulated and analyzed under the corresponding conditions of the Ricean channel, additive white Gaussian noise (AWGN) channel, and Rayleigh channel. The experimental results are presented in Figure 7. The channel simulation results are realized using the simulink tool in MATLAB. In Figure 7, with the decrease of SNE, the BER of signal in the Rayleigh channel is the highest, followed by the Ricean channel and finally the AWGN channel. In other words, the BER of the signal in the AWGN channel is the lowest. This result indicates that antichannel reduction technology should be added to the wireless communication system.

4.4. Determination of Each Effectiveness Evaluation Index. The normal communication of the two receivers in the simulated electromagnetic environment under the interference of normal interference and electronic jamming is the primary commitment task. Therefore, the communication quality and anti-interference ability can be restored as evaluation indexes. The coverage ability determines a certain range of the latest news received from each other, followed by recovery. Besides, the communication rate and the delay

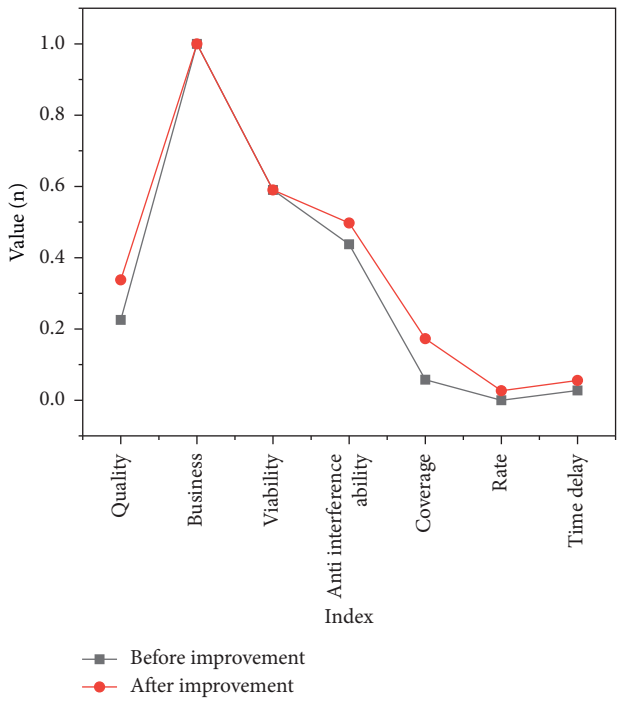


Figure 8: Comparison of effectiveness values of the system before and after optimization.

capability are relatively important indexes of communication capability and transceiver delay. In addition, communication congestion, living ability, and service also affect the communication performance of the wireless communication system. Finally, the corresponding matrix is shown in the following equation:

$$H = \begin{bmatrix} 1 & 2/5 & 2/5 & 1 & 2/3 & 1/2 & 1/2 \\ 5/2 & 1 & 1 & 5/2 & 5/3 & 5/4 & 5/4 \\ 5/2 & 1 & 1 & 5/2 & 5/3 & 5/4 & 5/4 \\ 1 & 2/5 & 2/5 & 1 & 2/3 & 1/2 & 1/2 \\ 3/2 & 3/5 & 3/5 & 3/2 & 1 & 3/4 & 3/4 \\ 2 & 4/5 & 4/5 & 2 & 4/3 & 1 & 1 \\ 2 & 4/5 & 4/5 & 2 & 4/3 & 1 & 1 \end{bmatrix}. \quad (28)$$

The division of this importance is not constant. On the contrary, there will be a variety of divisions. Different wireless communication systems, test environments, and index scores of different levels will affect the importance division and change the rating weights. Therefore, different importance division methods can be selected according to the actual test conditions and requirements. Because the division of importance depends on the experience and understanding of experts, the subjective judgment of the importance of each index of wireless communication system in a specific application environment will inevitably affect the objectivity of the evaluation. Therefore, when dividing the importance of each indicator, it is necessary to fully consider the opinions of many experts to improve the credibility of the system evaluation results. The feature vector of the normative judgment matrix is carried out for each column of elements, and then the mean value of the sum of elements of each row is taken as the combined weight Q:

$$Q = (0.2045, 0.0822, 0.0822, 0.2055, 0.1370, 0.1027, 0.1027)^T. \quad (29)$$

4.5. Effectiveness Evaluation. Figure 8 illustrates the comparison results of system effectiveness values before and after the system optimization. According to Figure 8, the performance of the optimized system has been improved in seven evaluation indexes: communication quality, service, survivability, anti-interference ability, coverage, speed, and delay. In addition, the communication quality and coverage have been improved, and the communication rate and communication delay have changed from good to qualified, suggesting excellent performance. However, the evaluation value of unqualified quality and standard quality decreases, while the evaluation value of extraordinary standard increases. At the same time, the anti-interference ability changes from good to excellent. Therefore, the system's overall efficiency has been improved, which also shows that the efficiency evaluation is effective and suitable for system improvement. The exact effectiveness improvement results can be obtained using other evaluation algorithms.

5. Conclusion

Under the background of the development of the efficiency evaluation component of wireless communication systems, the general method of wireless communication system efficiency evaluation is studied by combining computer simulation technology with system efficiency evaluation. Firstly, this study expounds on some evaluation indexes of the scheme evaluation model of wireless communication systems after clarifying the theoretical basis and process of effectiveness evaluation. Then, seven evaluation indexes are extracted and characterized to construct the efficiency evaluation index system of the wireless communication system. In addition, the wireless communication system is established, and the weight of each index is analyzed and determined in detail. Finally, the relevant conclusions are drawn to express the relationship between the effectiveness of wireless communication systems and the needs of system users. Experiments verify the effectiveness of wireless communication systems' interval number-based scheme evaluation model, which provides a favorable baseline for the final implementation of general components and the evolutionary evaluation of wireless communication system efficiency. The system effectiveness analysis results before and after optimization indicate that the system quality effectiveness is improved by 0.18, the system coverage area effectiveness is improved by 0.15, and the overall effectiveness of the model is verified. The follow-up research will refine the analysis and study of each module of the wireless system structure. It is expected to establish a communication system simulation environment based on massive statistical

data to ensure that the system simulation is closer to the actual system and the evaluation of the simulation system is more convincing.

Data Availability

The labeled dataset used to support the findings of this study is available from the corresponding author upon request.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This study was supported by the first batch of the Science and Technology Projects of System Operation Department of Shenzhen Power Supply Bureau Co., Ltd in 2020.

References

[1] L. Zhang, M. Z. Chen, W. Tang et al., "A wireless communication scheme based on space- and frequency-division multiplexing using digital metasurfaces," *Nature electronics*, vol. 4, no. 3, pp. 218–227, 2021.

[2] M. Wang, X. Wang, L. T. Yang, X. Deng, and L. Yi, "Multi-sensor fusion based intelligent sensor relocation for health and safety monitoring in BSNs," *Information Fusion*, vol. 54, pp. 61–71, 2020.

[3] D. Zhang, X. Han, X. Han, and C. Deng, "Review on the research and practice of deep learning and reinforcement learning in smart grids," *CSEE Journal of Power and Energy Systems*, vol. 4, no. 3, pp. 362–370, 2018.

[4] R. Umar, F. Yang, H. Xu, and S. Mughal, "Multi-level construction of polar--," *IET Communications*, vol. 12, no. 10, pp. 1253–1262, 2018.

[5] K. Takabayashi, H. Tanaka, C. Sugimoto, K. Sakakibara, and R. Kohno, "Performance evaluation of a quality of service control scheme in multi-hop WBAN based on IEEE 802.15.6," *Sensors*, vol. 18, no. 11, p. 3969, 2018.

[6] Y. Xu and X. Wang, "Three-way decision based on improved aggregation method of interval loss function," *Information Sciences*, vol. 508, pp. 214–233, 2020.

[7] B. I. Bakare and J. D. Enoch, "A review of simulation techniques for some wireless communication system [J]," *International Journal of Electronics, Communications and Computer Engineering*, vol. 10, no. 2, pp. 60–70, 2019.

[8] A. Sarkar, J. Dey, and A. Bhowmik, "Multilayer neural network synchronized secured session key based encryption in wireless communication," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 14, no. 1, p. 169, 2019.

[9] M. Jain, N. Sharma, A. Gupta, D. Rawal, and P. Garg, "Performance analysis of NOMA assisted underwater visible light communication system," *IEEE Wireless Communications Letters*, vol. 9, no. 8, pp. 1291–1294, 2020.

[10] S. Al-Rubaye, A. Al-Dulaimi, J. Cosmas, and A. Anpalagan, "Call admission control for non-standalone 5G ultra-dense networks," *IEEE Communications Letters*, vol. 22, no. 5, pp. 1058–1061, 2018.

[11] V. Suma, "Power efficient time-division random-access model based in wireless communication networks," *IRO Journal on Sustainable Wireless Systems*, vol. 2, no. 4, pp. 155–159, 2021.

[12] J.-Y. Choi, C. Mun, and J.-G. Yook, "Symbol-level selective channel estimation in packet-based OFDM systems," *Sensors*, vol. 20, no. 5, p. 1274, 2020.

[13] Q. Luo, C. Li, T. H. Luan, W. Shi, and W. Wu, "Self-Learning based computation offloading for internet of vehicles: model and algorithm," *IEEE Transactions on Wireless Communications*, vol. 20, no. 9, pp. 5913–5925, 2021.

[14] H. Sun, E. Viterbo, and R. Liu, "Efficient blind detection scheme based on simplified decoding of polar codes," *IEEE Wireless Communications Letters*, vol. 10, no. 4, pp. 864–868, 2021.

[15] D. Lee, Y. G. Sun, S. H. Kim et al., "DQN-based adaptive modulation scheme over wireless communication channels," *IEEE Communications Letters*, vol. 24, no. 6, pp. 1289–1293, 2020.

[16] M. Dibaei and A. Ghaffari, "Full-duplex medium access control protocols in wireless networks: a survey," *Wireless Networks*, vol. 26, no. 4, pp. 2825–2843, 2020.

[17] M. S. Rusli, N. D. Kamarudin, A. A.-H. A. Rahman, and M. N. Marsono, "Evaluation of scheme selection and parameter effects in the reconfigurable transmitting power in wireless network-on-chip," *Science & Technology Research institute for Defence (Stride)*, vol. 181, p. 170, 2018.

[18] W. Li, R. Li, K. Wu, R. Cheng, L. Su, and W. Cui, "Design and implementation of an SM2-based security authentication scheme with the key agreement for smart grid communications," *IEEE Access*, vol. 6, pp. 71194–71207, 2018.

[19] H. Lee, I. Jung, J. Heo, and D. Hong, "Exploiting intentional time-domain offset in downlink multicarrier NOMA systems," *IEEE Wireless Communications Letters*, vol. 10, no. 7, pp. 1577–1580, 2021.

[20] L. Zhu, D. J. Hill, and C. Lu, "Hierarchical deep learning machine for power system online transient stability prediction," *IEEE Transactions on Power Systems*, vol. 35, no. 3, pp. 2399–2411, 2020.

[21] G. Soni and K. Selvaradjou, "The finest superframe interval and GTS provision scheme (FSGPS) for time-sensitive IEEE 802.15. 4 applications [J]," *SN Computer Science*, vol. 2, no. 5, pp. 1–17, 2021.

[22] S. Sreethar, N. Nandhagopal, S. Anbu Karuppusamy, and M. Dharmalingam, "SARC: s," *Wireless Networks*, vol. 27, no. 6, pp. 3915–3926, 2021.

[23] X. Liu, J. Yu, F. Li, W. Lv, Y. Wang, and X. Cheng, "Data aggregation in wireless sensor networks: from the ps," *IEEE Internet of Things Journal*, vol. 7, no. 7, pp. 6495–6513, 2020.

[24] A. Chaisang and S. Promwong, "Experimental evaluation scheme of ultra-wideband human body transmission model for wireless body area network," *Sensors and Materials*, vol. 30, no. 10, p. 2211, 2018.

[25] S. Fu, X.-L. Qu, Y.-Z. Xiao, H.-J. Zhou, and G.-B. Fan, "Risky multi-attribute decision-making method based on the interval number of normal distribution," *Symmetry*, vol. 12, no. 2, p. 264, 2020.

[26] S. A. Busari, S. Mumtaz, S. Al-Rubaye, and J. Rodriguez, "5G m-wave mobile broadband: performance and challenges," *IEEE Communications Magazine*, vol. 56, no. 6, pp. 137–143, 2018.

[27] S. Verma, M. Ghazel, and M. Berbineau, "Model-based dependability evaluation of a wireless communication system in a virtually coupled train set," *IFAC-PapersOnLine*, vol. 54, no. 2, pp. 179–186, 2021.

[28] J. Zhang, H. Du, P. Zhang, J. Cheng, and L. Yang, "Performance analysis of 5G mobile relay systems for high-speed

Hindawi
Security and Communication Networks
Volume 2024, Article ID 9891407, 1 page
https://doi.org/10.1155/2024/9891407

Retraction

Retracted: Secure Two-Party Computation Based on Fast Cut-and-Choose Bilateral Oblivious Transfer

Security and Communication Networks

Received 8 January 2024; Accepted 8 January 2024; Published 9 January 2024

This article has been retracted by Hindawi, as publisher, following an investigation undertaken by the publisher [1]. This investigation has uncovered evidence of systematic manipulation of the publication and peer-review process. We cannot, therefore, vouch for the reliability or integrity of this article.

Please note that this notice is intended solely to alert readers that the peer-review process of this article has been compromised.

Wiley and Hindawi regret that the usual quality checks did not identify these issues before publication and have since put additional measures in place to safeguard research integrity.

We wish to credit our Research Integrity and Research Publishing teams and anonymous and named external researchers and research integrity experts for contributing to this investigation.

The corresponding author, as the representative of all authors, has been given the opportunity to register their agreement or disagreement to this retraction. We have kept a record of any response received.

References

[1] Y. Wang, K. Xiong, H. Tian, J. Zhang, and X. Yan, "Secure Two-Party Computation Based on Fast Cut-and-Choose Bilateral Oblivious Transfer," *Security and Communication Networks*, vol. 2022, Article ID 3880413, 10 pages, 2022.

Hindawi
Security and Communication Networks
Volume 2022, Article ID 3880413, 10 pages
https://doi.org/10.1155/2022/3880413

Research Article

Secure Two-Party Computation Based on Fast Cut-and-Choose Bilateral Oblivious Transfer

Yongjun Wang, Kun Xiong, He Tian, Jing Zhang, and Xixi Yan

School of Software, Henan Polytechnic University, Jiaozuo 454000, China

Correspondence should be addressed to Jing Zhang; zj_jsj@hpu.edu.cn

Received 22 February 2022; Revised 2 June 2022; Accepted 8 June 2022; Published 27 June 2022

Academic Editor: Zhiping Cai

In secure two-party computation, each party has its input and wants to jointly compute a function from which it obtains the output corresponding to its respective inputs. For achieving security against a malicious adversary, an effective approach is using cut-and-choose, which requires the circuit constructor P_1 to construct S copies of the circuit C (C is used to compute the function F). The circuit evaluator P_2 selects $S/2$ circuits to open for the check. If these $S/2$ circuits are correctly constructed, P_2 assumes that the remaining $S/2$ circuits are also correctly constructed and uses the remaining circuits to compute. However, this method introduces significant computational complexity and interactive rounds, mainly due to more circuits that must be used for security purposes and the need for multiple interactions to transmit the keys. In this paper, regarding the issue above, we present a novel secure two-party computation protocol, and it can achieve security against the malicious adversary. Concretely, we still use the idea of cut-and-choose but improve the cut-and-choose oblivious transfer (CCOT) of the usual secure two-party computation protocol into cut-and-choose bilateral oblivious transfer (CCBOT) and propose a variant of it that we call batch single-choice CCBOT, which makes our protocol only needs two rounds of interaction to complete the transmission of all keys and $28Sl$ of exponentiations. In addition, we use a check mechanism to prevent the case that p_1 cheats, but P_2 is powerless. Our proposed protocol with an error probability of 2^{-s} of P_1 significantly optimizes the communication rounds and computation overheads, solves the selective failure attack, and ensures the consistency of the input.

1. Introduction

1.1. Background. Secure two-party computation means that two mutually untrusted participants, each holding their input, collaborate to compute a function through a two-party computation protocol that satisfies multiple security properties and obtain the corresponding function output. These security properties mainly include privacy, correctness, input independence, guaranteed output delivery, and fairness [1]. Since professor Yao proposed secure two-party computation [2], it has become the subject of extensive research, with a focus on improving security and efficiency.

Yao's protocol based on oblivious transfer (OT) [3] and garbled circuit (GC) [2] is a well-known protocol of secure two-party computation. However, it only achieves security against the semihonest adversary. Because only one circuit is constructed, P_1 can easily cheat by constructing a wrong circuit. For improving the correctness of circuit computation and the security of the protocol, it is best to construct multiple circuits. Part of the circuits are used to check whether they are constructed correctly, and the rest circuits are used to compute the function. This method of dividing circuits to check and then for evaluation is called cut-and-choose [4]. It can solve the problem that Yao's protocol cannot achieve security against the malicious adversary. Its main idea is that P_1 constructs s identical circuits (only one circuit in Yao's protocol). Then P_2 selects some of them (usually half of the total) to check whether these selected circuits (called check circuits) are correct. If the check passes, P_2 can consider that the rest circuits (called computation circuits or evaluation circuits) are all correct. Finally, P_2 uses the evaluation circuits to compute and uses most of the same outputs as the final function output.

Although the protocols for cut-and-choose can combine the check of circuits and the oblivious transfer for transmitting keys to solve the problem of selective failure attacks [5], these protocols use CCOT [6–8] to transmit garbled keys. One significant feature of CCOT is that it can only transmit keys associated with P_2, s input wire. This feature to only transmit keys associated with one party will cause the protocol to generate many additional interactions for separately transmitting the relevant keys on P_1's input wire in check circuits and evaluation circuits, which seriously increases the number of interactions and round complexity. The CCOT protocol used in the famous Lindell and Pinkas protocol [9] requires 6 rounds of communication and cannot transmit all required keys. Additionally, it also requires additional interactions for zero-knowledge proofs, and there are 12 rounds of communication of the whole protocol. In addition to transmitting keys, additional interaction is needed to send the set $\mathcal{J}$ and verify its consistency of it in two interactions. The protocol [10] of Huang et al. uses a kind of multistage CCOT that still needs to send a cut-and-choose challenge and then uses additional interactions to send garbled input values. Similarly, more [11, 12] have the same problem. In addition, in most of Yao's garbled circuit protocols based on CCOT, the result takes most of the same values in all evaluation circuits. If there are a few evaluation circuits with different output values, then P_1 has cheated. However, P_2 will take most of the same value as the result according to the requirements of the protocol, even if it knows that P_1 is cheating. This method is likely to leak P_2's private input. P_1 can construct the wrong garbled circuits to cheat, but P_2 is powerless in this case.

With the intensive study of CCOT, CCBOT [13] has emerged. In CCBOT, the receiver R selects the received value according to its input, and the sender S can also actively choose other values to send to R. Compared with CCOT, CCBOT only needs one interaction to send all required keys. Almost all the secure two-party computation protocols using cut-and-choose technology complete the transmission of keys through CCOT. Currently, there has been a great deal of interest in CCBOT research, but there is still a lack of a complete and efficient secure two-party computation protocol that uses CCBOT to complete keys transfer. CCBOT makes the protocols for cut-and-choose have a new improvement. We believe that designing a secure and efficient two-party computing protocol based on CCBOT is research-intensive and challenging. Security here consists mainly of solving the input consistency problem and selective failure attack and achieving security against the malicious adversary. Efficiency is improved by using CCBOT to reduce the rounds of interaction and the complexity of communication between two parties. In addition, we are also committed to solving the problem that P_1 cheats, but P_2 is powerless.

In our paper, P_1 needs to construct many copies of the circuit, so we first introduce the cut-and-choose (introduce a new parameter s) into the CCBOT protocol of reference [14]. Then, for making P_2 input the same choice bit on each input wire, we improve CCBOT to the single-choice CCBOT. Since each input wire in each circuit must perform a single-choice CCBOT, it is necessary to perform the transfer key phase in batches. After the above improvements, we propose a batch single-choice CCBOT protocol, and see Section 4 for more details. Next, for the input consistency problem of P_1, we use a Diffie–Hellman pseudorandom synthesizer [15] to generate the keys $g^{a_i^0 \cdot r_j}$ and $g^{a_i^1 \cdot r_j}$ of its own input bits. This key structure makes it easy for P_1 to use the DDH assumption to prove the consistency of its inputs across all circuits. In addition, in our protocol, the inputs of both parties are done through only one interaction, which prevents the problem of inconsistent inputs between different interactions. And then, a selective failure attack is caused by the separation of circuit division from the oblivious transfer. Based on the features of the CCBOT protocol, we intertwine transmission keys with circuit checks. This method does not require the use of larger inputs and more circuits for the security of the protocol. Finally, for the problem that P_2 cannot abort the protocol when P_1 constructs the wrong circuits to cheat we have added an additional check mechanism. When the outputs of all evaluation circuits are inconsistent, P_2 will store a "proof" and then input this "proof" into the secure check protocol to obtain the private input of P_1 and compute $f(x, y)$ locally. The mechanism is detailed in reference [16].

1.2. Our Contributions. We first improve the CCBOT protocol of reference [14] and formalize the improved protocol. Based on this, we present a novel secure two-party protocol. It can achieve security against the malicious adversary. Our contribution consists mainly of the following:

(1) We improve the original CCBOT protocol to a variant called batch single-choice CCBOT. It can complete the oblivious transfer tasks of each gate in all circuits in parallel and requires two rounds of communication and $15s\ell$ exponents. Since only two rounds are required to complete all key transmissions, no additional interaction is required to send the keys associated with their own inputs in check circuits and evaluation circuits.

(2) We apply our batch single-choice CCBOT on Yao's protocol and propose a new secure two-party computation protocol that can solve the problem of input consistency and selective failure attack. It achieves security against the malicious adversary. Moreover, P_1's error probability is the optimal 2^{-s} in our protocol.

(3) We use a check mechanism of work [16] to prevent the case that P_2 finds out that P_1 is cheating but P_2 is powerless. In general, when the outputs of all evaluation circuits are inconsistent, P_2 will find the wire in s copies of the circuit but output different results and then store the garbled values b_0 corresponding to 0 and b_1 corresponding to 1 for the output of this output wire in different circuits. Finally, P_2 inputs them into the check protocol to obtain the private input of P_1, so as to calculate $f(x, y)$ locally.

2. Related Work

Secure multiparty computation is an active research field of cryptography, and there is more and more extensive research on secure two-party computation. Its classical architectures often use garbled circuits [17] or GMW protocols [18], with the main research being on using garbled circuits to design an efficient secure computation protocol in different security models [19, 20] and optimizing the efficiency of various security protocols [21–23]. Particularly, the problem of efficiency has attracted a great deal of attention due to the large amount of bandwidth it requires. How to efficiently perform the computation in a malicious model is essential. Taking the running time of the entire protocol into account, the cut-and-choose approach is almost the best method to achieve security against the malicious adversary.

Pinkas et al. first introduced the cut-and-choose approach [4] into the garbled circuit in 2003, and Lindell proposed the first secure two-party protocol with complete security proof in 2007 [24]. The most classic protocol can be traced back to reference [9]. It divides 50% check circuits and 50% evaluation circuits to achieve security against the malicious adversary, and P_1's cheating probability is $2^{-0.311s}$. Therefore, an error probability of 2^{-40} can only be achieved when s is set to 132 (132 gates). This means the cost of achieving security against the malicious adversary is 132 times that of a semihonest adversary. In contrast, it divides 60% check circuits and 40% evaluation circuits to get an error probability of $2^{-0.32s}$ in reference [25]. Reference [26] proposed the idea of a symmetrical cut-and-choose. The idea is essentially that two parties involved work together to construct s copies of garbled circuits, which are then checked by someone else. The probability of an error is $2^{-k+O(\log k)}$. In reference [27], it applies the cut-and-choose technique to three-party computation. The cost of achieving security against a malicious adversary is comparatively small to other semihonest 3PC.

Using the cut-and-choose technique will bring some problems. In order to solve the input consistency problem, earlier work [4] used commitment schemes, but the communication overhead was significant. Shelat and Shen proposed a consistency detection method [25] in 2011 that reduces the communication overhead by transmitting a small number of parameters instead of zero-knowledge proofs. In 2014, Frederiksen constructed a circuit extension [28] that uses function f' instead of $f(x, y)$. With this modification, the calculation result of the new function f' is the same as the original $f(x, y)$, but it needs to come from the constructor P_1 and the evaluator P_2 additional random input bits. With statistical security, it can be verified that the inputs of both parties to all circuits are consistent. In addition, there are some schemes [29–31] that also give solutions to the problem of input consistency. For the selective failure attack problem, the evaluator in work [24] takes the XOR value of the real input and multiple random bits as the OT input so that the evaluator has nothing to do with the real input when it exits. The constructor cannot infer the evaluator input by selective failure attack. References [25, 32] solved this problem by a committing OT and a circuit extension, respectively.

Reference [16] uses a check mechanism to prevent P_2 from being powerless. If P_2 finds that the output values of all evaluation circuits are inconsistent, it stores a piece of evidence and then inputs this evidence in the check protocol to obtain the private input x of P_1 and finally calculates the function $f(x, y)$ locally. The work [33] proposed a method to encode trapdoors in the output wires, allowing the evaluator to recover the input of the constructor when multiple outputs are obtained.

In 2015, Zhao et al. first proposed the CCBOT primitive based on the CCOT protocol and constructed a complete CCBOT protocol based on homomorphic encryption. This CCBOT protocol achieved security against the malicious adversary. And then, an improved version of CCBOT based on the decisional Diffie–Hellman (DDH) assumption [14] was proposed in 2016. It greatly improved the efficiency of CCBOT but without using cut-and-choose. Ning and Wang proposed a novel CCBOT protocol [34] based on the computational Diffie–Hellman (CDH) assumption in 2020. It achieved security against the malicious adversary and the error probability of P_1 is 2^{-s}.

3. Preliminaries

We define ℓ, n, a, and s as the length of inputs, computational safety parameter, arbitrary strings, and statistical security parameter, respectively. In order to give a formal definition of security, we first introduce how to describe the indistinguishability of the probability ensemble. As we know, the cut-and-choose technique requires multiple circuits. Therefore, the probability ensemble is related to computational security parameter n, arbitrary strings a, and statistical security parameter s. In this paper, we use (n, s) – indistinguishability to describe the indistinguishability of the probability ensemble, and its formal definition is as follows:

3.1. (n, s) – Indistinguishability. There are two probability ensembles X and Y. They are in the form of $X = \{X(a, n, s)\}_{n,s\in\mathbb{N};a\in(0,1)^*}$ and $Y = \{Y(a, n, s)\}_{n,s\in\mathbb{N};a\in\{0,1\}^*}$ and satisfy that for any n and s, the value range of the two probability distributions is a string of length l, where l is represented as a polynomial of $n + s$. If for every nonuniform polynomial-time distinguisher D, $s \in \mathbb{N}$, polynomial $p(\cdot)$, $a \in \{0, 1\}^*$, and $n \in \mathbb{N}$, there exists a constant $-1 < c < 0$, and the following inequality satisfies

$$|\Pr[D(X(a, n, s), a, n, s) = 1] - \Pr[D(Y(a, n, s), a, n, s) = 1]| < \frac{1}{p(n)} + \frac{1}{2^{c\cdot s}}. \quad (1)$$

We can say X and Y are (n, s) – indistinguishability and denoted by $X^{n,s} \equiv Y$.

3.2. Ideal/Real Simulation Paradigm and Definition of Security. In this paradigm, there is an ideal world and a real world. In the real world, adversary $\mathcal{A}$ executes the secure computation protocol jointly with another honest party

(joint output is denoted as $\mathrm{IDEAL}_{f,S(z),i}(x, y, n, s)$), and in the ideal world, the simulator $\mathcal{S}$ executes the secure computation protocol jointly with another honest participant (joint output is denoted as $\mathrm{REAL}_{\pi,\mathcal{A}(z),i}(x, y, n, s)$). Below, we express the security of a secure two-party computation protocol:

$$\left\{\mathrm{IDEAL}_{f,S(z),i}(x, y, n, s)\right\}^{n,s} \equiv \left\{\mathrm{REAL}_{\pi,\mathcal{A}(z),i}(x, y, n, s)\right\}, \tag{2}$$

where $x, y, z \in \{0,1\}^*$, $|x| = |y|$, and $n, s \in \mathbb{N}$. Then, we can conclude protocol π securely computes function f.

4. Cut-and-Choose Bilateral Obvious Transfer

The key transfer phase of our secure protocol uses the CCBOT protocol. A CCBOT protocol is a variant of CCOT with the additional property that the sender can actively send its own values to the receiver based on the subset selected by the receiver. The starting point for us to construct the CCBOT for Yao's protocol is the protocol of Wei et al. [14]. In the protocol of reference [14], b is the permutation bit of the sender S, and the value σ and τ are the choice-bit of the sender S and R, respectively. (x_0, x_1) are the garbled keys corresponding to 0 and 1 of S's input wires, and (r_0, r_1) are the garbled keys corresponding to 0 and 1 of R's input wires. Moreover, the receiver R has a choice-bit and indices set so that it can obtain the value of r corresponding to the choice-bit. Then it uses five tuples $(T_1, T_2, T_3, T_4, T_5)$ to transfer the values $(x_\sigma, x_{1-\sigma}, \sigma \oplus b, r_0)$ and r_1, respectively. After the transfer is complete, R either obtains the pairs (x_b, x_{1-b}), (r_0, r_1) or receives x_σ and r_τ. According to the value of j, R varies whether each of the five tuples is a DH tuple. If all the DH tuples have the same witness, S can obtain the corresponding values by the witness. To prevent the malicious R, here needs the zero-knowledge proof of the DH tuple to prove that the DH tuples generated by R are correct. We give the details of zero-knowledge proof of the DH tuple in the appendix.

It is worth noting that the CCBOT protocol constructed in reference [14] does not use the cut-and-choose technique. In order to apply the CCBOT protocol to Yao's protocol, the first step is to introduce the cut-and-choose technique into it, so a security parameter s is added. The essence of the CCBOT with the introduction of the cut-and-choose technique is to run s copies of the CCBOT protocol of reference [14]. Next, we will describe the functionality of CCBOT and improve it to single-choice CCBOT and batch single-choice CCBOT that we will use. As both single-choice CCBOT and batch single-choice CCBOT are based on the original CCBOT with certain restrictions and processing, these changes do not affect the security of the protocols, so we omit the security proofs for the following protocols, but give their functionality, detailed description, and approximate efficiency. In Figure 1, we formally define the functions of CCBOT, which are denoted by $\mathcal{F}_{\mathrm{ccbot}}$. In this protocol, there are $30s$ exponents and two rounds of communication.

For instantiating the CCBOT function, we describe its functionality in a secure protocol. Through $\mathcal{F}_{\mathrm{ccbot}}$, parts of these circuits are opened. P_2 obtains all the keys on the input wires of P_1 and P_2 in this part of the circuit. For the remaining circuit, P_2 receives the keys corresponding to its own input and the keys sent by P_1. For security, the order of the keys corresponding to P_2's input wires received by P_2 is replaced at random in check circuits. Obviously, P_2 can obtain the keys that are used to check circuits and evaluation circuits at one time, without the need for additional interactions to send additional keys and other proof of consistency.

CCBOT Functionality $\mathrm{F}_{\mathrm{ccbot}}$

Inputs:

— S inputs the vector of pairs $\{(x_0^j, x_1^j)\}_{i=1}^s, \{(r_0^j, r_1^j)\}_{i=1}^s$, permutation bit $b_1, \ldots, b_s \in \{0,1\}$, choice-bit $\sigma_1, \ldots, \sigma_s \in \{0,1\}$.

— R inputs choice-bit $\tau_1, \ldots, \tau_s \in \{0,1\}$ and the indices set $\mathrm{J} \subset [s]$.

Outputs:

— For every $j \in \mathrm{J}$, R receives the pairs $(x_{b_j}^j, x_{1-b_j}^j)$, (r_0^j, r_1^j), and the value of b_j.

— For every $j \notin \mathrm{J}$, R receives $x_{\sigma_j}^j$, $r_{\tau_j}^j$, and $\sigma_j \oplus b_j$.

Figure 1: The CCBOT functionality $\mathcal{F}_{\mathrm{ccbot}}$ between the sender and the receiver.

4.1. Single-Choice CCBOT. There will be a problem that the functionality $\mathcal{F}_{\mathrm{ccbot}}$ cannot guarantee that R inputs the identical choice-bit in the same input wire of all circuits. As we know, every bit of R's input needs an oblivious transfer. Therefore, it must be ensured that the inputs on the same input wire of R in all garbled circuits are identical. So we propose a variant of the original CCBOT protocol. Here, we use a single-choice CCBOT functionality $\mathcal{F}_{\mathrm{ccbot}}^S$ that is implemented by modifying the CCBOT protocol during the transmission phase for ensuring that R inputs the same choice-bit in each pair of tuples. Since R uses the same choice-bit in different tuples, then the key value associated with R's input wire only needs to be computed once so that this will reduce $s - 1$ exponents. As a result, in this protocol, there are $29s$ exponents and two rounds of communication.

In Figure 2, we formally define the protocol of single-choice CCBOT functionality $\mathcal{F}_{\mathrm{ccbot}}^S$, and a simple example is provided in Figure 3.

4.2. Batch Single-Choice CCBOT. Using the cut-and-choose approach requires the construction of s circuits. Single-choice CCBOT needs to be performed on all wires in every circuit. Hence, there we use an improvement of single-choice CCBOT called batch single-choice CCBOT. There are $15s\ell$ exponents and two rounds of communication in this protocol. In Figure 4, we formally define the protocol of batch single-choice CCBOT functionality $\mathcal{F}_{\mathrm{ccbot}}^{S,B}$, and a simple example is provided in Figure 5.

5. Secure Two-Party Computation Protocol

5.1. Protocol Description. The circuit constructor P_1 first locally constructs s garbled circuits as follows. P_1 chooses random value $a_1^0, a_1^1, \ldots, a_\ell^0, a_\ell^1$ and $r_1, \ldots, r_s$. Let the values $g^{a_i^0 \cdot r}$ and $g^{a_i^1 \cdot r}$ be the keys of P_1's input wire corresponding to 0 and 1 on the ith input wire in the jth circuit, respectively.

Single-Choice CCBOT Functionality $\mathrm{F}_{\mathrm{ccbot}}^{\mathrm{S}}$

Inputs:

— S inputs values $\{(x_0^j, x_1^j)\}_{j=1}^s$, $\{(r_0^j, r_1^j)\}_{j=1}^s$, permutation bit $b_1, \ldots, b_s \in \{0, 1\}$, and choice-bit $\sigma_1, \ldots, \sigma_s \in \{0,1\}$.

— R inputs choice-bit $\tau \in \{0,1\}$ and the indices set $\mathrm{J} \subset [s]$.

Outputs:

—For every $j \in \mathrm{J}$, R receives the pairs $(x_{b_j}^j, x_{1-b_j}^j)$, (r_0^j, r_1^j) and the value of b_j.

—For every $j \notin \mathrm{J}$, R receives $x_{\sigma_j}^j$, r_τ^j and $\sigma_j \oplus b_j$.

Figure 2: The single-choice CCBOT functionality $\mathcal{F}_{\mathrm{ccbot}}^{\mathrm{S}}$ between the sender and the receiver.

S's inputs are as follows, please note that it also input choice-bit σ_j and permutation bits b_j. R's inputs are τ and the indices set $\mathrm{J} \subset [s]$. R receives the values $(x_{b_j}^j, x_{1-b_j}^j)$ and (r_0^j, r_1^j) as well as the value b_j where $j \in \mathrm{J}$. For example, these are all pairs of S's inputs.

$$(x_0^1, x_1^1)(r_0^1, r_1^1) \quad (x_0^2, x_1^2)(r_0^2, r_1^2) \ldots (x_0^j, x_1^j)(r_0^j, r_1^j) \ldots (x_0^s, x_1^s)(r_0^s, r_1^s)$$

After the protocol, R receives the following values where $j \in \mathrm{J}$ and $\tau = 0$:

$$(x_{\sigma_1}^1)(r_0^1) \quad (x_{\sigma_1}^2)(r_0^2) \quad \ldots \quad (x_{b_j}^j, x_{1-b_j}^j)(r_0^j, r_1^j) \quad \ldots \quad (x_{\sigma_s}^s)(r_0^s)$$

Figure 3: A detailed description of $\mathcal{F}_{\mathrm{ccbot}}^{S}$ where $j \in \mathcal{J}$ and $\tau = 0$.

The keys associated with P_2's input wires are set to be $\vec{z}_1, \ldots, \vec{z}_\ell$. After two parties run the batch single-choice CCBOT protocol, P_2 has obtained all the keys ($\vec{z}_j$, $g^{a_i^{b_i} \cdot r_j}$, and $g^{a_i^{1-b_i} \cdot r_j}$ ($j \in \mathcal{J}$)) on the input wires of both parties in check circuits and the keys (z_{y_j} and $g^{a_i^{\sigma_i} \cdot r_j}$ ($j \notin \mathcal{J}$)) associated with the true inputs of both parties in evaluation circuits. Next, P_2 checks whether check circuits are correctly constructed and then decrypts evaluation circuits. If the output values of all evaluation circuits are inconsistent, P_2 will store the garbled values b_0 corresponding to 0 and b_1 corresponding to 1 for the output of this output wire of different circuits, respectively, and then P_1 and P_2 run a check protocol for preventing cheat. Essentially, P_1 and P_2 run the secure protocol of reference [9], and the circuits used in the secure protocol are for computing a bit-by-bit comparison function. If the check protocol is not aborted, P_2 obtains x and computes the function $f(x, y)$ locally.

Before giving a detailed protocol, it is worth noting that we have revised the garbled table (output translation table) commonly used in Yao's protocol. We respectively define k_i^0 as the garbled value corresponding to the bit 0, k_i^1 as the garbled value corresponding to the bit 1 of the wire i, and H as a hash function. Therefore, the garbled table on this wire is $[H(k_i^0), H(k_i^1)]$, where $k_i^0 \neq k_i^1$ and $H(k_i^0) \neq H(k_i^1)$. The complete protocol is shown in Figure 6.

5.2. Proof of Security. Here, we demonstrate the security of our protocol $\Pi_{2\mathrm{pc}}$ that is expressed as follows through the real/ideal simulation paradigm [35].

Theorem 1. *Assume that the batch single-choice CCBOT functionality in Section 4.2 is secure and the DDH assumption is hard. Then, the secure protocol in Figure 6 is secure for computing function $f(x, y)$ against the malicious adversary.*

Proof. We analyze our secure protocol $\Pi_{2\mathrm{pc}}$ in a hybrid model with a trusted party. The role of this trusted party is mainly to ensure the secure operation of batch single-choice CCBOT functionality of step 2 and the zero-knowledge proof of step 7. We prove the ability of our secure protocol against the malicious adversary in two parts: the first is the case of P_1 being corrupted, and the second is the case of P_2 being corrupted.

Batch Single-Choice CCBOT Functionality $\mathrm{F}_{\mathrm{ccbot}}^{\mathrm{S,B}}$

Inputs:

— S inputs ℓ vectors of pairs $\vec{x}_i$ and $\vec{r}_i$ of length s, for $i = 1, \ldots, \ell$

$\vec{x}_i = <(x_0^{i,1}, x_1^{i,1}), (x_0^{i,2}, x_1^{i,2}), \ldots, (x_0^{i,s}, x_1^{i,s})>$,

$\vec{r}_i = <(r_0^{i,1}, r_1^{i,1}), (r_0^{i,2}, r_1^{i,2}), \ldots, (r_0^{i,s}, r_1^{i,s})>$

S also inputs choice-bit σ_i and permutation bits $b_{i,j}$.

— R inputs $\tau_i \in \{0,1\}$ and the indices set $\mathrm{J} \subset [s]$, for $i = 1, \ldots, \ell$.

Outputs:

—For every $j \in \mathrm{J}$, R receives the jth pair of $\vec{x}_i$ and $\vec{r}_i$.(i.e., R receives $(x_{1-b_{i,j}}^{i,j}, x_{b_{i,j}}^{i,j})$, $(r_0^{i,j}, r_1^{i,j})$ and $b_{i,j}$)

—For every $j \notin \mathrm{J}$, R receives the value corresponding to σ_i in $\vec{x}_j$ and $\vec{r}_i$. (i.e., R receives $x_{\sigma_i}^{i,j}$, $r_{\tau_i}^{i,j}$ and $\sigma_i \oplus \tau_i$)

Figure 4: The batch single-choice CCBOT functionality $\mathcal{F}_{\mathrm{ccbot}}^{S,B}$ between the sender and the receiver.

Let the following matrix be the inputs of S.

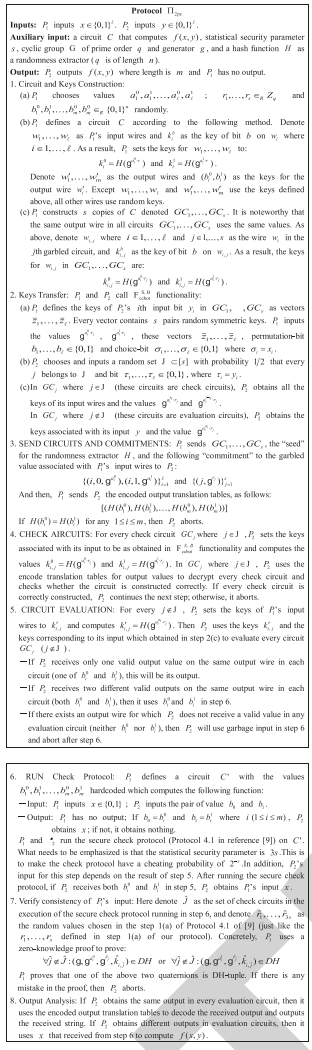
$$\begin{array}{cccc}
(x_0^{1,1}, x_1^{1,1})(r_0^{1,1}, r_1^{1,1}) & (x_0^{1,2}, x_1^{1,2})(r_0^{1,2}, r_1^{1,2}) & \cdots & (x_0^{1,s}, x_1^{1,s})(r_0^{1,s}, r_1^{1,s}) \\
(x_0^{2,1}, x_1^{2,1})(r_0^{2,1}, r_1^{2,1}) & (x_0^{2,2}, x_1^{2,2})(r_0^{2,2}, r_1^{2,2}) & \cdots & (x_0^{2,s}, x_1^{2,s})(r_0^{2,s}, r_1^{2,s}) \\
\vdots & \vdots & \vdots & \vdots \\
(x_0^{i,1}, x_1^{i,1})(r_0^{i,1}, r_1^{i,1}) & (x_0^{i,2}, x_1^{i,2})(r_0^{i,2}, r_1^{i,2}) & \cdots & (x_0^{i,s}, x_1^{i,s})(r_0^{i,s}, r_1^{i,s}) \\
\vdots & \vdots & \vdots & \vdots \\
(x_0^{\ell,1}, x_1^{\ell,1})(r_0^{\ell,1}, r_1^{\ell,1}) & (x_0^{\ell,2}, x_1^{\ell,2})(r_0^{\ell,2}, r_1^{\ell,2}) & \cdots & (x_0^{\ell,s}, x_1^{\ell,s})(r_0^{\ell,s}, r_1^{\ell,s})
\end{array}$$

For every $j \in \mathrm{J}$, R obtains both value of the vector $\vec{x}_i$ (the order of $(x_0^{i,j}, x_1^{i,j})$ depends on b_i) and $\vec{r}_i$. In addition, R receives one of the values of two vectors, depending on S's and R's inputs associated with that row. When $j \in \mathrm{J}$ and $\sigma_i = 0$. R obtains the following values.

$$\begin{array}{cccc}
(x_{\sigma_1}^{1,1})(r_{\tau_1}^{1,1}) & (x_{\sigma_1}^{1,2})(r_{\tau_1}^{1,2}) & \cdots & (x_{b_1}^{1,j}, x_{1-b_1}^{1,j})(r_0^{1,j}, r_1^{1,j}) \quad \cdots \quad (x_{\sigma_1}^{1,s})(r_{\tau_1}^{1,s}) \\
(x_{\sigma_2}^{2,1})(r_{\tau_2}^{2,1}) & (x_{\sigma_2}^{2,2})(r_{\tau_2}^{2,2}) & \cdots & (x_{b_2}^{2,j}, x_{1-b_2}^{2,j})(r_0^{2,j}, r_1^{2,j}) \quad \cdots \quad (x_{\sigma_2}^{2,s})(r_{\tau_2}^{2,s}) \\
\vdots & \vdots & \vdots & \vdots \\
(x_{\sigma_i}^{i,1})(r_{\tau_i}^{i,1}) & (x_{\sigma_i}^{i,2})(r_{\tau_i}^{i,2}) & \cdots & (x_{b_i}^{i,j}, x_{1-b_i}^{i,j})(r_0^{i,j}, r_1^{i,j}) \quad \cdots \quad (x_{\sigma_i}^{i,s})(r_{\tau_i}^{i,s}) \\
\vdots & \vdots & \vdots & \vdots \\
(x_{\sigma_\ell}^{\ell,1})(r_{\tau_\ell}^{\ell,1}) & (x_{\sigma_\ell}^{\ell,2})(r_{\tau_\ell}^{\ell,2}) & \cdots & (x_{\sigma_{iq}}^{\ell,j}, x_{1-b_\ell}^{\ell,j})(r_0^{\ell,j}, r_1^{\ell,j}) \quad \cdots \quad (x_{\sigma_\ell}^{\ell,s})(r_{\tau_\ell}^{\ell,s})
\end{array}$$

Figure 5: A detailed description of $\mathcal{F}_{\mathrm{ccbot}}^{S,B}$ where $j \in \mathcal{J}$ and $\sigma_i = 0$.

P_1 is corrupted: intuitively, one way for P_1 to cheat is by constructing the wrong circuit. In our secure protocol $\Pi_{2\mathrm{pc}}$, due to the check mechanism, if the output values of evaluation circuits are inconsistent, P_2 obtains the private input x of P_1 via the secure computation protocol of step 6. For causing the check mechanism to fail, the output values of all evaluation circuits must not differ. In that way, only when all check circuits are correctly constructed (check passes in step 4, and then P_2 decrypts evaluation circuits) and all evaluation circuits are not correctly constructed (because all evaluation circuits are wrong, no correct result output), P_1 can cheat. It is worth noting that after the batch single-choice CCBOT protocol of step 2 has been run and completed, whether a circuit is a check circuit or an evaluation circuit, whether it is correct, and whether it can be calculated has been determined. Of course, P_1 could also try to cheat by sending the incorrect values to the circuit input wires. However, these incorrect values do not pass the check of zero-knowledge proof, and the protocol is aborted. As a result, with the protocol in



Protocol Π_{2pc}

Inputs: P_1 inputs $x \in \{0,1\}^\ell$. P_2 inputs $y \in \{0,1\}^\ell$.

Auxiliary input: a circuit C that computes $f(x,y)$, statistical security parameter s, cyclic group G of prime order q and generator g, and a hash function H as a randomness extractor (q is of length n).

Output: P_1 outputs $f(x,y)$ where length is m and P_1 has no output.

1. Circuit and Keys Construction:

(a) P_1 chooses values $a_1^0, a_1^1, \ldots, a_\ell^0, a_\ell^1 : r_1, \ldots, r_\ell \in_R Z_q$ and $b_1^0, b_1^1, \ldots, b_m^0, b_m^1 \in_R \{0,1\}^n$ randomly.

(b) P_1 defines a circuit C according to the following method. Denote $w_1, \ldots, w_\ell$ as P_1's input wires and k_i^b as the key of bit b on w_i where $i = 1, \ldots, \ell$. As a result, P_1 sets the keys for $w_1, \ldots, w_\ell$ to:

$$k_i^b = H(g^{a_i^b}) \text{ and } k_i^b = H(g^{a_i^b}).$$

Denote $w_1', \ldots, w_m'$ as the output wires and (b_1^0, b_1^1) as the keys for the output wire w_i'. Except $w_1, \ldots, w_\ell$ and $w_1', \ldots, w_m'$ use the keys defined above, all other wires use random keys.

(c) P_1 constructs s copies of C denoted $GC_1, \ldots, GC_s$. It is noteworthy that the same output wire in all circuits $GC_1, \ldots, GC_s$ uses the same values. As above, denote $w_{i,j}$ where $i = 1, \ldots, \ell$ and $j = 1, \ldots, s$ as the wire w_i in the jth garbled circuit, and $k_{i,j}^b$ as the key of bit b on $w_{i,j}$. As a result, the keys for $w_{i,j}$ in $GC_1, \ldots, GC_s$ are:

$$k_{i,j}^b = H(g^{a_i^b \cdot r_j}) \text{ and } k_{i,j}^b = H(g^{a_i^b \cdot r_j}).$$

2. Keys Transfer: P_1 and P_2 call $F_{ABE}^{s,n}$ functionality:

(a) P_1 defines the keys of P_2's ith input bit y_i in $GC_1, \ldots, GC_s$ as vectors $\Xi_i, \ldots, \Xi_s$. Every vector contains s pairs random symmetric keys. P_2 inputs the values $g^{r_1}, \ldots, g^{r_s}$, these vectors $\Xi_1, \ldots, \Xi_s$, permutation-bit $b_1, \ldots, b_s \in \{0,1\}$ and choice-bit $\sigma_1, \ldots, \sigma_s \in \{0,1\}$ where $\sigma_i = y_i$.

(b) P_2 chooses and inputs a random set $J \subset [s]$ with probability 1/2 that every j belongs to J and bit $\tau_1, \ldots, \tau_s \in \{0,1\}$, where $\tau_i = y_i$.

(c) In GC_j where $j \in J$ (these circuits are check circuits), P_2 obtains all the keys of its input wires and the values g^{r_j} and $g^{a_i^{\tau_i} \cdot r_j}$.

In GC_j where $j \notin J$ (these circuits are evaluation circuits), P_2 obtains the keys associated with its input y and the value $g^{a_i^{\tau_i} \cdot r_j}$.

3. SEND CIRCUITS AND COMMITMENTS: P_1 sends $GC_1, \ldots, GC_s$, the "seed" for the randomness extractor H, and the following "commitment" to the garbled value associated with P_1's input wires to P_2:

$$\{(i, 0, g^{a_i^0}), (i, 1, g^{a_i^1})\}_{i=1}^{\ell} \text{ and } \{(j, g^{r_j})\}_{j=1}^{s}$$

And then, P_1 sends P_2 the encoded output translation tables, as follows:

$$\{(H(b_1^0), H(b_1^1)), \ldots, (H(b_m^0), H(b_m^1))\}$$

If $H(b_i^0) = H(b_i^1)$ for any $1 \le i \le m$, then P_2 aborts.

4. CHECK AIRCUITS: For every check circuit GC_j where $j \in J$, P_1 sets the keys associated with its input to be as obtained in $F_{ABE}^{s,n}$ functionality and computes the values $k_{i,j}^b = H(g^{a_i^b \cdot r_j})$ and $k_{i,j}^b = H(g^{a_i^b \cdot r_j})$. In GC_j where $j \in J$, P_2 uses the encode translation tables for output values to decrypt every check circuit and checks whether the circuit is constructed correctly. If every check circuit is correctly constructed, P_2 continues the next step; otherwise, it aborts.

5. CIRCUIT EVALUATION: For every $j \notin J$, P_2 sets the keys of P_1's input wires to $k_{i,j}^{\tau_i}$ and computes $k_{i,j}^{\tau_i} = H(g^{a_i^{\tau_i} \cdot r_j})$. Then P_2 uses the keys $k_{i,j}^{\tau_i}$ and the keys corresponding to its input which obtained in step 2(c) to evaluate every circuit GC_j ($j \notin J$).

- If P_2 receives only one valid output value on the same output wire in each circuit (one of b_i^0 and b_i^1), this will be its output.
- If P_2 receives two different valid outputs on the same output wire in each circuit (both b_i^0 and b_i^1), then it uses $b_i^0$and b_i^1 in step 6.
- If there exists an output wire for which P_2 does not receive a valid value in any evaluation circuit (neither b_i^0 nor b_i^1), then P_2 will use garbage input in step 6 and abort after step 6.

6. RUN Check Protocol: P_1 defines a circuit C' with the values $b_1^0, b_1^1, \ldots, b_m^0, b_m^1$ hardcoded which computes the following function:

- Input: P_1 inputs $x \in \{0,1\}$; P_2 inputs the pair of value b_0 and b_1.
- Output: P_1 has no output; If $b_0 = b_i^0$ and $b_1 = b_i^1$ where i ($1 \le i \le m$), P_2 obtains x; if not, it obtains nothing.

P_1 and P_2 run the secure check protocol (Protocol 4.1 in reference [9]) on C'. What needs to be emphasized is that the statistical security parameter is $3s$.This is to make the check protocol have a cheating probability of 2^{-s}.In addition, P_2's input for this step depends on the result of step 5. After running the secure check protocol, if P_2 receives both b_i^0 and b_i^1 in step 5, P_2 obtains P_1's input x.

7. Verify consistency of P_1's input: Here denote $\hat{J}$ as the set of check circuits in the execution of the secure check protocol running in step 6, and denote $\hat{r}_1, \ldots, \hat{r}_{3s}$ as the random values chosen in the step 1(a) of Protocol 4.1 of [9] (just like the $r_1, \ldots, r_s$ defined in step 1(a) of our protocol). Concretely, P_1 uses a zero-knowledge proof to prove:

$$\forall j \in \hat{J} : (g, g^{r_j}, g^{\hat{r}_j}, \hat{k}_{i,j}^{\tau_i}) \in DH \text{ or } \forall j \notin \hat{J} : (g, g^{r_j}, g^{\hat{r}_j}, \hat{k}_{i,j}^{\tau_i}) \in DH$$

P_1 proves that one of the above two quaternions is DH-tuple. If there is any mistake in the proof, then P_2 aborts.

8. Output Analysis: If P_2 obtains the same output in every evaluation circuit, then it uses the encoded output translation tables to decode the received output and outputs the received string. If P_2 obtains different outputs in evaluation circuits, then it uses x that received from step 6to compute $f(x,y)$.

Figure 6: Protocol of computing $f(x,y)$.

Figure 6, P_2 always obtains the final result $f(x,y)$ except in the case where all check circuits are correctly constructed and all evaluation circuits are incorrectly constructed, either because all the evaluation circuits are correct and output the same result or because P_1 cheats so that P_2 learns P_1's input x. Through the above analysis, below, we provide the formal proof.

We define $\mathcal{A}$ as the adversary controlling P_1 during the execution of the secure protocol. In the ideal world, there is a simulator $\mathcal{S}$ and a trusted party f. Simulator $\mathcal{S}$ plays the role of the real-world adversary $\mathcal{A}$ and executes the secure protocol with the trusted party f and P_2. Here is how $\mathcal{S}$ would work in the ideal world:

(1) $\mathcal{S}$ obtains the inputs that the adversary $\mathcal{A}$ inputs to the trusted party for the batch single-choice CCBOT functionality. These inputs form a $l \times s$ matrix of pairs $\left\{(x_0^{i,j}, x_1^{i,j}), (z_0^{i,j}, z_1^{i,j})\right\}$, where $i = 1, \ldots, \ell$ and $j = 1, \ldots, s$. $\mathcal{S}$ play the honest P_2 with input $y = 0^\ell$.

(2) $\mathcal{S}$ receives s copies of the circuit $GC_1, \ldots, GC_s$ that send by $\mathcal{A}$ and the values $\left\{(i, 0, g^{a_i^0}), (i, 1, g^{a_i^1})\right\}_{i=1}^{\ell}$ and $\left\{(j, g^{r_j})\right\}_{i=1}^{s}$.

(3) Under the restriction that the probability that j belongs to $\mathcal{J}$ is one half, $\mathcal{S}$ randomly selects a subset $\mathcal{J} \subset [s]$ and sends $\left\{(x_0^{i,j}, x_1^{i,j}), (z_0^{i,j}, z_1^{i,j})\right\}$ to $\mathcal{A}$, where $j \in \mathcal{J}$.

(4) $\mathcal{S}$ obtains all the keys of P_1 and P_2's input wires when $j \in \mathcal{J}$. Then, $\mathcal{S}$ decrypts the circuit through these keys and judges whether it is constructed correctly. Otherwise, $\mathcal{S}$ send $\perp$ to the trusted party and simulates aborting.

(5) Let $x = x_1, \ldots, x_\ell$ be the witness of the zero-knowledge proof in step 7. $\mathcal{S}$ receives $x = x_1, \ldots, x_\ell$ from $\mathcal{A}$. If one of the $x_1, \ldots, x_\ell$ is invalid, simulates aborting. Otherwise, $\mathcal{S}$ obtains x and sends it to the trusted party.

There we denote our secure protocol by π. We can conclude that

$$\left\{IDEAL_{f,S}(x, y, z, n, s)\right\}_{x,y,z \in \{0,1\}^*; n,s \in \mathbb{N}} \overset{n,s}{\equiv} \left\{\mathrm{REAL}_{\pi,\mathcal{A}}(x, y, n, s)\right\}_{x,y,z \in \{0,1\}^*; n,s \in \mathbb{N}}, \tag{3}$$

where $x| = |y|$.

Now, we formally calculate the probability of successful cheating for P_1. Let badAll be the case where all evaluation circuits are wrongly constructed and noAbort be the case where P_2 is not aborted in step 4. □

Claim 1. For every $s \in \mathbb{N}$, it holds that

$$\Pr[\text{noAbort} \wedge \text{badAll}] = \left(\frac{1}{2}\right)^s = 2^{-s}. \tag{4}$$

For proof of security, the joint distribution must be indistinguishable, that is, the joint distribution consisting of the outputs of $\mathcal{A}$ and P_2 of the real execution is indistinguishable from the joint distribution consisting of the outputs of $\mathcal{S}$ and P_2 of the ideal execution. It should be noted that since the input of P_2 in the simulation is $y = 0^\ell$, which is different from the input to P_2 in the real world. This may lead to a different probability of $\mathcal{S}$ aborting in the simulation than in the reality of P_2. In addition, We also need to show that if P_2 does not abort in a real protocol execution, then the probability that it also outputs an error result is $2^{-s} + \varepsilon(\cdot)$, where $\varepsilon(\cdot)$ is a negligible function.

Here, we define good and bad circuits. From the whole protocol, we can know whether a circuit is good or bad has been determined in step 3, and it is important to note that a circuit is either good or bad. We claim that a circuit is bad if it cannot be decrypted using the keys $[H(g^{a_1^0 \cdot r_j}), H(g^{a_1^1 \cdot r_j}), \ldots, H(g^{a_\ell^0 \cdot r_j}), H(g^{a_\ell^0 \cdot r_j})]$ of P_1's input

and the keys corresponding to P_2's input ($[(z_0^{1,j}, z_1^{1,j}), \ldots, (z_0^{\ell,j}, z_1^{\ell,j})]$) to get the correct output. These key values are part of the P_1's inputs to the batch single-choice CCBOT.

We now prove the (n, s) – indistinguishability according to claim 1. In fact, as long as the event (noAbort∧badAll) does not occur, the views of the ideal and real world are identically distributed. Firstly, we discuss that if there is a check circuit that is **bad**, then P_2 will detect and abort the protocol. Next, if all check circuits are **good** and at least one **good** circuit exists in the remaining evaluation circuits, and P_2 is not aborted during the entire protocol execution, then P_2 has the same output distribution in the real and simulated execution. This is due to the fact that if one of the evaluation circuits is **good**, then P_2 must be able to get the correct output from this circuit. And if a **bad** circuit outputs a result different from the correct output $f(x, y)$, P_2 must receive two different valid outputs on the same output wire in different evaluation circuits and saves a "proof", then P_2 will obtain P_1's private input x in step 6. Because the secure computation protocol in [9] has an error probability of $2^{-0.311s}$, so we use $3s$ to guarantee an error probability of $2^{-s} + \varepsilon(\cdot)$ for step 6, As a result, P_2 either obtains x or aborts the protocol in step 6. Finally, there is a case where an output wire does not output a valid value in all the evaluation circuits; then P_2 aborts. This is because in this case all the evaluation circuits are wrong and P_2 will continue with step 6. If there is a **bad** check circuit in step 6, then P_2 aborts; conversely, though all check circuits are **good**, P_2 still aborts because no valid value is received. Here, it may differ from the simulation, as it depends on the input of P_2. We conclude that P_2 obtains $f(x, y)$ in real and ideal executions as long as no aborts occur, which is exactly the same as the view of $\mathcal{A}$ in the execution.

From the above analysis, we know that the adversary cannot know whether the output $f(x, y)$ of P_2 is due to all evaluation circuits being correct so the outputs are the same or due to P_2 detecting cheating and then learning P_1's private input x. In addition, the adversary also does not know whether P_2 aborts the protocol because P_1 find that the check circuit is **bad** or because all the evaluation circuits do not output the same result. As a result, if and only if all check circuits are **good** and all evaluation circuits are **bad**, the simulation deviates from the real output distribution. Since the probability of each circuit being **good** or **bad** is exactly 1/2, the probability of P_1 cheating successfully is 2^{-s}.

P_2 is corrupted: In this case, since P_1 is honest, all circuits are **good,** and a circuit is either a check circuit or an evaluation circuit. P_2 will only obtain the same output. In other words, P_2 can only obtain the same value on the same output wire of different evaluation circuits. The security here is guaranteed by the DDH assumption. However, a malicious P_2 may cheat and want to obtain the private input x of P_1 by the following method. P_2 declares that it has obtained two different values on the same output wire of different evaluation circuits and then forges these two different values b_0 and b_1 in step 6 in order to obtain the value of x. In this case, since the hardcoded circuit is random and the computation protocol is secure in step 6, the probability of successful forgery is negligible. Below, we provide the formal proof.

We define $\mathcal{A}$ as the adversary controlling P_2 during the execution of the secure protocol Π_{2pc}. In the ideal world, there is a simulator $\mathcal{S}$ and a trusted party f. Simulator $\mathcal{S}$ plays the role of the real-world adversary $\mathcal{A}$ and executes the secure protocol with the trusted party f and $\mathcal{S}$. Here is how $\mathcal{S}$ would work in the ideal world:

(1) $\mathcal{S}$ obtains P_2's inputs that include $y = \sigma_1, \ldots, \sigma_\ell$ and a set $\mathcal{J} \subset [s]$ from $\mathcal{A}$.

(2) $\mathcal{S}$ sends $y = \sigma_1, \ldots, \sigma_\ell$ to the trusted party and obtains the output $z = f(x, y)$.

(3) $\mathcal{S}$ randomly selects a pair of values (b_0, b_1) and uses them as the input of P_2 in step 6.

(4) If $b_0 = b_i^0$ and $b_1 = b_i^1$, then simulation aborted. Otherwise, the simulation continues according to the protocol of step 6 and then ends.

We can conclude that

$$\left\{\text{IDEAL}_{f,S}(x, y, z, n, s)\right\}_{x,y,z\in\{0,1\}^*;n,s\in\mathbb{N}}{}^{n,s} \equiv \left\{\text{REAL}_{\pi,\mathcal{A}}(x, y, n, s)\right\}_{x,y,z\in\{0,1\}^*;n,s\in\mathbb{N}}, \tag{5}$$

where $x| = |y|$.

We know that the probability of P_2 successfully forging b_0 and b_1 is negligible. In the following, we need to prove that when the above situation does not exist, that is, when P_2 forgery fails, the output distribution of the real world and the simulated world are indistinguishable. In the ideal world, the simulation aborts if P_2 is successfully faked. Conversely, if the forgery fails and the simulation continues, then the secure computing protocol in step 6 has no output, that is, P_2 cannot obtain the private input of P_1 (P_2) only obtains $f(x, y)$ from the trusted party f. In the real world, P_2 obtains $f(x, y)$ by decrypting the circuit, so the output distribution of the ideal world and the real world are indistinguishable.

5.3. Efficiency. As shown in Table 1, we analyze the approximate efficiency of the entire protocol, including the exponentiations, symmetric encryptions, group elements sent, and communication rounds. According to the form, $x^a \cdot y^b$ only need 1.25 standard exponentiations; we calculate the exponentiations for each step: (1) $2s\ell$ for the input key choice and circuit preparation in step 1, (2) $15s\ell$ for the batch single-choice CCBOT of step 2, (3) $9s\ell$ for the secure check protocol of step 6, and (4) $2s\ell$ for verifying the consistency of P_1's input in step 7. In total, there are $28s\ell$ in our protocol.

For the symmetric encryptions, we calculate as follows: $8|C|$ for each circuit construction (s circuits, total $8|C|s$). After running step 2, there are roughly $s/2$ check circuits and

Table 1: Efficiency analysis of each step of our protocol.

Step	Exponentiations	Symmetric encryptions	Group elements sent	Communication rounds of $\mathcal{F}_{\text{ccbot}}^{S,B}$/ $\mathcal{F}_{\text{ccbot}}^{S,B}$ with zero-knowledge proof
1	$2s\ell$	$8\|C\|s$		
2	$15s\ell$		$11s\ell$	
3				
4		$s/2 \cdot 8\|C\|$		
5		$s/2 \cdot 2\|C\|$		2/6
6	$9s\ell$	$39s\ell$		
7	$2s\ell$		$21s\ell$	
8				
Total	$28s\ell$	$13\|C\|s + 39s\ell$	$32s\ell$	

Protocol $\Pi_{\text{ZKPK-DH tuples}}$

Joint statement: The value (G, g_0, g_1, u, v) are elements of a group G which has an order q, and a generator g.

Auxiliary input for the prover: A witness w such that $u = (g_0)^w$ and $v = (g_1)^w$.

The protocol:

1. P chooses a random $a \in \{1,\ldots,q\}$ and computes $\alpha = (g_0)^a$ and send α to V.
2. The verifier V choose random $s,t \in \{1,\ldots,q\}$, computes $c = (g_0)^s \cdot \alpha^t$ and sends c to P (this is a perfectly-hiding commitment to s).
3. P chooses a random $r \in \{1,\ldots,q\}$ and computes $A = (g_0)^r$ and $B = (g_1)^r$. It then sends (A, B) to V.
4. V sends s and t as above to P.
5. P verifies that $c = (g_0)^s \cdot \alpha^t$. If no, it aborts. Otherwise, it sends $z = s \cdot w + r$ to V. In addition, it sends a as chosen above.

V accepts if and only if $\alpha = (g_0)^a$, $A = (g_0)^z / u^s$ and $B = (g_1)^z / v^s$.

Figure 7: Protocol of zero-knowledge proof for DH tuples.

Protocol $\Pi_{\text{ZKPK-EDH tuples}}$

Common input: $(g_0, g_1, h_0, h_1, x_1, y_1, \ldots, x_n, y_n)$

Prover witness: for every i, there exist a constant a which satisfies either $h_0 = (g_0)^a$ and $x_i = (y_i)^a$ or $h_1 = (g_1)^a$ and $x_i = (y_i)^a$.

The protocol:

1. V picks $\mu_1,\ldots,\mu_n \in_R \{0,1\}^L$ where $2^L < q$, and sends $\mu_1,\ldots,\mu_n$ to P.
2. V and P locally compute $x = \Pi_{i=1}^n (x_i)^{\mu_i}$ and $y = \Pi_{i=1}^n (y_i)^{\mu_i}$
3. P uses protocol $\Pi_{\text{ZKPK-DH tuples}}$ to prove that either (g_0, h_0, x, y) or (g_1, h_1, x, y) is a DH tuple. V accepts if and only it accepts in $\Pi_{\text{ZKPK-DH tuples}}$.

Figure 8: Protocol of zero-knowledge proof for extended DH tuples.

$s/2$ evaluation circuits. A total of $s/2 \cdot 8|C| + s/2 \cdot 2|C| = 5|C|s$ symmetric encryptions are required for check and evaluation. In addition, the error probability of the security computation protocol [9] used by the check mechanism of step 6 is $2^{-0.311s}$. Therefore, $3s$ circuits are required so that keep the error probability at 2^{-s} and need $3 \times 13 \cdot s \cdot \ell = 39s\ell$. In total, there has $8|C|s + 5|C|s + 39s\ell = 13|C|s + 39s\ell$ symmetric encryptions.

6. Conclusion

In this paper, we propose an improvement of CCBOT that is called batch single-choice CCBOT. We formalize our batch single-choice CCBOT function and apply it to Yao's protocol and then present a new secure two-party computation protocol that achieves security against the malicious adversary. Our new protocol not only can reduce the number of interactive rounds of the protocol but also can solve the problem of input consistency and prevent selective failure attacks. In addition, a check mechanism is used to prevent P_1 from cheating but P_2 is powerless and the probability of error for P_2 is 2^{-s}.

In the future, we will continue to study common secure computation protocols, focusing on efficient constant-round secure multiparty based on garbled circuits in the malicious model.

Appendix

A. Zero-Knowledge Proof for Diffie–Hellman Tuples

We show the zero-knowledge proof for DH tuples in Figure 7. There are 12 exponentiations, including 8 of $x^a \cdot y^b$. Then, all the form $x^a \cdot y^b$ costs $8 \times 1.25 = 10$ exponentiations. Concretely, the zero-knowledge proof for DH tuples costs 11 exponentiations and 5 rounds of communication.

B. Zero-Knowledge Proof for Extended Diffie–Hellman Tuples

We show the zero-knowledge proof for extended DH tuples in Figure 8 that is used in protocol Π_{2pc}. According to the previous work [9], there are $n + 18$ exponentiations and five rounds of communication.

Data Availability

No data were used to support this study.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

The authors would like to thank their supervisor for always helping and supporting them. This work was supported by the Support Plan of the Scientific and Technological Innovation Team in Universities of Henan Province (No.

20IRTSTHN013), the Youth Talent Support Program of Henan Association for Science and Technology (No. 2021HYTP008), the Fundamental Research Funds for the Universities of Henan Province (No. NSFRF210312), and the PhD Foundation of Henan Polytechnic University (No. B2021-41).

References

[1] Y. Lindell, "Secure multiparty computation," *Communications of the ACM*, vol. 64, no. 1, pp. 86–96, 2021.

[2] A. C. Yao, "How to generate and exchange secrets," in *Proceedings of the 27th Annua Symposium on Foundations of Computer Science*, pp. 162–167, IEEE, Toronto, Canada, July1986.

[3] A. Shamir, "How to share a secret," *Communications of the ACM*, vol. 22, no. 11, pp. 612-613, 1979.

[4] B. Pinkas, "Fair secure two-party computation," in *Proceedings of the Int Conf on the Theory and Applications of Cryptographic Techniques*, pp. 87–105, Berlin, Heidelberg, May 2003.

[5] M. Kiraz and B. Schoenmakers, "A protocol issue for the malicious case of Yao's garbled circuit construction," *27th Symposium on Information Theory in the Benelux*, vol. 29, no. 4, pp. 283–290, 2006.

[6] V. Kolesnikov and R. Kumaresan, "On cut-and-choose oblivious transfer and its variants," in *Proceedings of the Advances in Cryptology ASIACRYPT 2015*, pp. 386–412, Berlin, Heidelberg, January 2015.

[7] X. Wei, L. Xu, M. Zhao, and H. Wang, "Secure extended wildcard pattern matching protocol from cut-and-choose oblivious transfer," *Information Sciences*, vol. 529, no. 11, 2020.

[8] X. Wei, L. Xu, H. Wang, and Z. Zheng, "Permutable Cut-And-Choose Oblivious Transfer and its Application," *IEEE Access*, vol. 8, pp. 17378–17389, 2020.

[9] Y. Lindell and B. Pinkas, "Secure Two-Party Computation via Cut-and-Choose Oblivious Transfer," *Theory of Cryptography*, vol. 25, no. 4, pp. 329–346, 2011.

[10] Y. Huang, J. Katz, V. Kolesnikov, R. Kumaresan, and A. J Malozemoff, "Amortizing garbled circuits," in *Proceedings of the Annual Cryptology Conferance*, pp. 458–475, Berlin, Heidelberg, May 2014.

[11] C. Hazay and Y. Lindell, *Efficient Secure Two-Party Protocols: Techniques and Constructions*, Information Security and Cryptography, Berlin, Heidelberg, pp. 3–254, 2010.

[12] Y. Lindell and B. Riva, *Cut-and-Choose Yao-Based Secure Computation in the Online/Offline and Batch Settings*, CRYPTO, Berlin, Heidelberg, pp. 476–494, 2014.

[13] C. Zhao, H. Jiang, X. Wei, Q. Xu, and M. Zhao, "Cut-and-choose bilateral oblivious transfer and its application," in *Proceedings of the 14th IEEE International Conference on Trust, Security and Privacy in Computing and Communications*, pp. 384–391, Helsinki. Finland, August 2015.

[14] X. Wei, H. Jiang, C. Zhao, M. Zhao, and Q. Xu, "Fast cut-and-choose bilateral oblivious transfer for malicious adversaries," in *Proceedings of the IEEE International Conference on Big Data Science and Engineering*, pp. 418–425, Tianjin, China, Februray 2016.

[15] M. Naor and O. Reingold, *Synthesizers and their application to the parallel construction of psuedo-random functions*, vol. 58, pp. 170–181, Journal of Computer and System Sciences, 1995.

[16] Y. Lindell, "Fast cut-and-choose-based protocols for malicious and covert adversaries," *Journal of Cryptology*, vol. 29, no. 2, pp. 456–490, 2016.

[17] Y. Huang, D. Evans, J. Katz, and L. Malka, "Faster Secure Two-Party Computation Using Garbled Circuits," in *Proceedings of the USENIX Security Symposium*, Boston, MA, USA, August 2011.

[18] O. Goldreich, S. Micali, and A. Wigderson, "How to play any mental game or A completeness theorem for protocols with honest majority," in *Proceedings of the nineteenth annual ACM symposium on Theory of computingThe 19th STOC*, pp. 218–229, New York, NY, USA, January 1987.

[19] A. Ben-Efraim, Y. Lindell, and E. Omri, "Efficient Scalable Constant-Round MPC via Garbled Circuits," in *Proceedings of the International Conference on the Theory and Application of Cryptology and Information Security*, pp. 471–498, ASIACRYPT, Cham, November 2017.

[20] P. Mohassel and B. Riva, "Garbled circuits checking garbled circuits: more efficient and secure two-party computation," in *Proceedings of the Annual Cryptology ConferenceCRYPTO*, pp. 36–53, Berlin, Heidelberg, July 2013.

[21] V. Kolesnikov and T. Schneider, *Improved Garbled Circuit: Free XOR Gates and Applications*, pp. 486–498, ICALP, Berlin, Heidelberg, 2008.

[22] N. Büscher, M. Franz, A. Holzer, H. Veith, and S. Katzenbeisser, "On compiling Boolean circuits optimized for secure multi-party computation," *Formal Methods in System Design*, vol. 51, no. 2, pp. 308–331, 2017.

[23] O. Biçer, "Efficiency Optimizations on Yao's Garbled Circuits and Their Practical Applications," 2017, https://arxiv.org/abs/1703.03473.

[24] Y. Lindell and B. Pinkas, "An efficient protocol for secure two-party computation in the presence of malicious adversaries," in *Proceedings of the Annual Int Conf on the Theory and Applications of Cryptographic Techniques*, pp. 52–78, Berlin, Heidelberg, May 2007.

[25] A. Shelat and C. H. Shen, "Two-output secure computation with malicious adversaries," in *Proceedings of the In Annual International Conference on the Theory and Applications of Cryptographic TechniquesEUROCRYPT*, pp. 386–405, Berlin, Heidelberg, 2011.

[26] Y. Huang, J. Katz, and D. Evans, "Efficient secure two-party computation using symmetric cut-and-choose," in *Proceedings of the Annual Cryptology ConferenceCRYPTO*, pp. 1–17, Berlin, Heidelberg, 2013.

[27] C. Chen, "Efficient Three-Party Computation: An Information-Theoretic Approach from Cut-And-Choose," 2019, https://arxiv.org/abs/1908.03718.

[28] T. K. Frederiksen and J. B. Nielsen, "Fast and Maliciously Secure Two-Party Computation Using the GPU," in *Proceedings of the International Conference on Applied Cryptography and Network Security*, Cham, January 2013.

[29] A. Afshar, P. Mohassel, B. Pinkas, and B. Riva, "Non-interactive secure computation based on cut-and-choose," in *Proceedings of the Annual International Conference on the Theory and Applications of Cryptographic Techniques*, Berlin, Heidelberg, 2014.

[30] L. T. A. N. Brandao, "Secure two-party computation with reusable bit-commitments, via a cut and-choose with forge-and-lose technique," in *Proceedings of the Int Conf on the Theory and Application of Cryptology and Information Security*, pp. 441–463, Berlin, Heidelberg, December 2013.

[31] B. Pinkas, T. Schneider, N. Smart, and S. Williams, "Secure two-party computation is practical," in *Proceedings of the*

Hindawi
Security and Communication Networks
Volume 2023, Article ID 9865347, 1 page
https://doi.org/10.1155/2023/9865347

Retraction

Retracted: Measurement of Economic Fluctuations Based on High-Frequency Financial Time Series

Security and Communication Networks

Received 8 August 2023; Accepted 8 August 2023; Published 9 August 2023

This article has been retracted by Hindawi following an investigation undertaken by the publisher [1]. This investigation has uncovered evidence of one or more of the following indicators of systematic manipulation of the publication process:

(1) Discrepancies in scope

(2) Discrepancies in the description of the research reported

(3) Discrepancies between the availability of data and the research described

(4) Inappropriate citations

(5) Incoherent, meaningless and/or irrelevant content included in the article

(6) Peer-review manipulation

The presence of these indicators undermines our confidence in the integrity of the article's content and we cannot, therefore, vouch for its reliability. Please note that this notice is intended solely to alert readers that the content of this article is unreliable. We have not investigated whether authors were aware of or involved in the systematic manipulation of the publication process.

Wiley and Hindawi regrets that the usual quality checks did not identify these issues before publication and have since put additional measures in place to safeguard research integrity.

We wish to credit our own Research Integrity and Research Publishing teams and anonymous and named external researchers and research integrity experts for contributing to this investigation.

The corresponding author, as the representative of all authors, has been given the opportunity to register their agreement or disagreement to this retraction. We have kept a record of any response received.

References

[1] H. Zhang, "Measurement of Economic Fluctuations Based on High-Frequency Financial Time Series," *Security and Communication Networks*, vol. 2022, Article ID 9310697, 18 pages, 2022.

Hindawi
Security and Communication Networks
Volume 2022, Article ID 9310697, 18 pages
https://doi.org/10.1155/2022/9310697

Research Article

Measurement of Economic Fluctuations Based on High-Frequency Financial Time Series

HuiLi Zhang

Yellow River Conservancy Technical Institute, KaiFeng, 475000, China

Correspondence should be addressed to HuiLi Zhang; zhanghuili@yrcti.edu.cn

Received 15 April 2022; Accepted 12 May 2022; Published 13 June 2022

Academic Editor: Fang Liu

In order to improve the analysis and forecasting effect of economic fluctuations, this paper combines the high-frequency financial sequence algorithm to conduct measured analysis of economic fluctuations. Under the continuous jump-diffusion price model, this paper considers the jump part and the continuous part in the process of asset pricing. Moreover, for the jump part, this paper uses the wavelet method to analyze the observation data, and obtains the estimator of the second-order jump covariation difference matrix and its convergence speed. For the continuous part, this paper adopts a two-scale realized volatility model under the continuous price model. In addition, this paper verifies the effect of the intelligent model proposed in this paper through simulation experiments. The simulation data shows that the economic fluctuation analysis system based on high-frequency financial time series proposed in this paper has good economic analysis and economic forecasting effects.

1. Introduction

When the economy suffers from monetary disruptions, such as an unexpected increase in the money supply, the increase in the money supply increases the aggregate consumer demand for commodities, that is, commodity market competition intensifies. At the same time, an expansion in aggregate demand leads to an increase in the general price level in the commodity market, but the relative price of each commodity does not actually change. Due to the incompleteness and asymmetry of information, a single manufacturer cannot observe the rise in the prices of all commodities, and mistakenly believes that the prices of the commodities it produces will rise. As a result, manufacturers will have wrong expectations about the demand for their own goods. When the price rises above the manufacturer's expected price, the manufacturer will increase investment and employment, and expand production. If all firms took such action, the level of output and employment would be higher than in competitive equilibrium. In such a case, the economy deviates upward from the potential level and the economy expands. Conversely, if the money supply falls unexpectedly, the general price level in the commodity market falls. When prices fall and fall below firms' expected prices, firms scale back production, output and employment fall below full employment levels, the economy deviates downward from potential, and the economy contracts.

Supply-side shocks, especially productivity shocks, are also one of the important factors affecting economic volatility. When a positive technological shock occurs in the economy, it will lead to an increase in the marginal product of labor. In the labor market, the demand for labor increases and real wages rise. If the economic person expects the technical shock to be temporary, the future real wages may fall, that is, the current leisure price will be higher, and the economic person will tend to replace the current leisure with future leisure. The result is that the economic man reduces the leisure time of the current period and provides more labor supply. As a result, current employment increases and total output increases. If the economic man predicts that the technological shock will be permanent, producers will invest more because of the higher marginal return on capital in the future. The increase in demand for investment goods raises the real interest rate. Consumers believe that the price of current leisure time will rise, and consumers will replace current leisure time with future leisure time. As a result,

employment increased and output increased. When a negative technical shock occurs in the economy, if the technical shock is temporary, the demand for labor in the labor market will decrease, employment will decline, and output will decline. If the negative technology shock is permanent, producers will reduce investment. The decline in demand for investment goods leads to a decline in the real interest rate. Consumers believe that the price of current leisure time has fallen, so consumers will increase current leisure time and reduce labor supply. Reduced labor supply and reduced employment, resulting in lower output.

This paper combines the high-frequency financial sequence algorithm to conduct measured analysis of economic fluctuations, and builds an intelligent economic analysis and forecasting system to promote the analysis and forecasting effect of subsequent economic fluctuations.

2. Related Work

When a country's economy is very dependent on external demand, once the international economic environment deteriorates and external demand weakens, it is difficult to make up for the decline in external demand by increasing domestic demand in the short term. Therefore, higher trade openness means that changes in final demand will become more difficult. The higher the stability, the stronger the volatility of the macro economy [1]. Trade openness helps a country absorb advanced technologies from developed countries, improve resource allocation efficiency, and prompt the government to implement better macro-control policies, thereby improving the ability to cope with domestic shocks and helping to ease economic fluctuations [2]. The impact of trade opening on economic fluctuations is uncertain, which depends on whether potential external shocks can materialize and the magnitude of the shocks. According to the theory of real business cycles, technological shocks are the main source of economic fluctuations [3]. Technological progress is mainly divided into independent innovation and technology introduction. The latter has the characteristics of low cost and fast speed compared with the former. Therefore, developers often adopt the method of importing technology from developed countries to achieve economic catch-up [4]. For a long time, technology introduction has also been used as the main way of technological progress, which makes technological shocks mainly come from external. For developers, technological progress under technology introduction does not always bring about economic fluctuations [5]. Generally speaking, technology introduction improves the efficiency of resource allocation and the potential growth rate of the economy, can maintain a stable long-term economic growth path, and also strengthens the macroeconomy's ability to resist other shocks. However, in the period of economic transformation, the introduction of technologies supporting the old economic growth model will bring certain obstacles to the adjustment of economic structure [6]. The negative impact of technology introduction on economic development will gradually appear, and may cause economic fluctuations [7]. The impact of technology introduction on economic fluctuations mainly depends on the stage of economic development. Short-term international capital is highly speculative, and seeking arbitrage is the main incentive for its flow [8]. When the economy is prosperous, a large amount of short-term international capital flows to seek arbitrage opportunities, resulting in flooding of liquidity, pushing up asset prices, and causing economic overheating [9]. When the economy is depressed, there will be a massive outflow of short-term international capital, triggering market panic and falling asset prices, further aggravating the downward pressure on the economy. The pro-cyclical feature of short-term international capital makes it easy to become an amplifier of the economic cycle, so generally speaking, short-term international capital flows will bring about economic fluctuations [10].

There are a lot of unstable mechanisms in the economy, these unstable mechanisms may not only cause economic fluctuations; but also when the economy fluctuates, the unstable mechanisms will lead to the continuous expansion of economic fluctuations [11]. The research constructs a model of instability mechanism in Harrods economy from the perspective of investment demand. The current output or aggregate demand in this model is determined by the current investment through a multiplier effect. To define a capacity utilization rate, the current capacity utilization rate is equal to the ratio of the current total demand to the current capacity, where the current capacity is defined as the product of the output-capital ratio and the capital existing in the previous period [12]. The capital accumulation equation determines that the capital stock in the current period is equal to the capital stock in the previous period minus depreciation plus additional investment in the current period. At the end of the model, an investment equation is also constructed, and the investment is negatively correlated with the production capacity, that is to say, the investment depends on the capacity utilization rate of the previous period [13]. When examining the stability of the model, it is found that the system is unstable. The study found that enterprises will not only improve their own production capacity through investment behavior, but also bring about an increase in total social demand through the multiplier effect [14]. Generally speaking, the output-capital ratio will not be greater than 1, because the return on investment is often not realized in one period; on the other hand, the investment multiplier is often greater than 1. This means: when the economy is good, companies will increase investment. The total demand increment created by the investment behavior through the multiplier effect will be greater than the actual increase in the production capacity of the enterprise [15]. The result is that companies will continue to invest more, the economy will grow hotter, and the economy will move further and further away from equilibrium. Conversely, when there is a recession, companies reduce investment. The decline in aggregate demand will outweigh the decline in the productive capacity of firms, with the result that investment continues to decline and the economy becomes more sluggish. The price equation is constructed. Add price and monetary policy into the investment equation as stabilizing mechanisms, and test the stability of the model. Finally, it

was found that when the economy fluctuated, price adjustment as a "weak stability mechanism" could not make the economy stable [16]. The expansion of the economy will be accompanied by the accumulation of debts. When the accumulation of debts reaches a certain level (such as the Minsky moment), a large amount of debt in the field of international lending exceeds the borrower's own repayment ability, resulting in inability to repay the debt or the need to defer debt repayment. The phenomenon will inevitably bring huge pressure to the economy, and the crisis will break out [17]. In order to pursue GDP and stimulate economic growth, monetary authorities will implement loose monetary policies, mainly for two reasons: a large number of currency issuance and low interest rates. Stimulated by low interest rates, the manufacturing industry borrows money to buy equipment and build factories, real estate companies borrow money to buy land and build a large number of houses, and the government borrows money for infrastructure construction.

3. Estimation of market microstructure noise error under high frequency financial data

Due to the existence of market microstructure noise, there is a certain deviation between the high-frequency financial data we observe and collect and the unobservable real data. The time period [0, T] is divided into N points, that is, $0 = t_0 < t_1 < t_2 < \cdots t_N = T$, where $\Delta_{t_i} = t_1 - t_{i-1}$, $i = 1, 2, \ldots, N$.

Then, the observed value of the log price at time t_i is:

$$Y_{t_1} = X_{t_1} + \varepsilon_{t_i}, i = 0, 1, \ldots, N, t \in [0, T]. \tag{1}$$

Among them, ε_4 is the market microstructure noise. For unobservable real data X_t, we assume that the logarithmic price process obeys a stochastic differential formula, that is:

$$dX_t = \mu_t \mathrm{d}t + \sigma_t \mathrm{d}W_t. \tag{2}$$

Among them, μ_t is the drift coefficient, σ_t is the instantaneous volatility, and W_t is a standard Brownian motion.

In fact, it exists in a semi-martingale form as follows:

$$X_t = \int_0 \mu_s \mathrm{d}s + \int_0 \sigma_s \mathrm{d}W_s. \tag{3}$$

We assume that the asset price data is observed at time interval δ on [0, T], which is denoted as:

$$R^* (i, \delta) = \ln S_i - \ln S_{i-\delta} = X_t - X_{i-\delta}. \tag{4}$$

The above formula is the continuous compound interest rate of financial assets in the i-th time interval, that is, the logarithmic rate of return. In the financial environment of risk-free arbitrage, the logarithmic rate of return R° of financial assets obeys a special semi-martingale process. If (Ω, I, P) is a complete probability space, and the information filter $(I_t)_{t\in[0,T]} \subseteq I$ is an ascending σ subalgebraic sequence, I_t is P complete and right continuous. $S_t (t \in [0, T]$ is the same as the above definition, it represents the price process of financial native assets in this space, that is, S_t is in the information set I_t at time t.

The logarithmic rate of return of investing in a financial native asset in the Δ time period on day t is:

$$R^* (i, \Delta) = X_1 - X_{i-\Delta}. \tag{5}$$

Among them, t represents the t day, $\Delta > 0$.

When $\Delta = 1$, the realized volatility on day t is defined as follows:

$$[Y, Y]_i = \sum_{i=1}^{n} \left(Y_{t_1} - Y_{t_{t-1}}\right)^2. \tag{6}$$

The above formula is the realized volatility on day t.

The observed (logarithmic) rate of return is now defined as:

$$r_{i,N} = Y_{t_1} - Y_{t_{t-1}}, \quad i = 1, 2, \ldots, N. \tag{7}$$

Accordingly, the effective rate of return is:

$$r^*_{i,N} = X_{t_i} - X_{t_H}, \quad i = 1, 2, \ldots, N. \tag{8}$$

When $\Delta = 1$, the realized volatility on day t is defined as follows:

$$(\mathrm{RV})\mathrm{RV} = \sum_{i=1}^{N} r^2_{i,N}. \tag{9}$$

The noise series of returns is the difference between the observed return and the effective return and is defined as $e_{i,N} = r_{i,N} - r^*_{i,N}$, $i = 1, 2, \ldots, N$.

It can be seen that $e_{i,N} = \varepsilon_{t_i} - \varepsilon_{i_{t-1}}$, $i = 1, 2, \ldots, N$, that is, the noise series of returns has MA(1). We assume that ε_t is an i.i.d. sequence that satisfies:

$$E\varepsilon_{t_1} = E\varepsilon = 0, E\varepsilon^2_{t_1} = E\varepsilon^2. \tag{10}$$

Moreover, it is not related to the effective price X_t. The following formula is obtained:

$$\mathrm{RV} = 2\,\mathrm{NE}\,\varepsilon^2 + O_p\left(N^{1/2}\right). \tag{11}$$

In fact, their results are based on the following formula:

$$RV = \sum_{i=1}^{N} r^2_{i,N} = \sum_{i=1}^{N} r_{i,N}{}^2 + 2\sum_{i=1}^{N} r^{\bullet}_{i,N} e_{i,N} + \sum_{i=1}^{N} e^2_{i,N}. \tag{12}$$

When the sampling frequency is very high, that is, $(N \longrightarrow \infty)$, and the sum of the squares of the noise constitutes the main part of the above formula as $(\mathrm{RV} \longrightarrow \sum_{i=1}^{N} e^2_{i,N})$. Therefore, the RV of the highest frequency data can be used as an estimate of the noise sequence variance.

The Realized Volatility (RV) based on observational data is as follows:

$$\sum_{i=1}^{N} r^2_{i,N} = \sum_{i=1}^{N} r^*_{i,N}{}^2 + 2\sum_{i=1}^{N} r^*_{i,N} e_{i,N} + \sum_{i=1}^{N} e^2_{i,N}. \tag{13}$$

Its conditional mean and variance are as follows:

$$E(\mathrm{RV}|X) = \mathrm{RV}_X + 2\,\mathrm{NE}\,\varepsilon^2,$$
$$\mathrm{Var}(\mathrm{RV}|X) = 4\,\mathrm{NE}\,\varepsilon^4 + O_p(1), \tag{14}$$

Among them, there are:

$$\mathrm{RV}_X = \sum_{i=1}^{N} {r_{i,N}}^2. \tag{15}$$

Therefore, for the efficient price process X, when $N \longrightarrow \infty$, we have its asymptotic normality as follows:

$$N^{-1/2}\left(\mathrm{RV} - 2\mathrm{NE}\,\varepsilon^2\right) \xrightarrow{d} 2\left(E\varepsilon^4\right)^{1/2} Z_{\mathrm{nolse}}. \tag{16}$$

From the above analysis, we can obtain the estimator of the variance of the noise series as follows:

$$\widehat{E}\varepsilon^2 = \frac{\mathrm{RV}}{2N}. \tag{17}$$

For a certain real data process X, when $N \longrightarrow \infty$, we have:

$$N^{1/}\left(\widehat{E}\varepsilon^2 - E\varepsilon^2\right) \xrightarrow{d} N\left(0, E\varepsilon^4\right). \tag{18}$$

Among them, the asymptotic variance $E\varepsilon^4$ can obtain a consistent estimator as follows:

$$\widehat{E}\varepsilon^4 = \frac{1}{2N}\sum_{i=1}^{N} r_{i,N}^4 - 3\left(\widehat{E}^2\right)^2. \tag{19}$$

We assume that the full set is $G, G = \{t_0, t_1, \ldots, t_N\}$, and it is divided into K disjoint subsets $G^{(k)}, k = 1, 2, \ldots, K$, that is, $G = \cup_{k=1}^{K} G^{(k)}$. Among them, when $k \neq l$, $G^{(k)} \cap G^{(l)} = \phi$.

The method for selecting the elements of $G^{(k)}$ in the k-th subset is to start with t_{k-1}, and then take every K steps as sampling points until T. That is to say, $G^{(k)} = \{t_{k-1}, t_{k-1+K}, t_{k-1+2K}, \ldots t_{k-1+n_k K}\}$.

Among them, $k = 1, 2, \ldots, K, n_k$ is an integer that makes $t_{k-1+n_k K}$ the last element in $G^{(k)}$. Thus, we obtain an estimate of volatility, that is:

$$\mathrm{RV}^{(\mathrm{avg})} = \frac{1}{K}\sum_{k=1}^{K} \mathrm{RV}^{(k)}. \tag{20}$$

Its mean and variance are:

$$E\left(\mathrm{RV}^{(\mathrm{arg})}|X\right) = \mathrm{RV}_X^{(\mathrm{ang})} + 2\overline{n}E\varepsilon^2,$$
$$\mathrm{Var}\left(\mathrm{RV}^{(\mathrm{avg})}|X\right) = \frac{1}{K^2}\sum_{k=1}^{K}\mathrm{Var}\left(RV^{(\mathrm{avg})}|X\right) \tag{21}$$
$$= 4\frac{\overline{n}}{K}E\varepsilon^4 + O_p\left(\frac{1}{K}\right).$$

Among them, $\overline{n} = 1/K\sum_{k=1}^{K} n_k = N - K + 1/K$.

From the estimator of the variance of the first noise series and 11, we have a revised estimator of volatility as follows:

$$\mathrm{RV}^{(adt)} = \mathrm{aRV}^{(avg)} - b\frac{\overline{n}}{N}\mathrm{RV}. \tag{22}$$

According to 7 and 12, there are:

$$E\left(\mathrm{RV}^{(\mathrm{at})}|X\right) = \mathrm{aE}\left(\mathrm{RV}^{\left(\mathrm{aq}_g\right)}|X\right) - b\frac{\overline{n}}{N}E(\mathrm{RV}|X)$$
$$= a\left(\mathrm{RV}_X^{(\mathrm{avg})} + 2\overline{n}E\varepsilon^2\right) - b\frac{\overline{n}}{N}\left(\mathrm{RV}_X + 2\mathrm{NE}\,\varepsilon^2\right)$$
$$= \mathrm{aRV}_X^{(\mathrm{ang})} - b\frac{\overline{n}}{N}\mathrm{RV}_X + 2(a-b)\overline{n}E\varepsilon^2. \tag{23}$$

In order to completely eliminate the effect of $E\varepsilon^2$, we reasonably take a = b, which is an unbiased estimate of volatility, so that we can get another estimator of $E\varepsilon^2$, as follows:

$$\widehat{E}\varepsilon^2_{(\mathrm{adj})} = \frac{1}{2}(N - \overline{n})^{-1}\left(\mathrm{RV} - \mathrm{RV}^{(\mathrm{arg})}\right). \tag{24}$$

Furthermore, it satisfies $E(\widehat{E}\varepsilon^2_{(\mathrm{adj})}|X) = E\varepsilon^2 + 1/2(N - \overline{n})^{-1}(\sqrt{\mathrm{RV}}_X - \mathrm{RV}_X^{(\mathrm{arg})})$., and it is higher-order unbiased.

For a certain real data process X, we assume that $N^{1/2}(\widehat{E}\varepsilon^2_{(\mathrm{adj})} - E\varepsilon^2)$. and $N^{1/2}(\widehat{E}\varepsilon^2 - E\varepsilon^2)$ have the same asymptotic distribution when $\max_i \Delta_{t_1} \longrightarrow 0\,(i = 1, 2, \ldots, N)$ and $N \longrightarrow \infty, N/K \longrightarrow \infty$.

When $K = O(N^{2/3})$, there are:

$$\widehat{E}\varepsilon^2_{(\mathrm{adj})} - E\varepsilon^2 = \left(\widehat{E}\varepsilon^2 - E\varepsilon^2\right)\left(1 + O\left(K^{-1}\right)\right) + O_p\left(KN^{-3/2}\right)$$
$$= \widehat{E}\varepsilon^2 - E\varepsilon^2 + O_p\left(N^{-1/2}K^{-1}\right) + O_p\left(\mathrm{KN}^{-3/2}\right)$$
$$= \widehat{E}\varepsilon^2 - E\varepsilon^2 + O_p\left(N^{-5/6}\right). \tag{25}$$

According to the previous definition, the noise sequence has a MA(A) structure. Therefore, under the condition, and the drift coefficient is not timed, $E(r_{i,N}r_{i+1,N}) = -E\varepsilon^2$, and the higher-order autocovariances are all 0. Thus, we have an estimator of $E\varepsilon^2$ as follows:

$$\widehat{E}\varepsilon^2_A = -\frac{1}{N-1}\sum_{i=1}^{N-1} r_{i,N}r_{i+1,N}. \tag{26}$$

We assume that Y_t and X_t satisfy 1 and 2, and it satisfies 4, X_t and ε_t are independent, we have:

$$\widehat{E}\varepsilon^2_A = -\frac{1}{N-1}\sum_{i=1}^{N-1} r_{i,N}r_{i+1,N} \xrightarrow{p} E\varepsilon^2,$$
$$N^{1/2}\left(\widehat{E}\varepsilon_1^2 - E\varepsilon^2\right) \xrightarrow{d} N\left(0, 5E\varepsilon^4\right). \tag{27}$$

The noise sequence ε_t is a covariance stationary process (weak stationary process) with mean 0, and its autocovariance function is defined as $\pi(s) = E(\varepsilon_t\varepsilon_{t+s})$.

For $s = 0, \pi(0) = E\varepsilon^2$ is the variance of the noise. Obviously, the noise sequence is a special case of it.

The estimator bias is bias$(\mathrm{RV}) = E(\mathrm{RV} - \mathrm{RV}_X)$..

In fact, the full estimator bias is $E(\mathrm{RV} - \mathrm{IV}^*) = E(\mathrm{RV} - \mathrm{RV}_X) + E(\mathrm{RV}_X - \mathrm{IV}^*)$, where the former term is due to noise and the latter term is due to computational discretization. Without loss of generality, we examine the above

definitions regarding the form of estimator bias arising from noise.

The correlation between noise and effective price is $\gamma_N^{(h)}$, and for $h = 0, \pm 1, \pm 2, \cdots$, we define $\gamma_N^{(h)} = E(r_{i,N} e_{i+h,N})$.

When $r_{i,N}^*$ and $e_{t,N}$ are independent, $\gamma_N^{(h)} = 0$, when $h = 0, \gamma_N^{(0)} = E(r_{i,N}^* e_{i,N})$.

We have:

$$\text{bias}(\text{RV}) = 2N\gamma_N^{(0)} + 2N(\pi(0) - \pi(\Delta_N)). \tag{28}$$

Among them, $\Delta_N = T/N$.

We assume that $\pi(\cdot)$ is derivable at 0 and $\lim_{N\longrightarrow\infty} \gamma_N^{(0)}/\Delta_N = \gamma_N$,, when $N \longrightarrow \infty$ and $\Delta_N \longrightarrow 0$, we have:

$$\begin{aligned}\lim_{N\longrightarrow\infty} \text{bias}(\text{RV}) &= 2N\Delta_N \lim_{N\longrightarrow\infty} \gamma_N^{(0)}/\Delta_N \\ &\quad + 2N\Delta_N \lim_{N\longrightarrow\infty} (\pi(0) - \pi(\Delta_N))/\Delta_N \\ &= 2T(\gamma_N - \pi'(0)).\end{aligned} \tag{29}$$

The noise sequence satisfies the following conditions:

(1) For the finite number $\rho_0 \geq 0$, if $s > \rho_0$, then $\pi(s) = 0$;

(2) For finite numbers $\rho_0 \geq 0$ and $t_1 < t_2$ 3, if $s \notin [t_1 - \rho_0, t_2 + \rho_0]$, then $E(\varepsilon_t(X_{t_1} - X_{t_2})) = 0$;

(3) For $i \neq j, E(r_{i,N}^* r_{j,N}^*) = 0$.

We can see that the above conditions (1) and (2) say that the correlation of the noisy series process is limited to a period not exceeding ρ_0, and the condition (3) states that the effective price increments (over an arbitrarily long period) are uncorrelated. A method for RV estimation by introducing q_N-term autocorrelation is proposed.

When there exists an integer q_N such that $q_N/N > \rho_0$, we have:

$$\text{bias}\left(\text{RV}_{\text{AC},q_N}\right) = 0. \tag{30}$$

Among them, $\text{RV}_{\text{AC},q_N} = \sum_{i=1}^{N} r_{i,N}^2 + 2\sum_{h=1}^{q_N} N/N - h \sum_{i=1}^{N-h} r_{i,N} r_{i+h,N}$.

For w, N and q_N, the relational expression $q_N = \text{ceil}(w/\text{TN})$ should be satisfied. When the window parameter w is determined, N is given, and q_N can be defined. For N, it can be determined under the optimal sampling problem.

In fact, q_N is a typical choice: when $N \longrightarrow \infty$, $q_N/N \longrightarrow 0$, for example $q_N = \text{int}(4(N/100)^{2/9})$. However, we believe that correlation is specific to time period, it is independent of N, and it is inappropriate here.

Under the definition of estimation bias, there are:

$$\begin{aligned}\text{bias}\left(\text{RV}_{\text{NC},q_N}^{\widetilde{N}}\right) &= E\left(\text{RV}_{\text{NC},q_N}^{\widetilde{N}}\right) - E(\text{RV}_X) = 0 \\ \text{bias}\left(\text{RV}^{(N)}\right) &= E\left(\text{RV}^{(N)}\right) - E(\text{RV}_X) = 2N\gamma_N^{(0)} \\ &\quad + 2N(\pi(0) - \pi(\Delta_N)).\end{aligned} \tag{31}$$

Therefore, there is the following formula:

$$E\left(\text{RV}^{(N)}\right) - E\left(\text{RV}_{\text{AC},q_N}^{\widetilde{N}}\right) = 2N\gamma_N^{(0)} + 2N(\pi(0) - \pi(\Delta_N)). \tag{32}$$

Among them, N and $\widetilde{N}$ may be different or the same.

On the one hand, $\gamma_N^{(0)}$ represents the correlation between noise and effective price, and it remains unchanged over time. $\pi(\Delta_N)$ is the correlation of noise series in the time period, and the correlation between noise series is limited. If $\Delta_N > \rho_0$, then $\pi(\Delta_N) = 0$. Therefore, the appropriate frequency N_l is chosen such that $\Delta_N = T/N_l > \rho_0$, then $\pi(\Delta_{N_1}) = 0$. From formula (32), we have:

$$E\left(\text{RV}^{(N)}\right) - E\left(\text{RV}_{\text{AC},q_N}^{\widetilde{N}}\right) = 2N_l\left(\gamma_N^{(0)} + \pi(0)\right)\gamma_N^{(0)}. \tag{33}$$

On the other hand, when $N \longrightarrow \infty$, $\max \Delta_t \longrightarrow 0$ and thus $\pi(\Delta_N) \longrightarrow \pi(0)$. Therefore, we can choose the highest frequency N_h as possible, then by formula (32), we have:

$$E\left(\text{RV}^{(N_k)}\right) - E\left(\text{RV}_{\text{AC},q_R}^{\widetilde{N}}\right) \longrightarrow 2N_h\gamma_{N_k}^{(0)}. \tag{34}$$

From formula (33) and formula (34), the noise variance expression under the assumption of correlated series noise can be obtained, as follows:

$$\begin{aligned}\pi(0) &= \frac{E\left(\text{RV}^{(N_l)}\right) - E\left(\text{RV}_{\text{AC},q_N}^{\widetilde{N}}\right)}{2N_l} \\ &\quad - \lim_{N_h \longrightarrow \infty} \frac{E\left(\text{RV}^{(N_h)}\right) - E\left(\text{RV}_{\text{AC},q_N}^{\widetilde{N}}\right)}{2N_h}.\end{aligned} \tag{35}$$

Then, for a fairly large N_h and N_l and $\widetilde{N}$, the sample mean is used to replace the expected value, and the noise variance estimator under the assumption of correlated series noise can be obtained.

$$\widehat{\pi}(0) = \frac{\overline{\text{RV}}^{(N_l)} - \overline{\text{RV}}_{\text{AC},q_N}^{(\overline{N})}}{2N_l} - \frac{\overline{\text{RV}}^{(N_k)} - \overline{\text{RV}}_{\text{AC},q_N}^{(\overline{N})}}{2N_h}. \tag{36}$$

Among them, n represents the number of working days. For the frequency selection of N_h, N_l and $\widetilde{N}$, N_h is easy to determine, using the highest frequency available. N_l is the frequency at which noise correlation is removed. As long as N_l is taken to make $\Delta_{N_1} > \rho_0$, the influence of the correlation between noises on sampling estimation can be eliminated.

Due to the existence of microscopic noise in the market, there is a certain degree of deviation between the high-frequency financial data we observed and collected and the underlying real data, and the time period [0, 1] is divided as follows:

$$0 = t_0 < t_1 < \cdots < t_n = 1. \tag{37}$$

The observed value of the log price at time t_i is:

$$Y_{t_i} = X_{t_i} + \varepsilon_{t_1}, t_t = \frac{i}{n}, \quad i = 0, 1, \ldots, n.t \in [0, 1]. \tag{38}$$

Among them, ε_{t_t} is the microstructure noise, which satisfies $E\varepsilon_{t_1} = E\varepsilon = 0, E\varepsilon_{t_t}^2 = E\varepsilon^2$, and ε and the logarithmic price X are independent of each other.

$\Delta Y_t = Y_{t_i} - Y_{t_{i-1}}, (i = 1, 2, \ldots, n)$ is the logarithmic rate of return of financial assets over time period $[t_{i-1}, t_t]$ based on observational data.

The real logarithmic price X_t exists in a semi-martingale form:

$$X_t = \int_0 \mu_s \mathrm{d}s + \int_0 \sigma_s \mathrm{d}W_s + \sum_{l=1}^{N(t)} L_l, \quad t \in [0, 1]. \tag{39}$$

The three parts on the right side of the formula are the drift, diffusion and jump parts of X, respectively. For the diffusion part, W_t is a standard Brownian motion and the diffusion coefficient σ_t^2 is called the point volatility. For the jump part, $N(t)$ represents the number of jumps up to time t, and S represents the height of the l-th jump.

The logarithmic price process in the form of formula (39) has quadratic variation as follows:

$$[X, X] = \int_b \sigma_s^2 \mathrm{d}s + \sum_{l=1}^{N(t)} L_l^2. \tag{40}$$

For two assets X_1, X_2, the observed value of the logarithmic price at time t_i is:

$$Y_{1t_i} = X_{1t_t} + \varepsilon_{1t_i}, Y_{2t_i} = X_{2t_i} + \varepsilon_{2t_i}, t_t = \frac{i}{n}, \quad i = 0, 1, \ldots, n. \tag{41}$$

Among them, ε_{k_i} is ii.d., satisfying $E\varepsilon_{k_i} = E\varepsilon_k = 0, E\varepsilon_{k_i}^{21} = E\varepsilon_k^2$, and ε_k and the corresponding logarithmic price X_k are independent of each other, $k = 1, 2$.

Its true logarithmic price $X_{11}`X_{21}$ also exists in semi-martingale form as formula (39), as follows:

$$\begin{aligned} X_{1t} &= \int_d \mu_{1s} \mathrm{d}s + \int_b \sigma_{1s} \mathrm{d}W_{1s} + \sum_{l=1}^{N_1(t)} L_{1l}, \quad t \in [0, 1], \\ X_{2t} &= \int_0 \mu_{2s} \mathrm{d}s + \int_d \sigma_{2s} \mathrm{d}W_{2s} + \sum_{i=1}^{N_2(t)} L_{2l}, \quad t \in [0, 1]. \end{aligned} \tag{42}$$

The corresponding logarithmic price process $X_1`X_2$ also has a quadratic covariance matrix as follows:

$$\begin{pmatrix} [X_1, X_1] & [X_1, X_2] \\ [X_2, X_1] & [X_2, X_2] \end{pmatrix} = \begin{pmatrix} \int_0^1 \sigma_{11s}^2 \mathrm{d}s & \int_0^1 \sigma_{12s}^2 \mathrm{d}s \\ \int_0^1 \sigma_{21s}^2 \mathrm{d}s & \int_0^1 \sigma_{22s}^2 \mathrm{d}s \end{pmatrix} + \begin{pmatrix} \sum_{l=1}^{N_1(t)} L_{1l}^2 & \sum_{l=1}^{N'(t)} L_{1l} L_{2l} \\ \sum_{l=1}^{N'(t)} L_{1l} L_{2l} & \sum_{l=1}^{N_2(t)} L_{2l}^2 \end{pmatrix}. \tag{43}$$

Among them, the set of corresponding jump points is denoted as $A_1`A_2$, $N'(t)$ represents the number of elements of $A_1 \cup A_2$. For the jump covariation matrix, we have:

$$\Gamma\Delta\begin{pmatrix} \xi_{11} & \xi_{12} \\ \xi_{21} & \xi_{22} \end{pmatrix} = \begin{pmatrix} \sum_{l=1}^{N_1(t)} L_{1l}^2 & \sum_{l=1}^{N'(t)} L_{ll} L_{2l} \\ \sum_{l=1}^{N'(t)} L_{1l} L_{2l} & \sum_{l=1}^{N_2(t)} L_{2l}^2 \end{pmatrix}. \tag{44}$$

Among them, the jump difference is $\xi_{\mathrm{kk}} = \sum_{l=1}^{N_k(t)} L_{\mathrm{kl}}{}^2$, $k = 1, 2$, and the jump covariance difference is $\xi_{12} = \xi_{21} = \sum_{l=1}^{N'(t)} L_{1l} L_{2l}$. For the volatility matrix, there are:

$$\theta = \begin{pmatrix} \theta_{11} & \theta_{12} \\ \theta_{21} & \theta_{22} \end{pmatrix} = \begin{pmatrix} \int_0 \sigma_{11s}^2 \mathrm{d}s & \int_0 \sigma_{12s}^2 \mathrm{d}s \\ \int_0 \sigma_{21s}^2 \mathrm{d}s & \int_0 \sigma_{22s}^2 \mathrm{d}s \end{pmatrix}. \tag{45}$$

Among them, $\int_0 \sigma_{12s}^2 \mathrm{d}s = \int_0 \sigma_{21s}^2 \mathrm{d}s$

The wavelet analysis method is a time-frequency localized analysis method with a fixed window size but its shape can be changed, and both the time window and the frequency window can be changed. That is, it has higher frequency resolution and lower time resolution in the low frequency part, and higher time resolution and lower frequency resolution in the high frequency part. Therefore, it is called a mathematical microscope. It not only inherits and develops the localization idea of short-time Fourier transform, but also has the characteristics of multi-resolution analysis. It uses multi-scale wavelet to analyze high-frequency data without sampling, there is no trouble of sampling, and it can also deal with mutation and noise problems at the same time. The wavelet transform is:

$$w_f(s, k) = \int_R f(x) g_{s,k}(x) dx. \tag{46}$$

Among them, there are:

$$g_{s,k}(x) = g\left(\frac{(x-k/s)}{\sqrt{s}}\right). \tag{47}$$

Among them, k is the time domain index, s is the scale. $K = 2^{-j}k, s = 2^{-j}$. If $g_{s,k}(x) = \varphi_{j,k}(x)$ or $g_{s,k}(x) = \psi_{j,k}(x)$, there are:

$$\varphi_{j,k} = 2^{j/2}\varphi\left(2^j x - k\right), \psi_{j,k} = 2^{J/2}\psi\left(2^j x - k\right). \tag{48}$$

Moreover, $\int_R \varphi_{j,k}(x) = 0, \int_R \psi_{j,k}(x) = 0, \varphi_{j,k}$ is called the parent wavelet, and $\psi_{j,k}$ is called the mother wavelet. For any function $f(x)$, we have:

$$f(x) = \sum_k^R c_k^{j_0}\varphi_{j_0,k}(x) + \sum_{j\geq j_0}\sum_k d_k^j\psi_{j,k}(x). \tag{49}$$

Among them, $c_k^{j_0}$ is the scale coefficient, d_k^j is the degree of detail coefficient. For the orthogonal wavelet family, there is $c_k^j = \int_R f(x)\varphi_{j,k}(x)\mathrm{d}x, d_k^j = \int_R f(x)\psi_{j,k}(x)\mathrm{d}x.$.

The estimates of the jump points τ_{1l}`$\tau_{2l}$ are $\widehat{\tau}_{1l}$`$\widehat{\tau}_{2l}$, and the number of elements $\widehat{N}_k(t)$ of $\{\widehat{\tau}_{kl}\}$ is recorded as the estimate of $N_k(t)$, k=1,2. Then, we use the estimated jump point to estimate the jump height of each jump, so that the jump variation $\widehat{\xi}_{11}$`$\widehat{\xi}_{22}$ and jump covariation difference $\widehat{\xi}_{12}$`$\widehat{\xi}_{21}$ can be estimated.

For $\delta_n > 0$, $\widehat{I}_{k+} = [\widehat{\tau}_{kl}, \widehat{\tau}_{kl} + \delta_n), \widehat{I}_{k-} = (\widehat{\tau}_{kl} - \delta_n, \widehat{\tau}_{kl}]k = 1, 2$, where m_{k+}, m_{k-} are the observation points of each asset in the interval $\widehat{I}_{k+}, \widehat{I}_{k-}$, k=1,2.

Therefore, the estimators of jump difference and jump covariation are:

$$\widehat{\xi}_{kt} = \sum_{l=1}^{\widehat{N}_k(t)}\widehat{L}_{kl}^{\ 2}, \quad k = 1, 2\,\widehat{\xi}_{12} = \widehat{\xi}_{21} = \sum_{l=1}^{\widehat{N}'(t)}\widehat{L}_{1l}\widehat{L}_{2l}. \tag{50}$$

Thus, the estimator of the second-order hop covariance matrix is obtained:

$$\widehat{\Gamma} = \begin{pmatrix}\widehat{\xi}_{11} & \widehat{\xi}_{12}\\ \widehat{\xi}_{21} & \widehat{\xi}_{22}\end{pmatrix}. \tag{51}$$

Now, we consider the convergence rate of the jump covariation difference matrix.

We first make the following assumptions.

(A_1) wavelet (φ, ψ) is differentiable in hop estimation.

$(A_2)\mu_{kt}, \sigma_{kt}^2$ is continuous almost everywhere with respect to t, and $E(\max_{0\leq s\leq 1}\mu_{kd}^2) < +\infty, E(\max_{0\leq s\leq 1}\sigma_{kt}^2) < +\infty, k = 1, 2$.

(A_3) is on the interval [0,1], $\widehat{q}_k = \widehat{N}_k(t)$.

$$\begin{aligned} q_k = N_k(t) < +\infty, \tau_{k1} < \tau_{k2} < \cdots < \tau_{\mathrm{kl}} \\ < \cdots, 0 < \left|L_{k|}\right| < +\infty, \quad k = 1, 2. \end{aligned} \tag{52}$$

$(A_4)(\mu_{\mathrm{kt}}, \sigma_{\mathrm{kt}}^2, W_{\mathrm{kt}})(N_k(t), L_{\mathrm{kl}})$ is independent of ε_{kt}, and $\varepsilon_{\mathrm{kt}}$ ii.$d.$, $E(\varepsilon_{\mathrm{kt}}^4) < +\infty, \quad k = 1, 2$.

The continuous part of $(A_5)X_k$ obeys the process, k=1,2.

We assume that $\delta_n \sim n^{-1/2}$, under the condition of $A_1 \sim A_4$, when $n \longrightarrow \infty$, there are:

$$\widehat{\Gamma} - \Gamma = O_p\left(n^{-1/4}\right). \tag{53}$$

To prove the theorem, we need the following two lemmas.

Under the condition of $A_1 \sim A_4$, we have:

$\lim_{n\longrightarrow\infty}P(\widehat{q}_k = q_k, \sum_{l=1}^{q_k}$
$|\widehat{\tau}_l - \tau_l| \leq n^{-1}\log^2 n|X) = 1, \quad k = 1, 2$ is established.

We assume that $\delta_n \sim n^{1/2}$, under the condition of $A_1 \sim A_4$, when $n \longrightarrow \infty$, we have:

$\Pi_k = \widehat{L}_{\mathrm{kd}} - L_{\mathrm{kl}} = O_p(n^{-1/4}), \quad k = 1, 2$ is established.

The proof is as follows:

(1) The elements on the off-diagonal line are first considered:

$$\widehat{\xi}_{12} - \xi_{12} = \sum_{l=1}^{\widehat{N}'(t)}\widehat{L}_{1l}\widehat{L}_{21} - \sum_{l=1}^{N'(t)}L_{1l}L_{2l}. \tag{54}$$

For $\forall d > 0$, $\widehat{N}'(t) = \widehat{q}, N\prime(t) = q$, $\lim_{n\longrightarrow\infty}P(\widehat{q} \neq q) = 0$, Therefore, there are:

$$\lim_{d\longrightarrow\infty}\lim_{n\longrightarrow\infty}P\left(\left|\widehat{\xi}_{12} - \xi_{12}\right| > \mathrm{d}n^{-1/4}\right) \leq \lim_{d\longrightarrow\infty}\lim_{n\longrightarrow\infty}P\left(\widehat{q} = q, \left|\widehat{\xi}_{12} - \xi_{12}\right| > \mathrm{d}n^{-1/4}\right). \tag{55}$$

When $\widehat{q} = q$, then there are:

$$\begin{aligned}\widehat{\xi}_{12} - \xi_{12} &= \sum_{l=1}^{q}\left(\widehat{L}_{1l}\widehat{L}_{2l} - L_{1l}L_{2l}\right)\\ &= \sum_{l=1}^{q}\left[\left(\widehat{L}_{1l} - L_{1l}\right)\widehat{L}_{2l} + \left(\widehat{L}_{2l} - L_{2l}\right)L_{1l}\right]\\ &= \sum_{l=1}^{q}\left(\Pi_1\widehat{L}_{2l} + \Pi_2 L_{1l}\right).\end{aligned} \tag{56}$$

Among them, there are:

$$\begin{aligned}\Pi_1 &= \widehat{L}_{1l} - L_{1l},\\ \Pi_2 &= \widehat{L}_{2l} - L_{2l},\\ \widehat{L}_{1l} - L_{1l} &= O_p\left(n^{-1/4}\right),\\ \widehat{L}_{2l} - L_{2l} &= O_P\left(n^{-1/4}\right),\end{aligned} \tag{57}$$

Moreover, because $\widehat{L}_{2l} = O_p(1), L_{1l} = O_p(1),$, so, there are:

$$\begin{aligned}\Pi_1\widehat{L}_{2l} &= O_p\left(n^{1/4}\right),\\ \Pi_2 L_{1l} &= O_p\left(n^{-1/4}\right),\end{aligned} \tag{58}$$

The proof is as follows:

$$\sum_{l=1}^{q}\left|\Pi_1\widehat{L}_{2l}\right| = O_p\left(n^{1/4}\right), \sum_{l=1}^{q}\left|\Pi_2 L_{1l}\right| = O_p\left(n^{1/4}\right)$$

$$P\left(\sum_{l=1}^{q}\left|\Pi_1\widehat{L}_{2l}\right| > d_1 n^{1/4}\right) \le P(N>m) + P\left(\sum_{l=1}^{m}\left|\Pi_1\widehat{L}_{2l}\right| > d_1 n^{1/4}, N \le m\right) \tag{59}$$

$$\le P(N>m) + P\left(\sum_{l=1}^{m}\left|\Pi_1\widehat{L}_{21}\right| > d_1 n^{1/4}\right) \le P(N>m) + \sum_{l=1}^{m} p\left(\left|\Pi_1\widehat{L}_{21} > \frac{d_1}{m} n^{-1/4}\right|\right),$$

m is fixed, and because the following formula exists:

$$\Pi_1\widehat{L}_{2l} = O_p\left(n^{-1/4}\right). \tag{60}$$

Therefore, there are:

$$\lim_{d_1 \longrightarrow \infty}\lim_{n\longrightarrow\infty} P\left(\sum_{l=1}^{q}\left|\Pi_1\widehat{L}_{2l}\right| > d_1 n^{-1/4}\right) \le P(N>m). \tag{61}$$

When $m \longrightarrow \infty$, there are:

$$\lim_{d_1 \longrightarrow \infty}\lim_{n\longrightarrow\infty} P\left(\sum_{l=1}^{q}\left|\Pi_1\widehat{L}_{2l}\right| > d_1 n^{-1/4}\right) \le \lim_{m\longrightarrow\infty} P(N>m) = 0, \tag{62}$$

Thus, there are:

$$\sum_{l=1}^{q}\left|\Pi_1\widehat{L}_{2l}\right| = O_p\left(n^{1/4}\right). \tag{63}$$

Similarly, it can be proved that $\sum_{l=1}^{q}|\Pi_2 L_{ll}| = O_p(n^{-1/4})$., as follows:

$$P\left(\widehat{q} = q, \left|\widehat{\xi}_{12} - \xi_{12}\right| > \mathrm{d}n^{-1/4}\right) \le P\left(\sum_{l=1}^{q}\left\{\left|\Pi_1\widehat{L}_{2l}\right| + \left|\Pi_2 L_{11}\right|\right\} > \mathrm{d}n^{-1/4}\right)$$

$$\le P\left(\sum_{l=1}^{q}\left|\Pi_1\widehat{L}_{2l}\right| > \mathrm{d}n^{-1/4}/2\right) + P\left(\sum_{l=1}^{q}\left|\Pi_2 L_{1l}\right| > \mathrm{d}n^{-1/4}/2\right) \longrightarrow 0. \tag{64}$$

Thus, there are:

$$\widehat{\xi}_{12} - \xi_{12} = O_p\left(n^{-1/4}\right). \tag{65}$$

(2) The elements on the diagonal are considered again

$$\widehat{\xi}_{\mathrm{kt}} - \xi_{\mathrm{kk}} = \sum_{l=1}^{\widehat{q}_k}\widehat{L}_{\mathrm{kl}}{}^2 - \sum_{l=1}^{q_k} L_{\mathrm{kl}}{}^2, \quad k = 1, 2, \tag{66}$$

For $\forall d > 0$, there are:

$$P\left(\left|\widehat{\xi}_{\mathrm{kk}} - \xi_{\mathrm{kk}}\right| > \mathrm{d}n^{1/4}\right) \le P\left(\widehat{q}_k = q_k, \left|\widehat{\xi}_{\mathrm{kk}} - \xi_{\mathrm{kk}}\right| > \mathrm{d}n^{-1/4}\right) + P\left(\widehat{q}_k \ne q_k\right),$$

$$\lim_{n\longrightarrow\infty} P\left(\widehat{q}_k \ne q_k\right) = 0, \tag{67}$$

Thus, there are:

$$\lim_{d\longrightarrow\infty n\longrightarrow\infty} P\left(\left|\widehat{\xi}_{\mathrm{kk}} - \xi_{\mathrm{kk}}\right| > \mathrm{d}n^{-1/4}\right) \le \lim_{d\longrightarrow\infty}\lim_{n\longrightarrow\infty} P\left(\widehat{q}_k = q_k, \left|\widehat{\xi}_{\mathrm{kk}} - \xi_{\mathrm{kk}}\right| > \mathrm{d}n^{1/4}\right). \tag{68}$$

When $\widehat{q}_k = q_k$, then there are:

$$\widehat{\xi}_{\mathrm{kk}} - \xi_{\mathrm{kk}} = \sum_{l=1}^{q_k}\left(\widehat{L}_{\mathrm{kl}}^2 - L_{\mathrm{kl}}^2\right) = \sum_{l=1}^{q_k}\left(\Pi_{kl}^2 + 2\Pi_k L_{kl}\right), \tag{69}$$

$$\Pi_k = O_p\left(n^{-1/4}\right).$$

At the same time, it is easy to know that $L_{kl} = O_P(1)$. Therefore, there is $\Pi_k L_{kl} = O_p(n^{1/4}), \Pi^2{}_k = O_p(n^{-1/2})$. The proof of formula 1 is easy to obtain:

$$\widehat{\xi}_{\mathrm{kk}} - \xi_{\mathrm{kk}} = O_P\left(n^{-1/4}\right), \quad k = 1, 2, \tag{70}$$

Combining 1 and 2, we can get:

$$\widehat{\Gamma} - \Gamma = O_p\left(n^{-1/4}\right). \tag{71}$$

We assume that in the estimation of the jump process, the wavelet method is used to obtain the estimators $\widehat{\tau}_{\mathrm{kd}}$ and $\widehat{L}_{\mathrm{kd}}$ of all jump points and jump heights of X_k, respectively. Therefore, the estimators of the jump parts of the counting process $N_k(t)$ and X_{kt} are respectively $\widehat{N}_k(t) = \sum_{l=1}^{\widehat{q}_k} I(\widehat{\tau}_{kl} \le t)$, $\widehat{X}^d_{\mathrm{kt}} = \sum_{l=1}^{\widehat{N}_k(t)} \widehat{L}_{\mathrm{kt}} = \sum_{\widehat{t}_{k_i} \le t} \widehat{L}_{\mathrm{kl}}$., where $I(\cdot)$ is an indicative function, k=1,2.

In order to eliminate the impact of the jumping process on the data, we can do the following: $Y^*_{\mathrm{kt}_1} = Y_{\mathrm{kk}_t} - \widehat{X}^d_{\mathrm{kt}_i} = Y_{k_t} - \sum_{t_t \le t_i} \widehat{L}_{\mathrm{kl}}, 4k = 1, 2$.

In the continuous diffusion price model, the best estimator of the integrated volatility θ is obtained by averaging the realized volatility under different optimal sampling data. However, under the jump-diffusion price model, if the estimates of jump points and jump heights are very accurate, the effect of the jump process on the average realized volatility will be asymptotically negligible. To prove it, some notations are now introduced. M is an integer, and the entire sample is sparse to obtain M sub-samples, which are defined as follows:

$$\begin{aligned}
\left[Y^*_k, Y^*_k\right]^{(M)} &= \frac{1}{M}\sum_{m=1}^{M}\sum_{j=1}^{n/M}\left(Y^*_{k_{m+\mu}} - Y^*_{k_{m+(-1)}}\right)^2 = \frac{1}{M}\sum_{i=1}^{n-M}\left(Y^*_{k_{i+\mu}} - Y^*_{k_i}\right)^2, k = 1, 2 \\
\left[Y^*_1, Y^*_2\right]^{(M)} &= \left[Y^*_2, Y^*_1\right]^{(M)} \\
&= \frac{1}{M}\sum_{m=1}^{M}\sum_{j=1}^{n/M}\left(Y^*_{1t_{m+\mu}} - Y^*_{1t^*_{m+(j-1)\mu}}\right)\left(Y^*_{2t_{m+\mu}} - Y^*_{2t^*_{m+((-1)\mu}}\right) = \frac{1}{M}\sum_{i=1}^{n-M}\left(Y^*_{1t_{i+\mu}} - Y^*_{1t_i}\right)\left(Y^*_{2t_{i+N}} - Y^*_{2t_i}\right).
\end{aligned} \tag{72}$$

Moreover, there is $\theta^* = \left(\begin{bmatrix} Y^*_1, Y^*_1 \\ Y^*_2, Y^*_1 \end{bmatrix}^{(M)} \begin{bmatrix} (M) \\ Y^*_1, Y^*_2 \\ Y^*_2, Y^*_2 \end{bmatrix}^{(M)}\right)$.

For comparison, denoting the X_k and Y_k continuous parts with X^c_k and Y^c_k, there are:

$$X^c_{kt} = \int_0 \mu_{\mathrm{ks}}\mathrm{d}s + \int_b \sigma_{\mathrm{ks}}\mathrm{d}W_{\mathrm{ks}}, Y^c_{\mathrm{kt}} = X^c_{\mathrm{ka}} + \varepsilon_{\mathrm{kt}}, \quad k = 1, 2. \tag{73}$$

The following formula is defined:

$$\begin{aligned}
\left[Y^c_k, Y^c_k\right]^{(M)} &= \frac{1}{M}\sum_{m=1}^{M}\sum_{j=1}^{n/M}\left(Y^c_{\mathrm{kk}_{m+M}} - Y^c_{k_{m+(-1)}}\right)^2 = \frac{1}{M}\sum_{i=1}^{n-M}\left(Y^c_{\mathrm{kk}_{i+\mu}} - Y^c_{k_1}\right)^2, \quad k = 1, 2, \\
\left[Y^c_1, Y^c_2\right]^{(M)} &= \left[Y^c_2, Y^c_1\right]^{(M)} \\
&= \frac{1}{M}\sum_{m=1}^{M}\sum_{j=1}^{n/M}\left(Y^c_{1t_{++M}} - Y^c_{1t_{t+1-1\mu}}\right)\left(Y^c_{2t_{++\mu}} - Y^c_{2t_{i+c}(-1)M}\right) = \frac{1}{M}\sum_{i=1}^{n-M}\left(Y^c_{1t_{i+\mu}} - Y^c_{1t_i}\right)\left(Y^c_{2t_{i+\mu}} - Y^c_{2t_i}\right).
\end{aligned} \tag{74}$$

Moreover, there is $\theta^c = \left(\begin{bmatrix} Y^c_1, Y^c_1 \\ Y^c_2, Y^c_1 \end{bmatrix}^{(M)} \begin{bmatrix} Y^c_1, Y^c_2 \\ Y^c_2, Y^c_2 \end{bmatrix}^{(M)}\right)$.

It is worth noting that Y^c_k is not directly observable, it is only used as a theoretical comparison of Y^*_k, k=1,2.

Now, we generalize the dual-scale realized volatility to the two-asset jump-diffusion price model to obtain an estimator of θ as follows:

$$\widehat{\theta}_M = \begin{pmatrix} \widehat{\theta}_{11M} & \widehat{\theta}_{12M} \\ \widehat{\theta}_{21M} & \widehat{\theta}_{22M} \end{pmatrix}. \tag{75}$$

Among them, there are:

$$\begin{aligned}
\widehat{\theta}_{kkM} &= \left[Y^*_k, Y^*_k\right]^{(M)} - \frac{1}{M}\left[Y^*_k, Y^*_k\right]^{(1)}, k = 1, 2; \\
\widehat{\theta}_{12M} &= \widehat{\theta}_{21M} = \left[Y^*_1, Y^*_2\right]^{(M)} - \frac{1}{M}\left[Y^*_1, Y^*_2\right]^{(1)},
\end{aligned} \tag{76}$$

We assume that $M/n + \log^2 n/M \longrightarrow 0$, under the condition of $A_1 \sim A_4$, $\theta^* - \theta^c = O_p(n^{-1/4} + M^{-1}\log^2 n)$ holds.

We assume that $M = O(n^{2/3})(c > 0)$, under the condition of $A_1 \sim A_5$, $\widehat{\theta}_M - \theta = O_p(n^{-1/6})$ is established.

Under the condition of $A_1 \sim A_4$, $\lim_{n\to\infty} P(\widehat{q}_k = q_k, \sum_{l=1}^{q_k} |\widehat{\tau}_{kt} - \tau_{kt}| \le n^{-1}\log^2 n | X) = 1$, $k = 1, 2$. holds.

$$E\left[\max\left|X_t^c\right|\right] \le 2\int_0^1 E\left(\mu_s^2\right)\mathrm{d}s + 8E\left[\left|\int_0^1 \sigma_s \mathrm{d}W_s\right|^2\right] = \int_0^1 E\left(2\mu_s^2 + 8\sigma_s^2\right)\mathrm{d}s. \tag{77}$$

We assume that $X_n = O_p(a_n), Y_n = O_p(b_n)$, and a_n, b_n are greater than 0, n is a positive integer, there is $X_n + Y_n = O_p(a_n + b_n)$.

The proof is as follows: The following formula holds, as follows:

$$\left|\frac{X_n + Y_n}{a_n + b_n}\right| = \left|\frac{X_n}{a_n + b_n} + \frac{Y_n}{a_n + b_n}\right| \le \left|\frac{X_n}{a_n + b_n}\right| + \left|\frac{Y_n}{a_n + b_n}\right| < \left|\frac{X_n}{a_n}\right| + \left|\frac{Y_n}{b_n}\right|. \tag{78}$$

It is also known that the following formula exists:

$$\lim_{A\longrightarrow\infty} P\left(\left|\frac{X_n + Y_n}{a_n + b_n}\right| \ge A\right) < \lim_{A\longrightarrow\infty} P\left(\left|\frac{X_n}{a_n}\right| + \left|\frac{Y_n}{b_n}\right| \ge A\right) \le \lim_{A\longrightarrow\infty} P\left(\left|\frac{X_n}{a_n}\right| \ge \frac{A}{2}\right) + \lim_{A\longrightarrow\infty} P\left(\left|\frac{Y_n}{b_n}\right| \ge \frac{A}{2}\right) = 0. \tag{79}$$

Thus, there are:

$$X_n + Y_n = O_p(a_n + b_n). \tag{80}$$

The proof is as follows:

We assume that X_k has $q_k = N_k$ hops in τ_{kl}, which are denoted as the hop part of X_k, as follows:

$$X_{kt}^d = \sum_{l=1}^{N_k(t)} L_{\mathrm{kl}} = \sum_{T_i\ A3/4t} L_{\mathrm{kl}}, \quad k = 1, 2, \tag{81}$$

Because there is the following formula:

$$Y_{k_1} = X_{k_1} + \varepsilon_{k_1} = X_{k_1}^c + X_{k_1}^d + \varepsilon_{k_1} = Y_{k_1}^c + X_{k_1}^d$$
$$Y_{k_i}^{\bullet} = Y_{k_1} - \widehat{X}_{k_1}^d = Y_{k_1}^c + X_{k_1}^d - \widehat{X}_{k_1}^d. \tag{82}$$

Thus, there are:

$$Y_{\mathrm{kk}_{t+M}}^* - Y_{\mathrm{kt}_1}^* = Y_{\mathrm{kl}_{1+M}}^c - Y_{kt_1}^c + \sum_{t_1<\tau_k\le t_{l+\mu}} L_{\mathrm{kd}} \quad - \sum_{t_i<i_{\mathrm{kl}}\le t_{i+M}} \widehat{L}_{\mathrm{kl}} \equiv Y_{\mathrm{kt}_{i+M}}^c - Y_{\mathrm{kt}_l}^c + \xi_{\mathrm{ki}}. \tag{83}$$

It is equivalent to:

$$\Omega_n = \left\{\min\left\{\tau_{kl} - \tau_{k(l-1)}, \quad l = 1, \ldots q_k\right\} > M/n\right\} \cap \left\{\widehat{\tau}_{\mathrm{kl}} - \tau_{\mathrm{kl}}\right| \le n^{-1}\log^2 n, \quad l = 1, \ldots q_k = \widehat{q}_k\right\}. \tag{84}$$

From the condition (A_3), it can be known that:

$$\lim_{n\longrightarrow\infty} P(\Omega_n) = 1. \tag{85}$$

Therefore, it is only necessary to prove that $\theta^* - \theta^c = O_p(n^{-1/4} + M^{-1}\log^2 n)$ holds in Ω_n.

It is worth noting that in Ω_n, X_{kt} has at most one jump in the interval $[t_i, t_{i+M}]$ of length M/n, and since $M/n(n^{-1}\log^2 n) = M/\log^2 n \longrightarrow \infty$, the distance between τ_{kl} and $\widehat{\tau}_{kl}$ is very small. Therefore, there are the following three cases (k=1,2):

(i) $t_t, t_{l+M} < \tau_{kl}, \widehat{\tau}_{kl}$ or $t_t, t_{t+M} > \tau_{kl}, \widehat{\tau}_{kl}, a_{.s}$ is established;

(ii) $t_i < \tau_{kl}, \widehat{\tau}_{kl} < t_{i+M}$, is established, at this time, $n(M/n - |\tau_{kl} - \widehat{\tau}_{k|}|) \le M$;

(iii) We might as well set $\tau_{kl} \le \widehat{\tau}_{kl}, t_l \in (\tau_{kl}, \widehat{\tau}_{kl})$ or $t_{l+k} \in (\tau_{kl}, \widehat{\tau}_{kl})$, is established;

At this time, $2n|\tau_{kl} - \widehat{\tau}_{kl}| \le 2\log^2 n$.

In the above three cases, $\xi_{kt} = 0; L_{kt} - \widehat{L}_{k|}; L_{k|}$ or $\widehat{L}_{k\,d}$ holds.

Correspondingly, there are:

$$\left(Y_{1_{t+\mu}^*}^* - Y_{1t_t}^*\right)\left(Y_{2t_{t+\mu}}^* - Y_{2t_i}^*\right) - \left(Y_{1t_{t+\alpha}}^c - Y_{1t_t}^c\right)\left(Y_{2t_{t+\alpha}}^c - Y_{2t_i}^c\right) = 0; O_p\left(\left|L_{1l} - \widehat{L}_{1l}\right|\right) + O_p\left(\left|L_{2l} - \widehat{L}_{2l}\right|\right)O_p\left(\left|L_{11}\right| + \left|\widehat{L}_{1l}\right|\right) + O_p\left(\left|L_{2l}\right| + \left|\widehat{L}_{2l}\right|\right)$$
$$\left(Y_{k_{t+\mu}}^* - Y_{k_t}^*\right)^2 - \left(Y_{k_{t+\mu}}^c - Y_{k_t}^c\right)^2 = 0; O_p\left(\left|L_k - \widehat{L}_{k|}\right|\right)O_p\left(\left|L_k\right| + \left|\widehat{L}_{k|}\right|\right). \tag{86}$$

(1) Off-diagonal elements are considered first:

$$\begin{aligned}&\left[Y_1^*, Y_2^*\right]^{(M)} - \left[Y_1^c, Y_2^c\right]^{(M)}\\&= \frac{1}{M}\sum_{i=1}^{n-M}\left[\left(Y^*_{i_t+\alpha} - Y^*_{1t_i}\right)\left(Y^*_{2t^*_{++\mu}} - Y^*_{2t_t}\right)\right.\\&\left.-\left(Y^c_{1t_{t+\mu}} - Y^c_{1t_i}\right)\left(Y^c_{2t_{++\mu}} - Y^c_{2t_i}\right)\right].\end{aligned} \tag{87}$$

From the above discussion, it can be seen that the following formula holds:

$$\left[Y_1^*, Y_2^*\right]^{(M)} - \left[Y_1^c, Y_2^c\right]^{(M)} = O_p\left(H_{n,M}\right), \tag{88}$$

Among them, there are:

$$\begin{aligned}H_{n,M} &= \sum_{l=1}^{q_1}\left|L_{\mathrm{ll}} - \widehat{L}_{1l}\right| + \sum_{l=1}^{q_2}\left|L_{2l} - \widehat{L}_{2l}\right|\\&+ 2M^{-1}\log^2 n\sum_{l=1}^{q_1}\left(\left|L_{1l}\right| + \left|\widehat{L}_{1l}\right|\right)\\&+ 2M^{-1}\log^2 n\sum_{l=1}^{q_2}\left(\left|L_{2l}\right| + \left|\widehat{L}_{2l}\right|\right).\end{aligned} \tag{89}$$

From the condition (A_3), it can be known that:

$$\begin{aligned}&\sum_{l=1}^{q_k}\left|L_{\mathrm{kd}} - \widehat{L}_{\mathrm{kl}}\right| = O_p\left(n^{-1/4}\right), \sum_{l=1}^{q_l}\left(\left|L_{\mathrm{kl}}\right| + \left|\widehat{L}_{\mathrm{kl}}\right|\right) = O_p(1),\\&H_{n,M} = O_p\left(n^{-1/4} + M^{-1}\log^2 n\right).\end{aligned} \tag{90}$$

Thus, there are:

$$\left[Y_1^*, Y_2^*\right]^{(M)} - \left[Y_1^c, Y_2^c\right]^{(M)} = O_p\left(n^{-1/4} + M^{-1}\log^2 n\right). \tag{91}$$

(2) The elements on the diagonal are now considered

$$\begin{aligned}&\left[Y_k^*, Y_k^*\right]^{(M)} - \left[Y_k^c, Y_k^c\right]^{(M)}\\&= \frac{1}{M}\sum_{i=1}^{n-M}\left[\left(Y_{k^*_{k+\alpha}} - Y^*_{k_i}\right)^2 - \left(Y^c_{k_{k+\mu}} - Y^c_{k_i}\right)^2\right], \quad k = 1, 2.\end{aligned} \tag{92}$$

Likewise, we get:

$$\left[Y_k^*, Y_k^{P_k^*}\right]^{(M)} - \left[Y_k^c, Y_k^c\right]^{(M)} = O_p\left(J_{n,M}\right). \tag{93}$$

Among them, there are:

$$J_{n,\mu} = \sum_{i=1}^{q_k}\left|L_{kl} - \widehat{L}_k\right| + 2M^{-1}\log^2 n\sum_{t=1}^{q_k}\left(\left|L_k\right| + \left|\widehat{L}_{kl}\right|\right), \tag{94}$$

Because there is the following formula:

$$\begin{aligned}\sum_{l=1}^{q_k}\left|L_{\mathrm{kl}} - \widehat{L}_{\mathrm{kl}}\right| &= O_p\left(n^{-1/4}\right),\\\sum_{l=1}^{q_k}\left(\left|L_{\mathrm{kl}}\right| + \left|\widehat{L}_{\mathrm{kl}}\right|\right) &= O_p(1),\end{aligned} \tag{95}$$

Therefore, there are:

$$J_{n,M} = O_p\left(n^{-1/4} + M^{-1}\log^2 n\right). \tag{96}$$

Thus, there are:

$$\left[Y_k^*, Y_k^*\right]^{(M)} - \left[Y_k^c, Y_k^c\right]^{(M)} = O_p\left(n^{1/4} + M^{-1}\log^2 n\right). \tag{97}$$

Combining formulas (1) and (2), we can get:

$$\theta^* - \theta^c = O_p\left(n^{-1/4} + M^{-1}\log^2 n\right). \tag{98}$$

The proof is as follows:

$\widehat{\theta}_M^c = \begin{pmatrix}\widehat{\theta}_{11M}^c & \widehat{\theta}_{12M}^c\\ \widehat{\theta}_{21M}^c & \widehat{\theta}_{22M}^c\end{pmatrix}$ is the two-scale realized volatility estimator of θ under the continuous diffusion price model.

Among them, there are:

$$\begin{aligned}\widehat{\theta}_{kkM}^c &= \left[Y_k^c, Y_k^c\right]^{(M)} - \frac{1}{M}\left[Y_k^c, Y_k^c\right]^{(1)}, k = 1, 2\\\widehat{\theta}_{12M}^c &= \widehat{\theta}_{21M}^c = \left[Y_1^c, Y_2^c\right](M) - \frac{1}{M}\left[Y_1^c, Y_2^c\right]^{(1)}\end{aligned} \tag{99}$$

$$\widehat{\theta}_M^c - \theta = O_p\left(n^{-1/6}\right).$$

Therefore, it is now only necessary to prove that $\widehat{\theta}_M - \widehat{\theta}_M^c = O_p(n^{-1/6})$.

(1) The elements on the off-diagonal line are considered first

$$\widehat{\theta}_{12M}^* - \widehat{\theta}_{12M}^c = \left[Y_1^*, Y_2^*\right]^{(M)} - \left[Y_1^c, Y_2^c\right]^{(M)} + \frac{1}{M}\left\{\left[Y_1^*, Y_2^*\right]^{(1)} - \left[Y_1^c, Y_2^c\right]^{(1)}\right\}. \tag{100}$$

When $M = O(n^{2/3})$, then there are:

$$[Y_1^*, Y_2^*]^{(M)} - [Y_1^c, Y_2^c]^{(M)} = O_p\left(n^{-1/6}\right), \tag{101}$$

The following evidence shows that when $M = O(n^{2/3})$, there are:

$$\begin{aligned}[Y_1^*, Y_2^*]^{(1)} - [Y_1^c, Y_2^c]^{(1)} &= O_p\left(n^{1/4}\log n\right)\\ Y^*_{k_{t+1}} - Y^*_{k_1} &= Y^c_{k_{t+1}} - Y^c_{k_1} + \sum_{t_1<\tau_{kl}\le t_{t+1}} L_{\mathrm{kl}} - \sum_{t_1<\widehat{\tau}_{kl}\le s_{l+1}} \widehat{L}_{\mathrm{kd}} \equiv Y^c_{k_{l+1}} - Y^c_{k_i} + \zeta_{\mathrm{ki}}, \quad i = 1, \ldots n-1.\end{aligned} \tag{102}$$

In these (n-1) intervals $[t_i, t_{i+1}]$, at least $n - 1 - (\widehat{q}_k + q_k)$ does not contain $\tau_{kl}, \widehat{\tau}_{kl}$, at this time, $\zeta_{ki} = 0$. There are at most $(q_k + \widehat{q}_k)$ non-zero ζ_{ki} s, and $\zeta_{\mathrm{kd}} = L_{\mathrm{kl}} - \widehat{L}_{\mathrm{kl}}$; L_{kl} or $\widehat{L}_{\mathrm{kl}}$ at this time.

Therefore, there are:

$$\begin{aligned}\left|[Y_1^*, Y_2^*]^{(1)} - [Y_1^c, Y_2^c]^{(1)}\right| \le{}& \sum_{l=1}^{1} L_{1l}^2 + \sum_{l=1}^{q_1} \widehat{L}_{1l}^2 + \sum_{l=1}^{q_2} L_{2l}^2 + \sum_{l=1}^{\widehat{q}_2} \widehat{L}_{2l}^2 + 2\max_{1\le i\le n}\left|Y^c_{2t_l}\right|\left\{\sum_{l=1}^{q_l}|L_{1l}| + \sum_{l=1}^{\widehat{q}_l}|\widehat{L}_{1l}|\right\}\\ &+ 2\max_{1\le i\le n}\left|Y^c_{1t_l}\right|\left\{\sum_{l=1}^{q_2}|L_{2l}| + \sum_{l=1}^{\widehat{q}_2}|\widehat{L}_{2l}|\right\}.\end{aligned} \tag{103}$$

First, there is the following formula:

$$\begin{aligned}\sum_{l=1}^{q_k}|L_{kk}| = O_p(1), \sum_{l=1}^{q_k}|\widehat{L}_{\mathrm{kl}}| = O_p(1), \sum_{l=1}^{q_k} L_{\mathrm{kl}}^2 &= O_p(1), \sum_{l=1}^{q_k}\widehat{L}_{\mathrm{kl}}^2 = O_p(1).\end{aligned} \tag{104}$$

Second, there is the following formula:

$$\begin{aligned}\max_{1\le\le\le\le n}\left|Y^c_{k_i}\right| &\le \max_{1\le i\le 1\le n}\left\{X^c_{k_i}|+|\varepsilon_{k_i}|\right\}\\ &\le \max_{1\le\le\le\le n}\left|X^c_{ki}\right| + \max_{1\le\le\le n}\left|\varepsilon_{k_i}\right|.\end{aligned} \tag{105}$$

From the condition (A_2), it can be deduced that:

$$\max_{1\le\le\le 1}\left|X^c_{kt}\right| = O_p(1). \tag{106}$$

In addition, there is the following formula:

$$\begin{aligned}P\left(\max_{1\le i\le n}\left|\varepsilon_{k_1}\right| > \varepsilon^{1/4}\log n\right) &= 1 - \left[1 - P\left(\left|\varepsilon_{k_1}\right| > g^{1/4}\log n\right)\right]^n\\ &\le 1 - \left[1 - \frac{E\left(\varepsilon^2_{kk_1}\right)}{\varepsilon^2 n^{1/2}\log^2 n}\right]^n \longrightarrow 0\,(n \longrightarrow \infty).\end{aligned} \tag{107}$$

Therefore, there are:

$$\max_{1\le 1\le n}\left|\varepsilon_{k_i}\right| = O_p\left(n^{1/4}\log n\right). \tag{108}$$

$$[Y_1^*, Y_2^*]^{(1)} - [Y_1^c, Y_2^c]^{(1)} = O_p\left(n^{1/4}\log n\right). \tag{109}$$

When the above formula is established, there are:

In addition, there are:

$$\begin{aligned}M = O\left(n^{2/3}\right)O\left(n^{2/3}\right)\hat{\mathrm{E}}\pm,\ \frac{1}{\mathrm{M}}\left\{\mathrm{Y}_1^*, \mathrm{Y}_2^*\right]^{(1)} - \left[\mathrm{Y}_1^c, \mathrm{Y}_2^c\right]^{(1)}\right\} &= O_p\left(n^{-Y_6}\right)\\ \widehat{\theta}^*_{12M} - \widehat{\theta}^c_{12M} = [Y_1^*, Y_2^*]^{(M)} - [Y_1^c, Y_2^c]^{(M)} + \frac{1}{M}\left\{[Y_1^*, Y_2^*]^{(1)} - [Y_1^c, Y_2^c]^{(1)}\right\} &= O_p\left(n^{-1/6}\right).\end{aligned} \tag{110}$$

(2) The elements on the diagonal are now considered

$$\widehat{\theta}^{*}_{kkM} - \widehat{\theta}^{c}_{kcM} = \left[Y^{*}_{k}, Y^{*}_{k}\right]^{(M)} - \left[Y^{c}_{k}, Y^{c}_{k}\right]^{(M)} + \frac{1}{M}\left\{\left[Y^{*}_{k}, Y^{*}_{k}\right]^{(1)} - \left[Y^{c}_{k}, Y^{c}_{k}\right]^{(1)}\right\}. \tag{111}$$

Similarly, it can be obtained that when $M = O(n^{2/3})$, there are:

$$\begin{aligned} &\left[Y^{*}_{k}, Y^{*}_{k}\right]^{(M)} - \left[Y^{c}_{k}, Y^{c}_{k}\right]^{(M)} = O_p\left(n^{-1/6}\right); \\ &\left|\left[Y^{*}_{k}, Y^{*}_{k}\right]^{\eta_i)} - \left[Y^{c}_{k}, Y^{c}_{k}\right]^{(1)}\right| \le 2\sum_{l=1}^{q_k} L^{2}_{kl} + 2\sum_{l=1}^{q_k} \widehat{L}^{2}_{\mathrm{kl}} + 4\max_{1\le\le\le n}\left|Y^{c}_{k_i}\right|\left\{\sum_{k=1}^{q_k}\left|L_k\right| + \sum_{i=1}^{q_k}\left|\widehat{L}_{\mathrm{kl}}\right|\right\}. \end{aligned} \tag{112}$$

Therefore, there are:

$$\frac{1}{M}\left\{\left[Y^{*}_{k}, Y^{*}_{k}\right]^{(1)} - \left[Y^{c}_{k}, Y^{c}_{k}\right]^{(1)}\right\} = O_p\left(n^{-1/6}\right). \tag{113}$$

Thus, there are:

$$\widehat{\theta}^{*}_{\mathrm{kkM}} - \widehat{\theta}^{c}_{\mathrm{kkM}} = \left[Y^{*}_{k}, Y^{*}_{k}\right]^{(M)} - \left[Y^{c}_{k}, Y^{c}_{k}\right]^{(M)} + \frac{1}{M}\left\{\left[Y^{*}_{k}, Y^{*}_{k}\right]^{(1)} - \left[Y^{c}_{k}, Y^{c}_{k}\right]^{(1)}\right\} = O_p\left(n^{-1/6}\right). \tag{114}$$

Combining 1 and 2, we can get $\widehat{\theta}_M - \widehat{\theta}^{c}_{M} = O_p(n^{-1/6})$, that is, $\widehat{\theta}_M - \theta = O_p(n^{-1/6})$.

4. Economic fluctuation analysis based on high frequency time series

Changes in financial structure have enriched financial products. The pricing of financial products is different from that of ordinary commodities, and the pricing of financial products depends to a large extent on future expectations. Due to the complexity of the economic system, people cannot make accurate expectations. When people's expectations cannot be realized, it will lead to chaos or even collapse of the financial system. Moreover, when there is a problem in the financial system, it will have a profound impact on the real economy. The irrational expectations of investors will lead to violent fluctuations in the prices of financial assets, and the violent fluctuations in the prices of financial assets will be accompanied by a sudden change in the flow of a large number of funds, which will destroy the stable value relationship of the economic system and affect the continuous production capacity of the real economy. bad influence. In addition, asset price movements are influenced by speculative activities, supply and demand, and political factors. Figure 1 shows the transmission diagram of the mechanism of financial structure changes affecting economic fluctuations.

According to the "income-consumption effect", as more investment brings more jobs, more and more people regain their jobs, and income increases and consumption increases with it. Consumption is the driving force and purpose of production. When companies predict an increase in spending power, they will further expand production. As production resumes and expands, companies hire more workers. In this cycle, the effective social demand increases from AD1 to AD2, the price level rises from P1 to P0, and the expected profit increases. At the same time, the actual output returns to the potential output level Y0, and the economic growth rate gradually returns to the potential economic growth rate, thus slowing down economic fluctuations, as shown in Figure 2.

When the economy is booming, actual output (Y1) is higher than potential output (Y0), and the labor market is in short supply. In addition to the influence of factors such as rising living costs, the price of labor factors continues to rise, and the price of capital is underestimated, so the price of labor relative to capital is higher. According to the "price effect", in order to reduce the unit product cost, the enterprise will increase the degree of technological progress biased towards labor and reduce the degree of bias towards capital, as shown in Figure 3.

The relationship between the fluctuation of technological progress factor bias and the economic fluctuation is shown in Figure 4. It can be seen from the figure that the two are negatively correlated.

With a moderate degree of financial leverage, financial innovation can help companies transfer financial risks, reduce transaction costs, and improve the liquidity of financial resources. This is conducive to improving the efficiency of resource allocation, thereby promoting economic

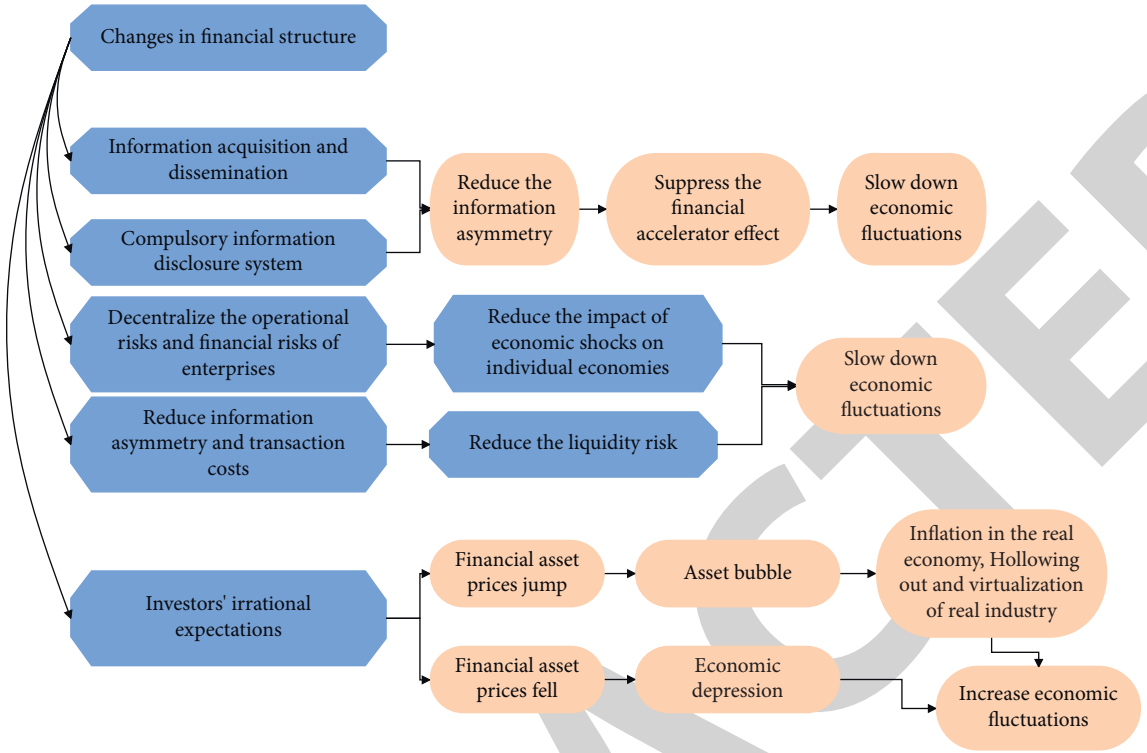


Figure 1: Transmission diagram of the mechanism of financial structure changes affecting economic fluctuations.

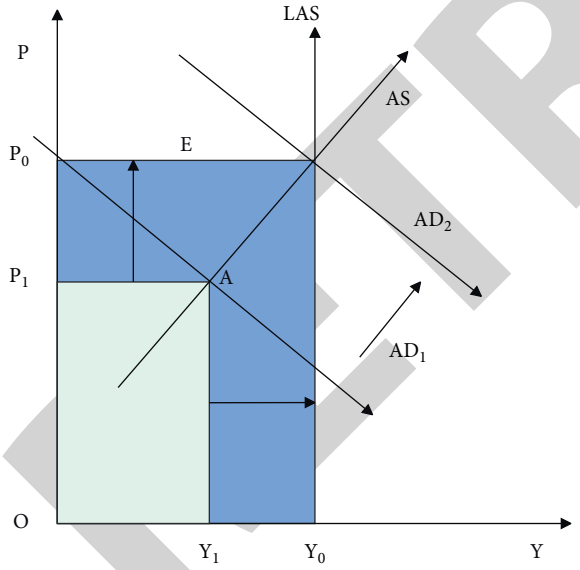


Figure 2: Biased capital during depression.

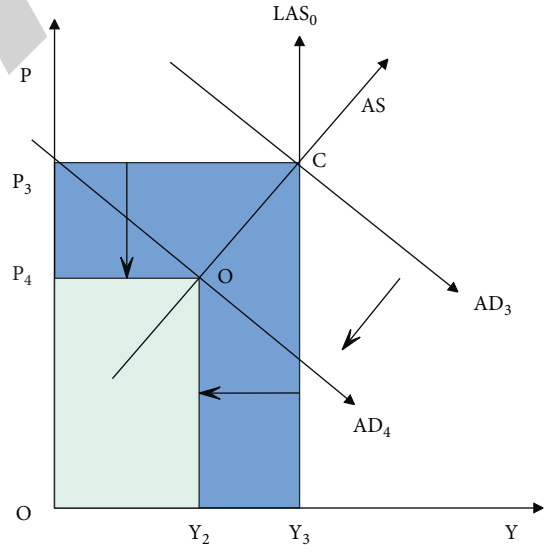


Figure 3: Biased labor in boom times.

development. Figure 5 shows the transmission mechanism model of financial leverage affecting economic fluctuations.

Figure 6 shows the RNN structure after unrolling in time series. From the perspective of time series expansion, each node in the figure from left to right represents the current layer of the recurrent neural network at each moment. From the perspective of the information processing structure of the network, the recurrent neural network can be roughly divided into three layers from top to bottom. The input layer represents the input state at the current moment, and it continues to progress as time unfolds. The hidden layer belongs to the memory structure, and the neurons in the hidden layer are also called memory units, which can store the information of the hidden layer at the previous moment. The output layer is the output state at the current moment. Figure 7 is the structure diagram of the LSTM deep network model.

The basic structure of the combined model is shown in Figure 8 below. First, it collects the original data of the

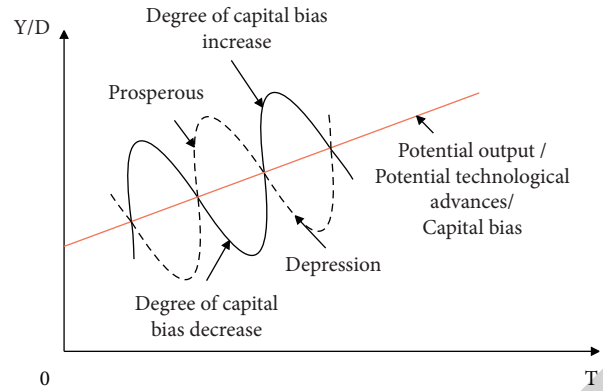


Figure 4: The relationship between the fluctuation of the degree of technological progress favoring capital and the fluctuation of the economy.

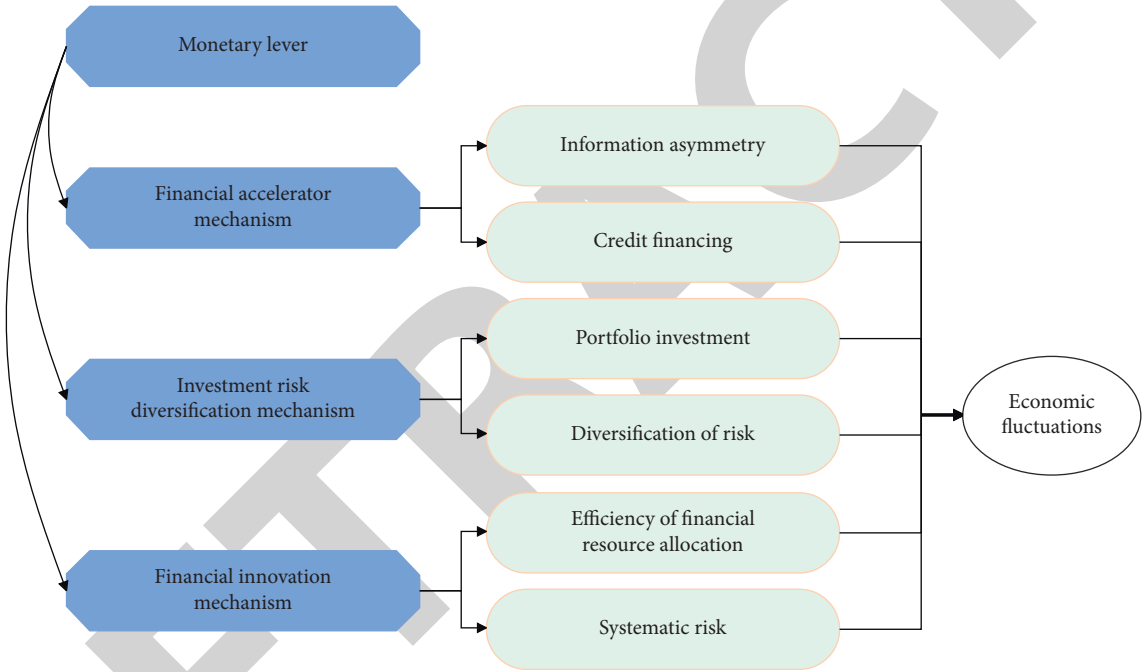


Figure 5: The transmission mechanism model of financial leverage affecting economic fluctuations.

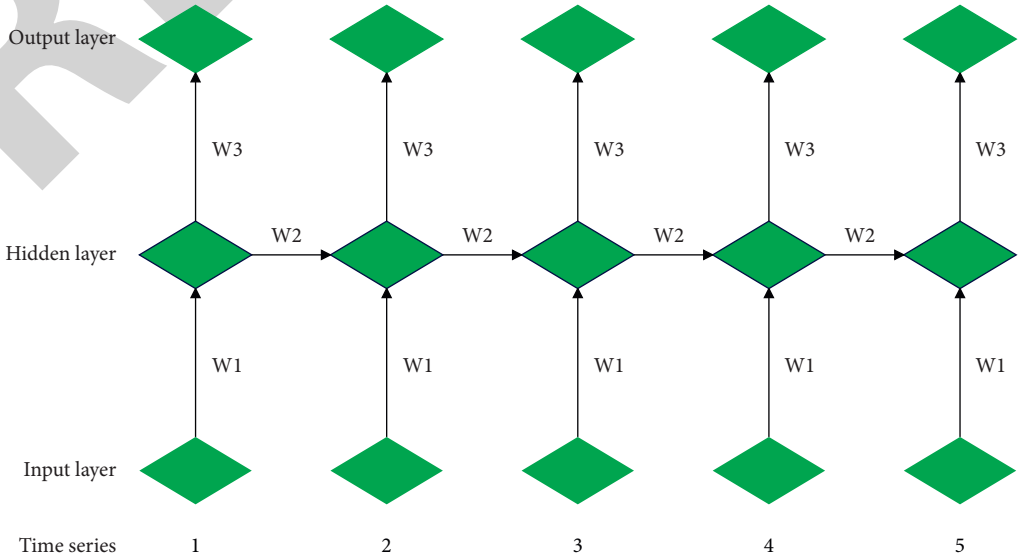


Figure 6: RNN network structure diagram after time series expansion.

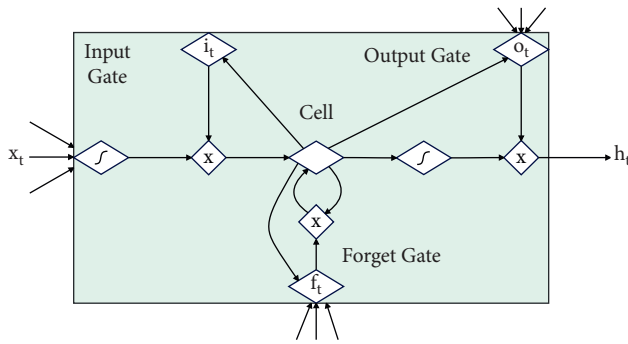


Figure 7: Structure diagram of the LSTM deep network model.

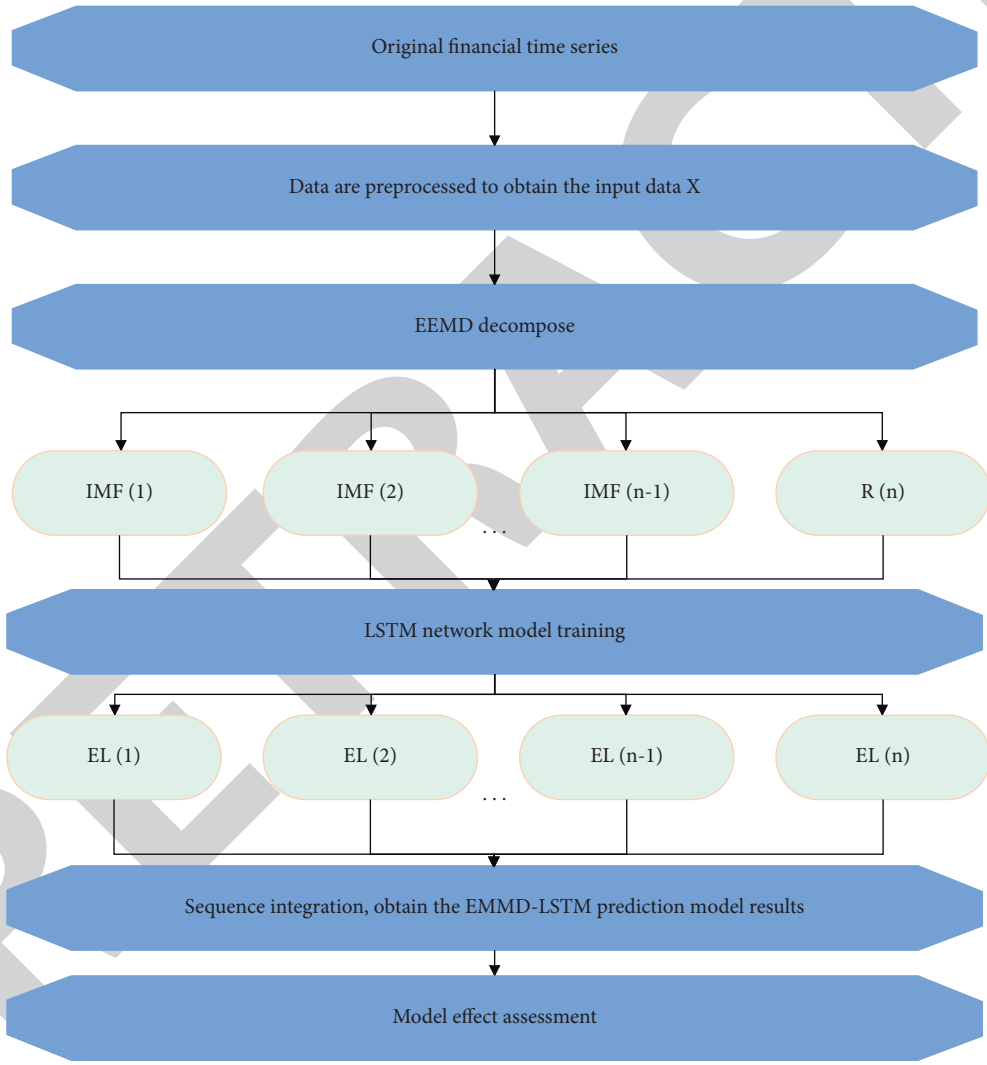


Figure 8: Flowchart of the EEMD-LSTM model.

financial practice sequence, preprocesses the input data, decomposes the preprocessed data through the EEMD algorithm, and decomposes it to obtain subsequences with different scale characteristics. After that, LSTM network is used to train and predict the decomposed sequences, and the final prediction result is obtained by comprehensive superposition. Finally, a comparative experiment is designed to evaluate the effect of the model.

On the basis of the above research, this paper combines Matlab to verify the effect of the model proposed in this paper, and the results shown in Table 1 and Table 2 are obtained.

From the above simulation data, it can be seen that the economic fluctuation analysis system based on high-frequency financial time series proposed in this paper has good economic analysis and economic forecasting effects.

Table 1: Economic analysis effect of economic fluctuation analysis system based on high-frequency financial time series.

Number	Economic Analysis	Number	Economic Analysis	Number	Economic Analysis
1	71.29	16	70.12	31	82.64
2	78.79	17	72.08	32	78.96
3	67.57	18	67.58	33	81.15
4	80.00	19	80.68	34	70.62
5	67.74	20	79.20	35	71.88
6	76.06	21	73.23	36	68.55
7	69.52	22	71.57	37	72.33
8	78.73	23	82.14	38	75.81
9	82.65	24	70.81	39	82.54
10	72.46	25	72.98	40	83.37
11	78.85	26	80.59	41	82.52
12	68.45	27	73.88	42	76.29
13	80.93	28	67.50	43	74.70
14	73.74	29	73.40	44	67.64
15	76.09	30	79.02	45	72.48

Table 2: Economic forecasting effect of economic fluctuation analysis system based on high-frequency financial time series.

Number	Economic forecast	Number	Economic forecast	Number	Economic forecast
1	70.85	16	66.89	31	62.88
2	70.09	17	63.28	32	65.51
3	75.32	18	70.19	33	73.46
4	70.07	19	76.13	34	69.29
5	75.58	20	65.14	35	76.39
6	72.69	21	78.53	36	69.17
7	70.37	22	73.26	37	75.00
8	77.31	23	66.43	38	77.01
9	67.36	24	70.95	39	65.81
10	74.14	25	65.89	40	61.83
11	66.97	26	73.50	41	76.37
12	80.26	27	64.69	42	63.72
13	64.69	28	68.96	43	74.47
14	71.89	29	69.74	44	78.03
15	77.05	30	73.99	45	70.94

5. Conclusion

In the field of financial economics, with the rapid development of science and technology, the collection and storage of high-frequency financial data has become easier and easier, which is of great significance for understanding market derivatives. Volatility provides important information to describe the dynamic evolution of market derivatives and their intrinsic properties, and is also an important basis for market derivatives pricing. Therefore, the description and prediction of the estimation model of volatility has always been an important subject in the field of financial statistics. This paper combines the high-frequency financial sequence algorithm to analyze the actual measurement of economic fluctuations, and builds an intelligent economic analysis and forecasting system. Moreover, this paper verifies the effect of the intelligent model proposed in this paper through simulation experiments. The simulation data shows that the economic fluctuation analysis system based on high-frequency financial time series proposed in this paper has good economic analysis and economic forecasting effects. [18–20]

Data Availability

The labeled dataset used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The author declare no competing interests.

Acknowledgments

This study is sponsored by Yellow River Conservancy Technical Institute.

References

[1] J. Pipek and S. Nagy, "An economic prediction of refinement coefficients in wavelet-based adaptive methods for electron structure calculations," *Journal of Computational Chemistry*, vol. 34, no. 6, pp. 460–465, 2013.

[2] S. Nagy and J. Pipek, "An economic prediction of the finer resolution level wavelet coefficients in electronic structure

Hindawi
Security and Communication Networks
Volume 2024, Article ID 9805652, 1 page
https://doi.org/10.1155/2024/9805652

Retraction

Retracted: Optimization of Substation Alarm Information Processing Based on BP Neural Network

Security and Communication Networks

Received 8 January 2024; Accepted 8 January 2024; Published 9 January 2024

This article has been retracted by Hindawi following an investigation undertaken by the publisher [1]. This investigation has uncovered evidence of one or more of the following indicators of systematic manipulation of the publication process:

(1) Discrepancies in scope

(2) Discrepancies in the description of the research reported

(3) Discrepancies between the availability of data and the research described

(4) Inappropriate citations

(5) Incoherent, meaningless and/or irrelevant content included in the article

(6) Manipulated or compromised peer review

The presence of these indicators undermines our confidence in the integrity of the article's content and we cannot, therefore, vouch for its reliability. Please note that this notice is intended solely to alert readers that the content of this article is unreliable. We have not investigated whether authors were aware of or involved in the systematic manipulation of the publication process.

Wiley and Hindawi regrets that the usual quality checks did not identify these issues before publication and have since put additional measures in place to safeguard research integrity.

We wish to credit our own Research Integrity and Research Publishing teams and anonymous and named external researchers and research integrity experts for contributing to this investigation.

The corresponding author, as the representative of all authors, has been given the opportunity to register their agreement or disagreement to this retraction. We have kept a record of any response received.

References

[1] T. Han, "Optimization of Substation Alarm Information Processing Based on BP Neural Network," *Security and Communication Networks*, vol. 2022, Article ID 6501238, 8 pages, 2022.

Hindawi
Security and Communication Networks
Volume 2022, Article ID 6501238, 8 pages
https://doi.org/10.1155/2022/6501238

Research Article

Optimization of Substation Alarm Information Processing Based on BP Neural Network

Tuanjun Han

Physics & Telecommunications Engineering Department, Shaanxi University of Technology, Hanzhong 723000, China

Correspondence should be addressed to Tuanjun Han; book03711@126.com

Received 8 March 2022; Revised 15 April 2022; Accepted 28 April 2022; Published 10 June 2022

Academic Editor: Zhiping Cai

When a fault occurs in the power grid, a large number of alarm messages will come out. In order to reduce the damage caused by power outages, the staff should find out the location and type of faults as soon as possible based on the alarm messages uploaded from the control center. However, we are currently facing problems in handling these alarm messages such as reliability of protection actions and circuit breaker tripping, correctness of received alarm messages, and the possibility of the existence of unreceived alarm messages. The fault tolerance of the BP neural network is studied in this paper, and the fault tolerance of the network corresponds to the size of the fuzzy zone formed by the test samples. The fault tolerance of the network is improved by eliminating the fuzzy zone, and a hierarchical causal rule reasoning network with a structure of four layers is established for each element in the station. An accessible path for the candidate cause of the fault is divided into two stages as follows: from the candidate cause to the protection operation and from the protection operation to the circuit breaker trip, which are assigned different credibility contribution rates. At the same time, the artificial bee colony algorithm is combined to identify the operation mode of the substation using its reasoning and judgment capacity and make the necessary corrections to get some output results of the neural network. The results of the examples suggest that the proposed evaluation method has a small workload of calculation and can identify the faulty components with high reliability and their causes, quickly and accurately.

1. Introduction

Upon the occurrence of a fault, the alarm window on the substation automation system that monitors the man-machine interface will generate a large amount of alarm information [1], which may be mixed with erroneous alarm information. As a result, the substation operators have to spend a long time reading and analyzing the information. In order to shorten the alarm processing time, the substation alarm information processing system is needed as a necessary high-level application [2, 3]. An artificial bee colony algorithm for fault diagnosis and recovery processing of substations is put forward in this paper. The system has integrated two knowledge expression modes of rules and processes. The fault area is identified using the method of searching for passive connected areas to confirm the power outage area, and the fault point is determined accordingly [1, 4]. The fault diagnosis is carried out based on the method of taking the intersection of the protection scopes, and the protection with the fault is diagnosed and recorded in the inference process and taken as an explanation for the cause of the fault. All these diagnoses and determination are conducted based on the premise that the alarm information is entirely correct. However, in the practical conditions on site, causes such as poor contact and device failure can result in omission and false issuance of the alarm information, which can affect the accuracy of the diagnosis. Hence, the alarm information processing system is required to have certain fault tolerance, and the redundant information is used to ensure the correct diagnosis results [5, 6]. In the fault diagnosis of substations based on the artificial neural network (ANN) proposed in this paper, the inherent fault tolerance of ANN itself is used. However, no special fault tolerance study is performed. At the same time, the influence of the substation operation mode on the network structure is not taken into consideration. Therefore, it cannot be applied

on site [7, 8]. The alarm processing issue is described as an unconstrained 0-1 integer programming problem, and the Tabu search algorithm is used to optimize the solution. However, when the Petri net is used for diagnosis, some changes cannot be triggered due to the operation failure of circuit breakers, which can affect the diagnosis effect to a certain extent. The genetic algorithm is used to optimize the solution. However, the calculation model is complicated, and the solution time is relatively long [9, 10]. If all the time sequence information is summarized to the dispatch center for centralized processing after the occurrence of a fault, the diagnosis model will be highly complicated and flooded with massive information, which is not conducive to timely and effective diagnosis and alarm processing. If a certain method can be adopted at the digital substation to deal with the alarms in the station in a timely manner before it is reported to the superior, it will play an essential role in ensuring the safe and stable operation of the system [11, 12].

Based on the existing studies, a substation alarm evaluation method based on the artificial bee colony algorithm optimized by the BP neural network algorithm is put forward in this paper. It is designed to identify the cause of the fault at the substation level from the alarm signal quickly. Based on the structure of the power grid, the substation, and the principles of protection, a causal rule network of four layers for each element is established. The fault source layer, the candidate cause layer, the protection operation layer, and the causality between operation layers of the circuit breaker are provided. For the possible candidate causes, the evaluation method of optimizing the BP neural network algorithm is used, which has a small workload of calculation and can obtain the faulty components and their causes with high reliability quickly and accurately upon the occurrence of a fault. The effectiveness of the proposed method is verified through the analysis of various faults in a practical substation.

2. Artificial Bee Colony Algorithm Model

In general, the alarm information of the substation includes protection operations, circuit breaker operations, self-inspections of the protection equipment (such as sampling faults, tripping failures, and protection calculation errors), communication failures, and so on. The protection operations and the circuit breaker operations herein are mainly used to establish the substation alarm evaluation based on the artificial bee colony algorithm, supplemented by the self-inspection of the protection equipment, communication failure, etc., to explain the cause of the alarm.

2.1. Modules of the Substation Alarm Information. The alarm information of the substation generally includes protection action, circuit breaker action, self-check of protection equipment (such as sampling fault, trip failure, and protection calculation error), communication fault, etc. Here, the artificial bee colony algorithm for substation alarm evaluation is constructed based on protection action and circuit breaker action, and the alarm reason is explained by self-check of protection equipment and communication fault.

The artificial bee colony algorithm model for the evaluation of substation alarm established in this paper involves the fault source F, the fault candidate cause C, the alarm event A, the inclusive relationship between the fault source and the fault candidate cause, the causal relationship between the fault candidate cause and the alarm event, the set of accessible paths for the candidate causes of the fault, the reliability of the failure source and the candidate cause, and other concepts.

The fault source F refers to the corresponding component F_i when the power grid fails, and it can specifically be divided into fault components such as the line L_i, the transformer T_i, and the busbar B_i.

The candidate cause for a fault refers to a set of possible candidate causes $C\,(=F_i) = \{c_1, c_2, \ldots, c_n\}$ when a component *Fi* fails. The source of the fault can contain multiple candidate causes that are independent of each other ("OR" relationship). The initiation probability of each candidate cause is $P_{FC}\,(F_i, c_j)$, which has certain differences.

An alarm event refers to an alarm generated by the operation of the each protection and circuit breaker due to a fault, where the protection outlet operation and circuit breaker operation x are taken into consideration.

2.2. Types of Causality Relationships in the Substation. There are two types of causality relationships in the substation, that is, the causality between the fault candidate cause C and the protection operation alarm a and the causality between the protection operation alarm a and the circuit breaker operation alarm x. One fault candidate cause c_i can trigger a number of alarm signs and form the alarm signs set $S_{CA}\,(=c_i) = \{a_1, a_2, \ldots, a_m\}$ and causality pairs $(c_i, a_1), \ldots, (c_i, a_m)$, which occur at the same time in general ("AND" relationship). For each causal relationship pair, the trigger probability of the alarm a_j induced by the candidate cause c_i is $P_{CA}\,(c_i, a_j)$. Due to the difference and priority of each candidate cause and to suppress false alarms to a certain extent, they are assigned different trigger probabilities. An alarm a_j may be triggered by a number of fault candidate causes. There is a causal relationship (a, x) between the protective outlet operation and the circuit breaker operation x that triggers the circuit breaker to trip, and its trigger probability is $P_{AX}\,(a, x)$. A protection operation a_j can have one or more corresponding trips of circuit breakers, and the circuit breaker trip set is $S_{AX}\,(=a_j) = \{x_1, x_2, \ldots, x_1\}$.

An accessible path of a fault candidate cause refers to a complete path composed of two subpaths due to two stages of the candidate cause c_i triggering a protection operation a_j and the protection operation triggering the trip of a specific circuit breaker x_k, $[(c_i, a_j), (a_j, x_k)]$ or $[(c_i, a_j), (a_j, x_k), \ldots, (a_j, x_l)]$.

The optimized BP neural network algorithm (CF) for the occurrence of the candidate cause of the fault refers to determining the actual degree of occurrence u_i ($u_i \in [0, 1]$) based on the alarm sign set of the candidate cause c_i. In a similar way, the credibility for the occurrence of a fault

source refers to that the degree of fidelity is determined based on the occurrence of the candidate cause set of the fault source. The operation probabilities of the protection a_j and the circuit breaker x_k are $P(a_j)$ and $P(x_k)$, respectively (if the operation is performed, it is set at 0.95; otherwise, it is set at 0.05). The cause for the lack of an alarm is its failure to operate or the failure of equipment communication.

The evaluation of the substation fault handling based on the artificial bee colony algorithm has four layers as follows: fault source (component), candidate cause, protection operation, and circuit breaker operation. An example of the alarm evaluation of a specific line in a substation based on the artificial bee colony algorithm is shown in Figure 1.

The marking of the protection operation a and the circuit breaker operation x stipulates that the main protection m, local backup protection $s1$, and remote backup protection $s2$ of the line (such as L_{211}) are marked as a^m_{L211}, a^{s1}_{L211}, and a^{s2}_{L211}, respectively. The main protection m of the transformer (such as T_1) and the backup protection Section 1 $s1$ and Section 2 $s2$ are marked as a^m_{L1}, a^{s1}_{L1}, and a^{s2}_{L1}, respectively. The main differential protection m of the busbar (such as B_1) is marked as a^m_{B1}, and the operation of the circuit breaker (such as 211) is marked as x_{211}.

There are six combinations of fault candidate causes of the line L_{211} on the 10 kV side: c_{211_1} (the line L_{211} failure, main protection operation, and the circuit breaker 211 normal operation), c_{211_2} (the line L_{211} failure, main protection failure, local backup protection operation, and the circuit breaker 211 normal operation), c_{211_3} (the line L_{211} failure, remote backup protection operation, and the circuit breaker 211 normal operation), c_{211_4} (the line L_{211} failure, main protection operation, and the circuit breaker 211 failure to operate), c_{211_5} (the line L_{211} failure, main protection failure to operate, local backup protection operation, and the circuit breaker 211 failure to operate), and c_{211_6} (the line L_{211} failure, remote backup protection operation, and the circuit breaker 211 failure to operate). There are three accessible subpaths for the candidate cause c_{211_4}: main protection operation and the circuit breaker 211 failure to operate; No. 1 main transformer backup overcurrent Section 1 protection operation and busbar tie section breaker 231 operation; No. 1 main transformer backup overcurrent stage II protection operation and the circuit breaker 201 operation. The initiation probability P_{CA} of each protection is 0.99, 0.96, and 0.93, respectively.

3. BP Neural Network Algorithm

3.1. The Advantages of Optimized BP Neural Network Algorithm. Based on the existing research, this paper proposes a substation alarm evaluation method based on the artificial bee colony algorithm and optimized BP neural network algorithm. The evaluation method using optimized BP neural network algorithm has small amount of calculation, and it can quickly and accurately obtain the fault components and their causes with high reliability when the fault occurs. The effectiveness of the proposed method is verified by the analysis of several practical substation fault examples.

When the power grid fails, the evaluation system at the station level receives a real-time report from each protection device and collects all the relevant alarms within a period of time. Based on the established artificial bee colony algorithm evaluation and its rules, the candidate causes for the fault are evaluated and the corresponding fault sources and causes are obtained. The optimized BP neural network algorithm evaluation method for the substation alarm is described as follows.

Step 1. Based on the collected protection operations and circuit breaker operation sets, the corresponding suspected candidate cause set C′ and its corresponding suspected fault source set F′ are identified by tracing back according to the causal relationship.

Step 2. For each suspected fault source, the credibility of all candidate causes is calculated. The calculation method is described as follows:

(1) For the failure candidate cause c_i, the credibility of all accessible paths is calculated. As mentioned earlier, an accessible path of the candidate causes is composed of two accessible subpaths of (c_i, a_j) and (a_j, x_k) in general (except for some individual cases). Based on the protection principle, a component failure will inevitably lead to a protection operation and the protection operation will trigger the trip of a circuit breaker. These two links are indispensable, and the link where the fault in the relay protection leads to the protection operation is more important. Hence, the two accessible subpaths are assigned different credibility contribution rates of P_{C1} and P_{C2} (0.54 and 0.46, respectively), instead of multiplying the credibility of each subpath. The credibility of the accessible path $= P_{C1}P(a_j)\,P_{CA}(c_i, a_j) + P_{C2}P(x_k)\,P_{AX}(a_j, x_k)$.

(2) For the failure candidate cause c_i, the credibility of all its accessible paths is integrated. If each accessible path is in an "AND" relationship (or a conditional "AND" relationship), the averaging method is used to obtain the original credibility of the candidate cause.

(3) The original credibility of each candidate cause for the fault source is multiplied by the trigger probability $P_{FC}(F_i, c_j)$ and is used as the credibility of the candidate cause.

Step 3. For a suspected fault source, the maximum value of the credibility of all candidate causes is selected. If it exceeds the preset evaluation threshold value (such as 0.55), it is considered that the component is faulty.

Step 4. Repeat Step 2 and Step 3 to process all suspected fault sources.

3.2. The Reason of Missing Alarm. The reliability of fault source occurrence is to determine the true degree of fault

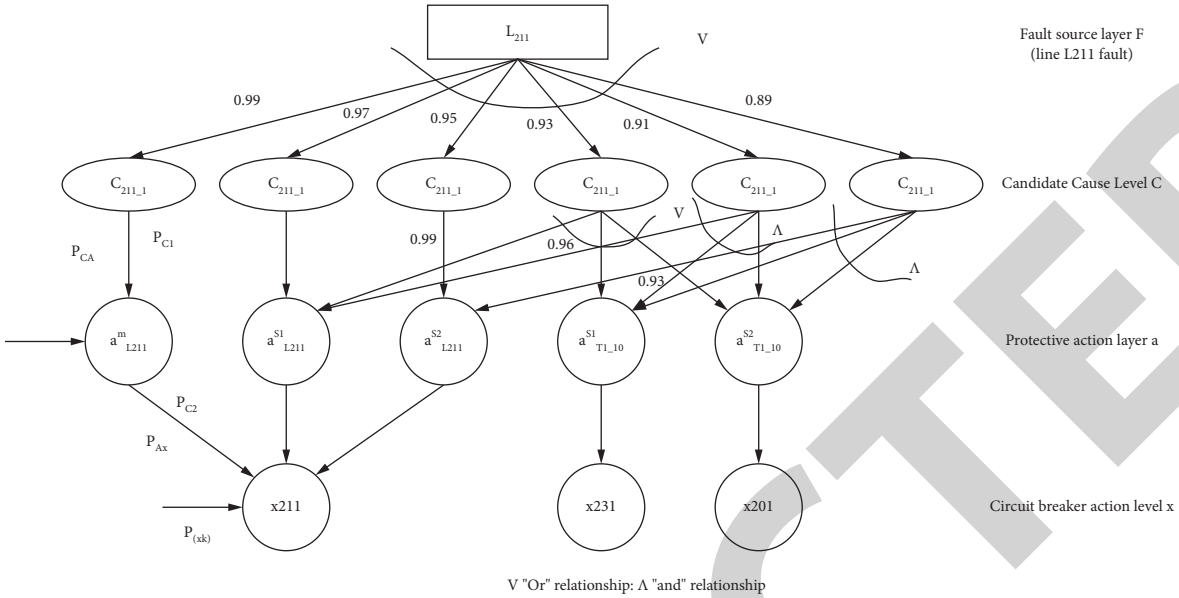


Figure 1: Example of the artificial bee colony algorithm for alarm evaluation of a specific line.

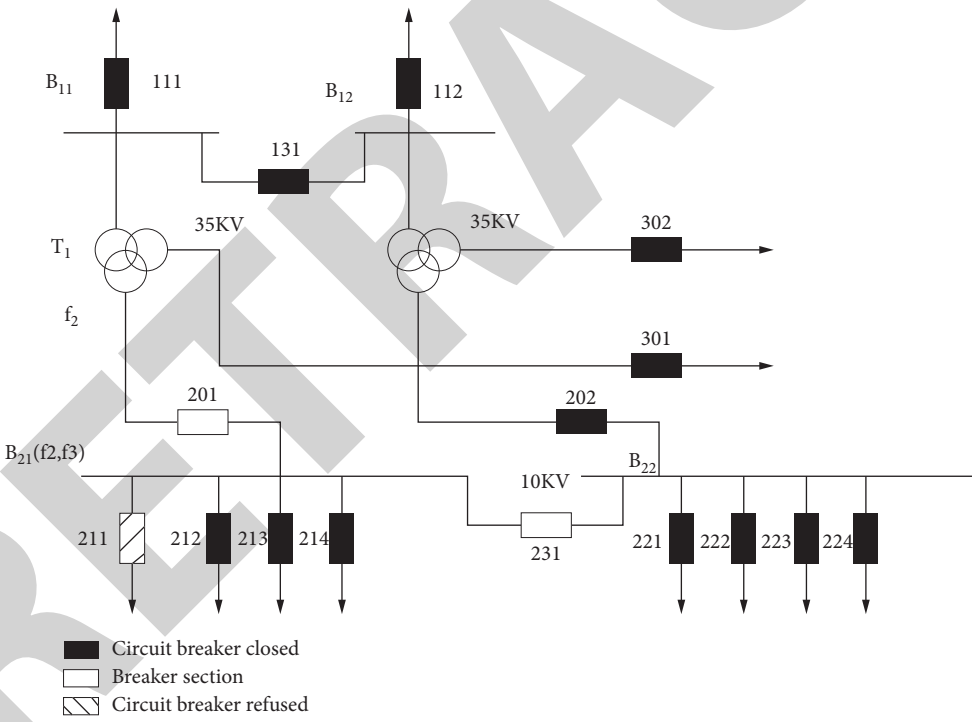


Figure 2: Main wiring structure of a substation.

source occurrence according to the occurrence of candidate cause set of the fault source. The action probabilities of protection *AJ* and circuit breaker *XK* are *p* (*AJ*) and *P* (*XK*), respectively (0.95 for protection *AJ* and 0.05 for circuit breaker *XK*). The reason of missing alarm is that it refuses to operate or its equipment communication fails.

4. Experimental Analysis and Results

4.1. Construction of the Practical Substation Alarm Evaluation Model. In this paper, a practical substation is taken as an example to establish an alarm evaluation model. The main wiring structure of the substation is shown in Figure 2.

The artificial bee colony algorithms for the evaluation of the lines on the left of 10 kV, the busbar B21, and the transformer *T*1 are shown in Figure 3 to 5. The initiation probabilities of each candidate cause for the busbar *B*21 are 0.99, 0.97, and 0.95, respectively; the initiation probability of each candidate cause for the transformer *T*1 is 0.99, 0.97, 0.95, and 0.93, respectively.

In Figure 4, the candidate cause c_{B21_1} of the busbar B_{21} suggests that the busbar B_{21} is faulty, the busbar differential

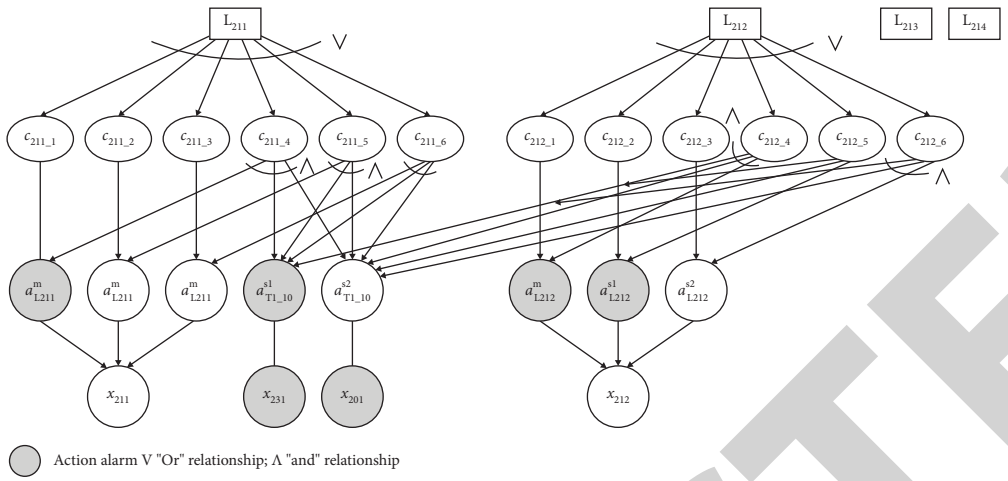


Figure 3: Alarm evaluation of each line on the left side of 10 kV based on the artificial bee colony algorithm (including fault scenario 1).

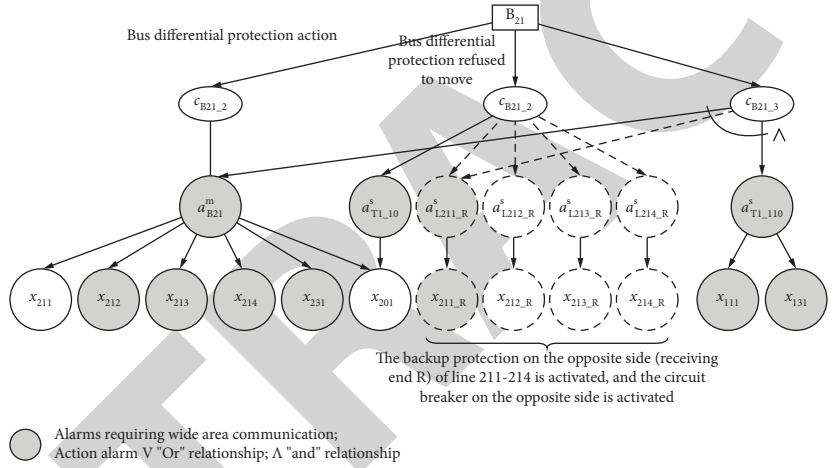


Figure 4: Alarm evaluation of the busbar $B21$ based on the artificial bee colony algorithm (including fault scenario 2).

protection is active, and the circuit breakers are normal. The c_{B21_2} indicates that the busbar B_{21} is faulty, the busbar differential protection fails, and the circuit breakers are normal, which are dependent on the 10 kV side backup protection operation of the transformer T_1 and the backup protection operation on the opposite side of lines 211~214 (receiving end R). Hence, it is necessary to obtain the protection operation and circuit breaker operation information on the opposite side of each line through wide-area communication. The c_{B21_3} indicates that the busbar B_{21} is faulty, the busbar differential protection operation is performed, the circuit breaker 201 fails to operate, and the circuit breaker 211 fails to operate (or the other circuit breakers with one or multiple feeders fail to operate), and its protection includes the busbar differential main protection, the 110 kV side backup protection of the transformer T_1, and the backup protection on the opposite side of the line 211. The 3rd protection corresponding to c_{B21_3} (the backup protection on the opposite side of the line 211 or the backup protection on the opposite side of the other lines 212 to 214) has certain conditions and restrictions to be involved in the evaluation: (1) the circuit breaker 211 is detected to fail to operate; (2) the backup protection operation and the circuit breaker operation information on the opposite side of the line can be obtained through the wide-area communication. Hence, the three protections corresponding to c_{B21_3} have a conditional "AND" relationship. Based on this conditional rule definition, the number of combinations of the circuit breaker 201 and circuit breaker failure to operate on each line can be reduced effectively, thereby reducing the number of candidate causes for the busbar B_{21}.

In Figure 5, the candidate cause c_{T1_3} of the transformer T_1 suggests that the transformer $T1$ fails, the main transformer differential protection operation is performed, the circuit breaker 201 fails to operate, and the circuit breaker 211 fails to operate (or the other circuit breakers with one or more feeders fail to operate). There is also a conditional "AND" relationship between the protection alarms. The case of c_{T1_4} is similar, which is not shown in the figure.

In the following section, the calculation process for the reliability of each of the six candidate causes when the line

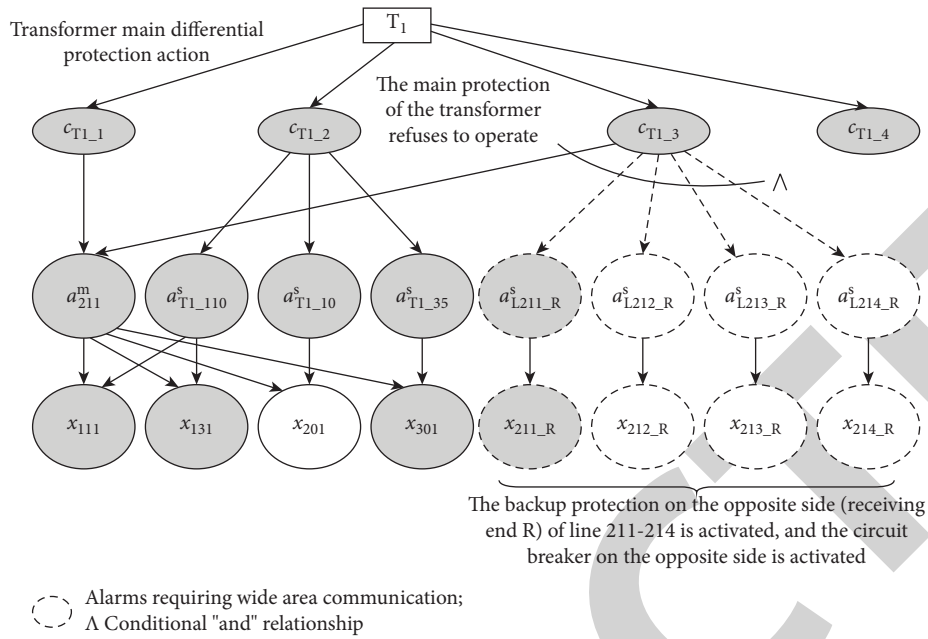


Figure 5: Alarm evaluation of the transformer T_1 based on the artificial bee colony algorithm (including fault scenario 2).

L_{21_1} fails is described. The accessible path of c_{211_1} is $[(c_{211\_1}, a^m_{L211}), (a^m_{L211}, x_{211})]$, and the accessible paths corresponding to the other candidate causes are shown in Figure 3.

u_{211_4} has 3 accessible subpaths, which are abbreviated as p_{41}, p_{42}, and p_{43}; then, the following can be obtained:

$$\begin{aligned} u_{41} &= 0.95 \times 0.99 \\ &= 0.9405\,(\text{onlythefirstsub} - \text{pathavailable}), \\ u_{42} &= 0.54 \times 0.95 \times 0.96 + 0.46 \\ &\quad \times 0.95 \times 0.99 = 0.9251, \\ u_{43} &= 0.54 \times 0.95 \times 0.93 + 0.46 \\ &\quad \times 0.95 \times 0.99 = 0.9097, \\ u_{211\_4} &= \frac{0.93\,(u_{41} + u_{42} + u_{43})}{3} = 0.8603, \end{aligned}$$

$$\text{similarly}, u_{211\_5} = 0.8418, u_{211\_6} = 0.8233. \tag{1}$$

4.2. Single Fault Accompanied by Protection and Circuit Breaker Failing to Operate and Lack of Information. In Figure 2, the 10 kV side line L_{211} has a failure (f_1) and the alarm is issued as follows: (1) the communication failure of the backup Section 2 protection equipment on the 10 kV side of the No. 1 main transformer is detected; (2) the line L211 main protection operation is received; (3) No. 1 main transformer back-up over-current protection is operated; (4) the breaker 231 trips; (5) the breaker 201 trips. The alarm assignment values based on the artificial bee colony algorithm are shown in Figure 3 above. The credibility of each candidate cause for the line L_{211} is calculated as follows:

$$\begin{aligned} u_{211\_1} &= (0.54 \times 0.95 \times 0.99 + 0.46 \times 0.05 \times 0.99) \times 0.99 = 0.5253, \\ u_{211\_2} &= (0.54 \times 0.05 \times 0.99 + 0.46 \times 0.05 \times 0.99) \times 0.97 = 0.0480, \\ u_{211\_3} &= (0.54 \times 0.05 \times 0.99 + 0.46 \times 0.05 \times 0.99) \times 0.95 = 0.0470, \\ u_{41} &= 0.9405, u42 = 0.9251, \\ u_{43} &= 0.54 \times 0.05 \times 0.93 + 0.46 \times 0.95 \times 0.99 = 0.4577, \\ u_{211\_4} &= \frac{0.93 \times (0.9405 + 0.9251 + 0.4577)}{3} = 0.7202, \\ u_{211\_5} &= 0.4345, u2116 = 0.4249. \end{aligned} \tag{2}$$

The six candidate causes for the line L_{211} are ranked according to their degrees of credibility. The credibility of the candidate cause c_{211_4} is the highest, which has exceeded the evaluation threshold value of 0.55.

Similarly, the credibility of each candidate cause for the line L_{212} is calculated as follows: $u_{212\_1} = 0.0490$, $u_{212\_2} = 0.0480$, $u_{212\_3} = 0.0470$, $u_{212\_4} = 0.4440$, $u_{212\_5} = 0.4345$, and $u_{212\_6} = 0.4249$, none of which exceeds the evaluation threshold value. The other lines are handled based on the similar method.

Finally, it is determined that the line L_{211} is faulty, the cause is c_{211_4}, and the result is correct. It can be observed that the line L_{211} backup protection a^{s1}_{L211} fails to operate, the circuit breaker x_{211} fails to operate, the 10 kV side backup protection $a^{s2}_{L2\_10}$ of the No. 1 main transformer operates correctly, and the circuit breaker 201 is tripped. However, it

is missing due to communication failure, and a total of 3 bits of information error are found. Nevertheless, the correct judgment is still made.

The main protection operation of the line in the candidate cause c_{211_1} is performed. Although circuit breaker 211 fails to operate, its credibility is 0.5253. It still has a certain degree of credibility, which is consistent with the protection principle. If the method of multiplying the credibility of each section in the subpath is used, the credibility may be extremely low, which suggests that it is relatively appropriate to assign different credibility contribution rates to the two stages of the path.

If the line L_{212} backup protection a^{s1}_{L212} malfunctions and the circuit breaker x_{212} does not operate at this point, then $u_{212\_5} = 0.7047$ and the line L_{212} fault will be misjudged. At this point, it is necessary to check whether the circuit breaker x_{212} has a tripping failure. If it does not fail, a false alarm of a^{s1}_{L212} is suspected. There are some problems with this evaluation when the protection is malfunctioning. When the reliability of the component is between 0.55 and 0.80, the evaluation situation needs to be analyzed more carefully and prudently.

4.3. Double Faults Accompanied by Two Circuit Breakers Failing to Operate. Transformer T_1 and busbar B_{21} fail at the same time (refer to f_2 and f_3 in Figure 2), and circuit breakers 201 and 211 fail to operate. The alarm sequence is as follows: (1) T_1 differential main protection operation is performed; (2) the circuit breaker 111 trips; (3) the circuit breaker 131 trips; (4) the circuit breaker 301 trips; (5) B_{21} main protection operation is performed; (6) the circuit breakers 212, 213, 214, and 231 trip in turn.

Firstly, the credibility of each candidate cause for the busbar $B21$ is calculated as follows:

$$u_{B21\_1} = \left[0.54 \times 0.95 \times 0.99 + 0.46 \times \frac{(0.95 \times 0.99 \times 4 + 0.05 \times 0.99 + 0.05 \times 0.99)}{6}\right] \times 0.99 = 0.7858. \quad (3)$$

For $c_{\mathrm{B21\_2}}$, if only the protection of $a^{s}_{T1\_10}$ is taken into consideration, then $u_{\mathrm{B21\_2}} = 0.5253$. If the backup protection and circuit breaker operation on the opposite side of the line L_{211} can be obtained, that is, $a^{s}_{T211\_R}$ is taken into consideration, then $u_{\mathrm{B21\_2}} = 0.7188$.

If only the subpaths $\mathrm{p_{B31}}$ and $\mathrm{p_{B32}}$ are taken into consideration, then $u_{\mathrm{B21\_3}} = (0.7937 + 0.9405)/2 \times 0.95 = 0.8237$.

If the backup protection and circuit breaker operation on the opposite side of the line L_{211} can be obtained, that is, the subpath $\mathrm{p_{B33}}$ is taken into consideration, then $u_{\mathrm{B3\_3}} = 0.54 \times 0.95 \times 0.99 + 0.46 \times 0.95 \times 0.99 = 0.9405$ and $u_{\mathrm{B21\_3}} = (0.7937 + 0.9405 + 0.9405)/3 \times 0.95 = 0.8470$.

The candidate cause cB213 has the highest credibility. Hence, it is determined that the busbar B_{21} is faulty, the cause is $c_{\mathrm{B21\_3}}$, and the result is correct.

The reliability of each candidate cause for the transformer T_1 is calculated as follows:

$$u_{T1\_1} = \left[0.54 \times 0.95 \times 0.99 + 0.46 \times \frac{(0.95 \times 0.99 \times 3 + 0.05 \times 0.99)}{4}\right] \times 0.99 = 0.8297. \quad (4)$$

$c_{\mathrm{T1\_2}}$ has 3 subpaths, and their credibility is as follows: $0.54 \times 0.95 \times 0.99 + 0.46 \times (0.95 \times 0.99 + 0.95 \times 0.99)/2 = 0.9405$; $0.54 \times 0.95 \times 0.99 + 0.46 \times 0.05 \times 0.99 = 0.5306$; $0.54 \times 0.95 \times 0.99 + 0.46 \times 0.95 \times 0.99 = 0.9405$.

$$u_{T1\_2} = \frac{(0.9405 + 0.5306 + 0.9405)}{3} \times 0.97 = 0.7798. \quad (5)$$

For c_{T1_3} and $u_{T1\_3} = 0.7962$, if the wide-area information such as the backup protection operation on the opposite side of line 211 after the circuit breaker 201 fails to operate and the circuit breaker tripping operation is taken into consideration, then $u_{T1\_3} = 0.8710$ and $u_{T1\_4} = 0.4389$.

If there is no wide-area communication available, the credibility of the candidate cause c_{T1_1} is the highest; otherwise, the credibility of c_{T1_3} is the highest. Based on both the candidate causes, it can be determined that the transformer T_1 fails and that the circuit breaker 201 fails to operate. Hence, the result is correct.

From the evaluation result of example 2, it can be seen that if the conditions for wide-area communication are available, the wide-area information on the opposite side of the line can be used to enhance the credibility in determination of the transformer and busbar faults.

5. Discussion

The alarm information processing system of the substation has relatively good fault tolerance with one input error, which can totally meet the online requirements. The established diagnosis model is not subjected to be affected by the influence of changes in the operation mode. In addition, before the information enters the diagnosis model, the artificial bee colony algorithm is used to identify the operation mode of the substation. In this way, when there is any change in the operating mode, it is not required to carry out restructuring and training, which have enhanced the

Hindawi
Security and Communication Networks
Volume 2024, Article ID 9816081, 1 page
https://doi.org/10.1155/2024/9816081

Retraction

Retracted: Engineering Management Model Analysis Using Partial Differential Equation Hilbert Space

Security and Communication Networks

Received 8 January 2024; Accepted 8 January 2024; Published 9 January 2024

This article has been retracted by Hindawi following an investigation undertaken by the publisher [1]. This investigation has uncovered evidence of one or more of the following indicators of systematic manipulation of the publication process:

(1) Discrepancies in scope
(2) Discrepancies in the description of the research reported
(3) Discrepancies between the availability of data and the research described
(4) Inappropriate citations
(5) Incoherent, meaningless and/or irrelevant content included in the article
(6) Manipulated or compromised peer review

The presence of these indicators undermines our confidence in the integrity of the article's content and we cannot, therefore, vouch for its reliability. Please note that this notice is intended solely to alert readers that the content of this article is unreliable. We have not investigated whether authors were aware of or involved in the systematic manipulation of the publication process.

In addition, our investigation has also shown that one or more of the following human-subject reporting requirements has not been met in this article: ethical approval by an Institutional Review Board (IRB) committee or equivalent, patient/participant consent to participate, and/or agreement to publish patient/participant details (where relevant).

Wiley and Hindawi regrets that the usual quality checks did not identify these issues before publication and have since put additional measures in place to safeguard research integrity.

We wish to credit our own Research Integrity and Research Publishing teams and anonymous and named external researchers and research integrity experts for contributing to this investigation.

The corresponding author, as the representative of all authors, has been given the opportunity to register their agreement or disagreement to this retraction. We have kept a record of any response received.

References

[1] C. Han, "Engineering Management Model Analysis Using Partial Differential Equation Hilbert Space," *Security and Communication Networks*, vol. 2022, Article ID 5853721, 8 pages, 2022.

Hindawi
Security and Communication Networks
Volume 2022, Article ID 5853721, 8 pages
https://doi.org/10.1155/2022/5853721

Research Article

Engineering Management Model Analysis Using Partial Differential Equation Hilbert Space

Chen Han

College of Physical Education, Chengdu University, Chengdu, Sichuan, 610106, China

Correspondence should be addressed to Chen Han; hanchen@cdu.edu.cn

Received 10 April 2022; Accepted 12 May 2022; Published 3 June 2022

Academic Editor: Fang Liu

In the process of the rapid development of science and technology, people study many problems with the help of the independent variables, but the according descriptions have not been accurate enough. Therefore, many problems must be described by a function of more than one variable to more accurately get the results that people need to use the functions containing more than one variable and their partial derivatives to study the real problems of the method. Partial differential equations are closely and directly related to many problems in physics, mechanics, and engineering. It becomes an important bridge between mathematical theory and practical problems in physics, mechanics, and engineering. And the elements in Hilbert space, vectors, can represent vectors, functions, and phase quantities, while the special solutions of partial differential equations in solving physical problems can satisfy the common properties of Hilbert space. The analogy of functions and phase quantities to vectors can establish the function space and phase quantity space with geometric intuition. Based on Hilbert space theory, the key and difficult problems in engineering management can be explained by clear mathematical models by using the analogy method. The purpose of this study is to enrich the means of the building engineering management model, to broaden the horizon of managers, and to solve the problems in engineering management from a new dimension.

1. Introduction

In mathematics, Hilbert space is a generalization of Euclidean space, which is no longer limited to the case of finite dimensions. Similar to Euclidean space, Hilbert space is also an inner product space, on which there are concepts of distance and angle (and the concepts of orthogonality and perpendicularity by extension). In addition, the Hilbert space is also a complete space, and all the Cauchy sequences on it are equivalent to the convergent sequences so that most of the concepts in calculus can be extended to the Hilbert space without hindrance. Hilbert spaces provide an efficient representation of Fourier series and Fourier transforms based on polynomial representations on any orthogonal system, and this is one of the core concepts of functional analysis. Hilbert spaces are one of the key concepts in formulaic mathematics and quantum mechanics. Engineering project management will be the project management object; engineering project management concept is different from other types of management; there are differences and similarities; in addition, the project has one-time characteristics, which puts forward higher requirements for project management methods, the need for a more scientific and comprehensive, and more regular management methods, as shown in Figure 1. Engineering project management from the formulation, project planning, project design, and implementation until the project is completed and put into use has been involved. Project management plays a very important role in the entire project engineering; engineering construction surface is large, involving a wide range of effects. It involves a consulting unit, construction units and design units, administrative departments, and construction units and material and equipment supply units; these units do not seem to interfere with each other, because the main projects do not connect closely, and due to the different forms of project management organization, so each unit in different stages are undertaking different tasks. Engineering project management, as a prerequisite to ensure the quality

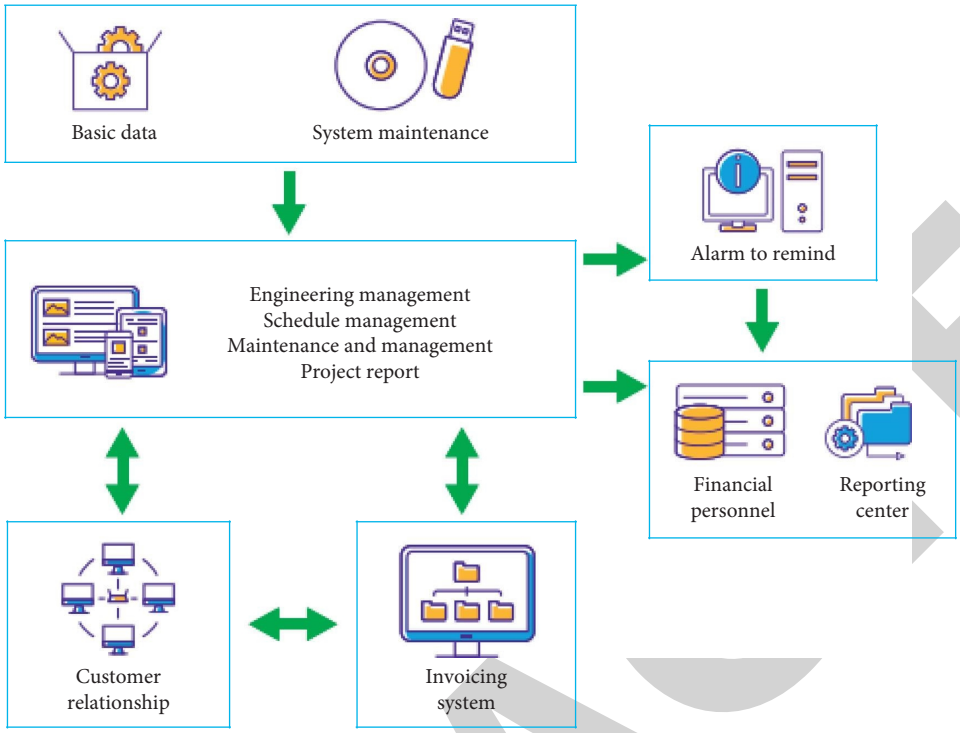


Figure 1: Conceptual diagram of Hilbert space.

and efficiency of the project, is related to the construction quality and construction efficiency of the whole project. Therefore, construction enterprises must change the traditional business model, strengthen enterprise management and technical innovation, actively explore new engineering project management mode, improve the overall level of enterprise project management, create more benefits, and lay a solid foundation for the long-term development of enterprises [1].

In engineering management, many aspects are involved. Therefore, when analyzing the management model, it is necessary to establish a number of qualitative and quantitative indicators from a systematic point of view. On the basis of the above analysis, an evaluation model is applied and the management model is evaluated. An attempt is made to establish a multidimensional Hilbert space of index space and an exponential model based on the excellent characteristics of the space vector paradigm; on this basis, the index analysis theory is established to make an evaluation of the overall impact of each index.

2. Overview

Betts and Lansley analyzed the literature of the journal CME (Journal of Construction Engineering and Management) during its first decade (from its inception in 1983 to 1992), providing information on the authors of the literature, the content of the literature, the sources of the literature, and the cited literature, and the general approach of CME research was counted. In particular, a research database was created to classify and analyze research content from four perspectives, research topics (7 categories), levels of analysis (6 categories), stages in the construction life cycle (7 categories), and sectors (6 categories), and to review research approaches to engineering management in terms of information sources (3 categories) and research contributions (5 levels). It was found that 70% of the CME literature at that time was based on cases or initial or near-initial data as empirical evidence and that research in engineering management lacked contributions and development of the theory and methods themselves [2]. Pietroforte et a1. conducted a literature review of the American Society of Civil Engineers (ASCE) journal CEM for the eighteen-year period 1983–2000 [3]. Pietroforte conducted a documentary analysis of the research trends in engineering management as reflected in the journal CEM from 1985 to 2002 from a historical perspective, including author information and research topics, and concluded that the main research findings included the following [3]. Abudayyek et a1. examined seven previous studies of project management trends in two journals, IJPM and PMJ, and concluded that the research collaboration between industry, government, and academia should be enhanced [4]. Keyword analysis of trends were carried out over the decade 1994–2003, comparing the similarities and differences in the topics covered by the two journals and their trends and further comparing previous studies to reveal a comprehensive trend in research in the field of project management [5].

Michael's study concluded that the process of total project control is a process of system control, which requires the use of modern information technology as a basis for collecting and processing information related to project engineering, and elaborated on the process of system control, which served as a good guide for later studies [6]. Jorg

Becker et al. used the identification function and the control function to conduct a relevant project total control. Jorg Becker et al. conducted a study related to total project control using identification and control functions, and the results showed that the combination of identification and control can ensure further achievement of project goals [6]. Lee's study proposed that the working platform of the total control model needs a unified information structure model, and the decomposition of the project structure and process structure can produce a "tree structure," which can realize a unified information structure [7]. Sacks studied the relationship between engineering information technology and lean construction and concluded that it can bring a significant increase in productivity to the construction industry and can realize lean construction in the construction industry, which is the technical basis for the smooth implementation of the integrated product development model [8]. Lauri argued that the 3D visual modeling and browsing of construction information technology in the engineering delivery model and the 3D model adding schedule information and cost information can effectively integrate and manage engineering information in all phases to achieve lean construction of engineering projects [9]. Lee suggested that integrated product multiparty contracts, lean construction ideas, engineering information modeling technology, and risk-sharing benefit-sharing teams are essential factors for the success of the integrated product development model. Also, it was pointed out that the lack of relevant legal provisions, lack of contract specifications, and revenue sharing and risk-sharing issues are the main obstacles to the success of the model [10].

3. Establishment of Hilbert's Index Space

3.1. Hilbert Space

3.1.1. Inner Product Space. If any vectors x, y, and z and any number c in a vector space X satisfy the following axiom [11]:

(1) $\langle x, y\rangle = \langle y, x\rangle$

(2) $\langle x + y, z\rangle = \langle x, z\rangle + \langle y, z\rangle$

(3) $\langle cx, y\rangle = c\langle x, y\rangle$

(4) $\langle x, x\rangle \geq 0$, and $\langle x, x\rangle = 0$ when and only when $x = 0$

The vector space endowed with inner products is called the inner product space. If condition (4) is satisfied, we say that the inner product is strict, and on the basis of the strict inner product space, we define a norm $\|.\|$: $\|x\| = \sqrt{(x, x)}$, namely, $\|x\|^2 = (x, x)$.

The distance between two vectors can be measured using the norm. This space is also called the metric space.

3.1.2. Hilbert Space. Hilbert space is a strict inner product space, which must satisfy both completeness and separability [12]. It was first developed by David Hilbert in his study of integral equations. The completeness here means that the Cauchy columns in space converge. Separability refers to the existence of countable dense subsets in a space [13, 14].

3.2. Establishment of Index Space. In the of management mode, the traditional methods mainly include the analytic hierarchy process, fuzzy comprehensive evaluation method, and grey relational comprehensive evaluation method, and traditional methods have shortages in the treatment of the quantitative data, the layers of index correlation, and specific problems. These methods have more obvious effect, but the method has higher subjective and cannot see the indicators change on the influence of the final evaluation results. The evaluation model constructed based on Hilbert space has good data processing function, including quantitative and qualitative data, and Hilbert space has weak compactness of unit sphere, which can explain the contribution of a certain index to the overall evaluation, that is, the influence of the change of each index on the overall result [15].

The main content of this study is to select appropriate indicators and establish Hilbert index space on the basis of analyzing the factors affecting project management. Then, according to the relative weight of indicators calculated by partial differential equation, the weight operator is generated and then establishes a standard Hilbert index subspace.

3.2.1. Establishment of Hierarchical Structure. On the basis of in-depth analysis of the actual problem, each factor concerned is decomposed into several levels from top to bottom according to different attributes, and the factors in the same level are subordinate to the factors in the upper level or have influence on the factors in the upper level, whether dominate the factors in the lower level or influence the factors in the lower level on the other hand. The uppermost level is the target level, which usually has only one factor, the lowermost level is usually the solution or object level, and the middle can have one or several levels, usually the criterion or indicator level [16].

To facilitate the calculation of the model structure, the data and information related to the hierarchical analysis method used in this paper are directly quoted from the hierarchy of indicators established in [17, 17], which is divided into three layers. The first layer is the target layer, which is the selection of a suitable engineering management mode; the second layer is the indicator layer, which is the main indicator system for evaluation, i.e., the main factors affecting the selection of engineering project management mode: engineering characteristics, owner's demand, and owner's preference; the third layer is the subindicator layer, which is the refinement of the second-layer indicators.

3.2.2. Generation of Weighting Operator. The weights of the indicators can be determined by using the improved hierarchical analysis method based on the cloud model. In this study, we adopt the 1~9 scaling method to determine the relative importance between two indicators and construct the judgment matrix of two comparisons of indicators based on the cloud model scaling to determine the weights of the criterion layer first and then the weights of the indicator layer. The specific method is referred to [17], and the results of citing [17] are obtained as follows:

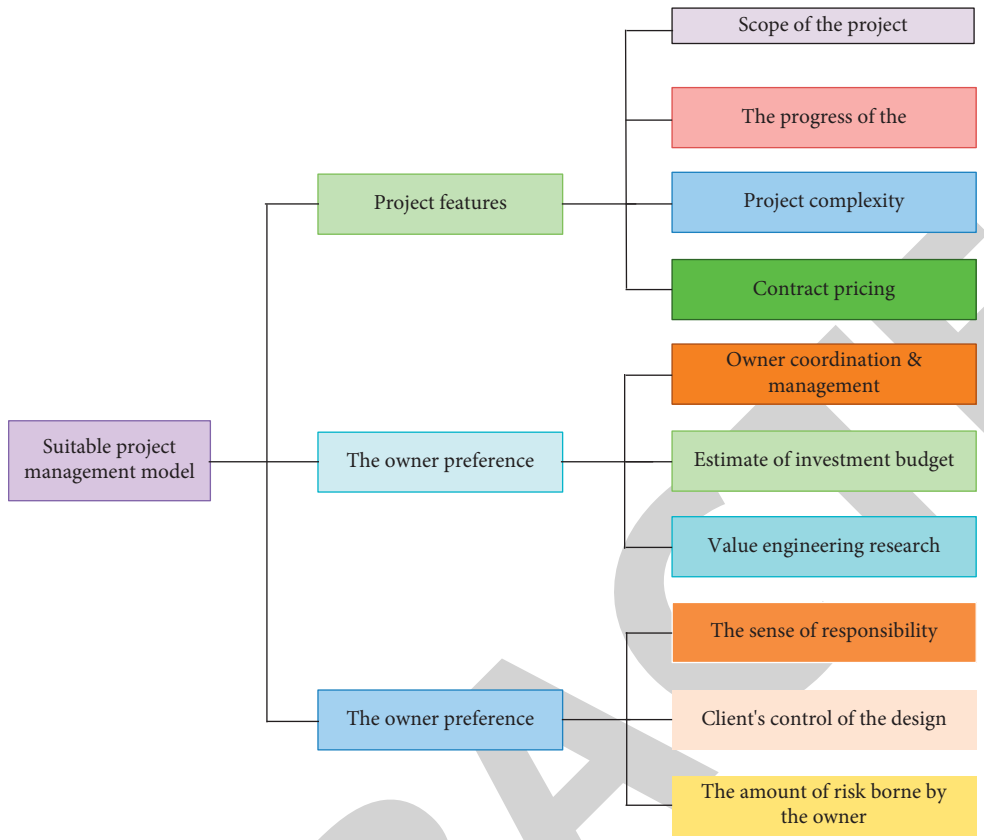


Figure 2: Influence index of project management mode.

$$\nabla_j = \frac{\sum_{i=1}^{k} w_{ij} + k/2 - 1}{k(k-1)}, i = 1, 2, \cdots, k. \quad (1)$$

3.3. Establishment of Standard Hilbert Index Subspaces. The factors that affect the project management mode mainly include the characteristics of the project, the needs of the owner, and the preference of the owner. The contents of each factor are shown in Figure 2.

The main influencing factors of project management mode include three categories and ten subcategories, and these indicators are irrelevant. Therefore, consider building a $n = 10$ dimension Hilbert index space (H^{10}), with each index representing one dimension of the index space, $e = \{e_1, e_2, ..., e_{10}\}$ is an orthonormal basis for H^{10}. Let N be a linear subspace of H^{10}, representing the spatial distribution of original index data. After the quantitative processing of indicators, y vector of each indicator element can be expressed as

$$y = \{\lambda_1 e_1, \lambda_2 e_2, \ldots, \lambda_{10} e_{10}\}, \quad \lambda_i \le 1. \quad (2)$$

Then, the coordinate of the element y vector in H^{10} is as follows:

$$y = (\lambda_1, \lambda_2, \ldots \lambda_{10}). \quad (3)$$

There is another linear subspace M of Hilbert space H^{10}, where M represents the standard subspace after considering the weight. Let the element of M be x; then, there exists mapping ∇ so that the expression for x is

$$x = \nabla \cdot y = (\nabla_1 y_1, \nabla_2 y_2, \ldots, \nabla_{10} y_{10}), \quad (i = 1, 2, j = 1, 2, \ldots 10). \quad (4)$$

Substitute (2) into (4)‘ x can also be expressed as

$$x = (\nabla_1 \lambda_1 e_1, \nabla_2 \lambda_2 e_2, \ldots, \nabla_{10} \lambda_{10} e_{10}). \quad (5)$$

The standard Hilbert linear index subspace M is obtained.

4. Impact Index Vector Norm Evaluation Model and Impact Index Analysis Based on *M*

4.1. Establishment of the Econometric Model. The evaluation index selected above is relatively independent, so the standard Hilbert space vector has excellent number multiplication characteristics. Based on the above consideration, the unit sphere is established, corresponding to the safety index vector. According to the weak compactness of unit sphere in Hilbert space, the norm of influence factor vector ||M|| can be used to represent the size of influence factor F of engineering management mode. So, the exponential function is

$$F = \|M\|. \quad (6)$$

The modeling process is shown in Figure 3.

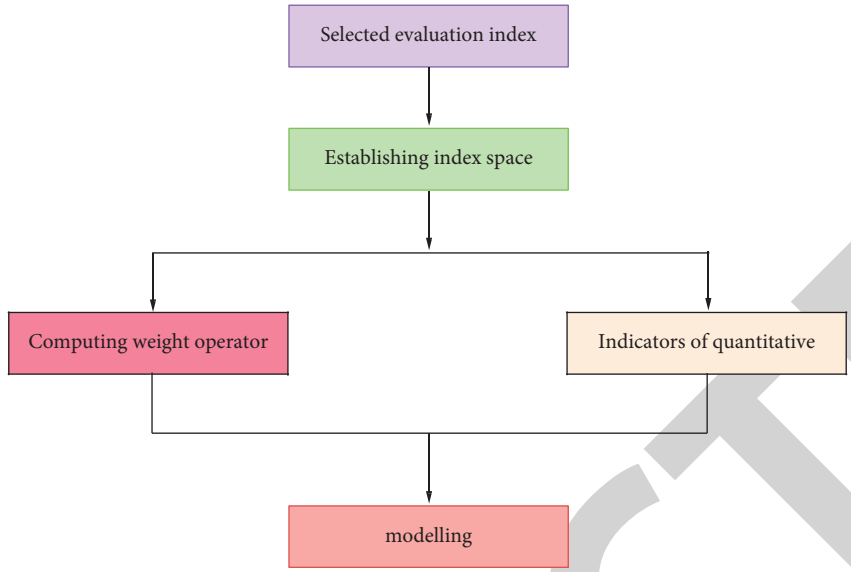


Figure 3: Modeling process.

||M|| is a function of the standard index subspace, which can be expressed as follows:

$$\|M\| = \sqrt{\nabla_1\lambda_1 e_1^2 + (\nabla_2\lambda_2 e_2)^2 + \ldots + (\nabla_{10}\lambda_{10}e_{10})^2}. \quad (7)$$

Therefore, the index influence function can be expressed as follows:

$$\|F\| = \sqrt{\nabla_1\lambda_1 e_1^2 + (\nabla_2\lambda_2 e_2)^2 + \ldots + (\nabla_{10}\lambda_{10}e_{10})^2}. \quad (8)$$

The influencing factors calculated by the above model can be used to measure the project management mode comprehensively and relatively simply. We can see at a glance whether this management mode is standard and provide a scientific and quantifiable basis for horizontal comparison and vertical comparison.

After calculation and research, the project management mode can be divided into grades, as shown in Table 1:

4.2. Index Analysis of Influencing Factors. Fundamental factor analysis is a method to analyze the factors that have an impact on management mode. As can be seen from the above, the influencing factor model can measure whether this management mode is optimal, but it cannot be used to solve practical problems because we do not know which specific factor causes this situation. Therefore, you need to apply the principle of indicator analysis to analyze each indicator in the indicator space to obtain the impact of each indicator on management indicators, that is, the contribution rate. In this study, partial differential equations are established to solve problems [18].

Partial differential equations are one of the largest and most widely used branches of mathematics. Because of its strong physical background, it is also called mathematical equation. A mathematical physical equation is a mathematical description of the laws of natural or social phenomena. After the establishment of calculus in the seventeenth century, the theory of ordinary differential equations is developed immediately. At that time, ordinary differential equations were applied to solve new problems in geometry and physics [19].

Table 1: Management mode scoring levels.

Grade	Tiny	Small	Medium	Larger	Great
Score	Under the 85	85–88	88–92	92–95	More than 95

Taking the calculation of the contribution rate of indicator $y_j\,(j = 1, 2, \ldots, 10)$ to influencing factors as an example, the natural logarithm of both sides of the influencing factor function is obtained as [20]

$$LnF = \frac{1}{2}Ln\left[(\nabla_1 y_1)^2 + (\nabla_2 y_2)^2 + \ldots + (\nabla_{10}y_{10})^2\right]. \quad (9)$$

The partial derivative of both sides with respect to y_i yields as

$$\begin{aligned}\frac{1}{F}\times\frac{\partial F}{\partial y_j} &= \frac{1}{2}\times\frac{1}{(\nabla_1 y_1)^2 + (\nabla_2 y_2)^2 + \ldots + (\nabla_{10}y_{10})^2}\times\partial\left(\nabla_j y_j\right)^2\\ &= \frac{1}{2}\times\frac{1}{(\nabla_1 y_1)^2 + (\nabla_2 y_2)^2 + \ldots + (\nabla_{10}y_{10})^2}\\ &\quad\times 2\left(\nabla_j y_j\right)\times\nabla_j y_j'\\ &= \frac{\nabla_j y_j\times\nabla_j y_j'}{(\nabla_1 y_1)^2 + (\nabla_2 y_2)^2 + \ldots + (\nabla_{10}y_{10})^2}.\end{aligned} \quad (10)$$

The symbol Δ is introduced to represent the change, and the formula above is simplified as follows:

$$\Delta F = \frac{F\times\nabla_j y_j\times\nabla_j}{(\nabla_1 y_1)^2 + (\nabla_2 y_2)^2 + \ldots + (\nabla_{10}y_{10})^2}\Delta y_j\,(j = 1, 2, \ldots, 10). \quad (11)$$

Table 2: Index of an engineering project.

Index	Project scope	Progress of works	Project complexity	Contract pricing	Coordination and management of owners	Estimate of investment budget	Value engineering research	Responsibility	Client's control of the design	The amount of risk taken by the owner
1-λj(%)	4	6	3	10	12	1	5	9	7	8
λj	96	94	97	90	88	99	95	91	93	92

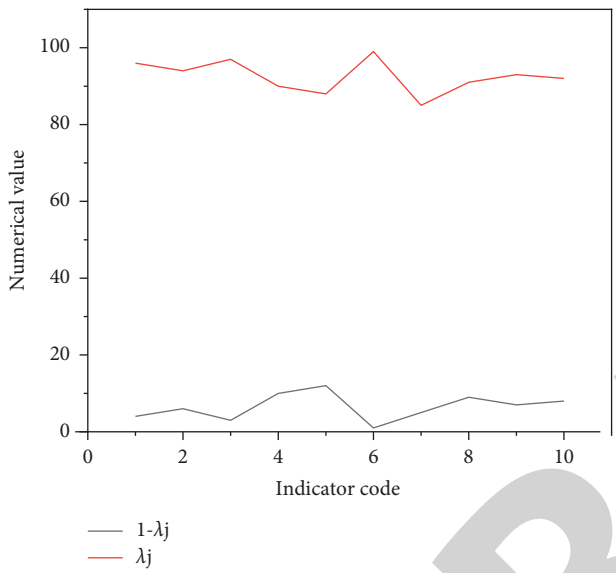


Figure 4: Line chart of engineering project indicators.

$F \times \nabla_j y_j \times \nabla_j / (\nabla_1 y_1)^2 + (\nabla_2 y_2)^2 + \cdots + (\nabla_{10} y_{10})^2$ in the above formula is defined as the index elastic operator and use $\alpha_j (j = 1, 2, \ldots, 10)$; then, the above equation can be expressed as

$$\Delta F = \alpha_j \Delta_{y_j} \quad (j = 1, 2, \ldots, 10). \tag{12}$$

Through the above methods, the contribution rate of each index change to the project management model can be quantitatively evaluated. When further applied to project management, it can guide the site to find out which specific factor has the greatest influence and does not reach the optimal and take targeted measures to ensure the maximum benefit of the project.

5. The Numerical Example

5.1. Calculate Whether the Management Mode Is Optimal. The data indicators of the influence of a company are as follows. Through the calculation of each indicator, we can get F, which is the current mode level. Index of an engineering project is shown in Table 2 and Figure 4.

By using the index space established above and substituting the values in Table 2 into formula (5), the index vector of the standard Hilbert index subspace can be obtained:

$$x = (96\nabla_1 e_1, 94\nabla_2 e_2, 97\nabla_3 e_3, 90\nabla_4 e_4, 88\nabla_5 e_5, 99\nabla_6 e_6, 95\nabla_7 e_7, 91\nabla_8 e_8, 93\nabla_9 e_9, 92\nabla_{10} e_{10}). \tag{13}$$

Then, based on the calculation results of [17], the weight operator is

$$\nabla = (0.266, 0.217, 0.327, 0.2, 0.384, 0.333, 0.283, 0.267, 0.4, 0.333). \tag{14}$$

By substituting x and ∇ into (8), it can be obtained that the influence index of the engineering factor is

$$F = 90.895. \tag{15}$$

5.2. Index Analysis. It can be seen that the score of this management mode is of medium grade and has not achieved the optimal effect, but the specific reasons are caused by the calculation of α to know which indicator has the greatest influence. The greater α is, the greater the influence on the whole management mode is. Then, according to this index, choose the appropriate management mode, in order to achieve the maximum benefit.

According to the definition of indicator elastic operator and the above calculation results, the indicator elastic operator can be obtained as

$$\alpha = (0.075, 0.049, 0.093, 0.04, 0.1427, 0.121, 0.084, 0.0714, 0.1637, 0.1122). \tag{16}$$

And $\Delta y_j = 1 (j = 1, 2, \ldots, 10)$; the above results are substituted into (12), and the contribution rate of each indicator to the total impact indicator is

$$\alpha = (0.075, 0.049, 0.093, 0.04, 0.1427, 0.121, 0.084, 0.0714, 0.1637, 0.1122). \tag{17}$$

5.3. Summary. From Table 2, it can be seen that the owner's control over the design is the most important factor affecting the management mode. Therefore, the owner's control over

the design should be strengthened. If the economic management personnel of the enterprise fail to analyze the economic situation in the design stage in time, the construction drawing is found to exceed the budget after the construction drawing budget is completed. In this case, in order to guarantee the project, carry on smoothly; some owners will be in the design; request a change to construction drawing design unit, although this will control the project cost, but it will seriously affect the speed of engineering construction and also can lead to a rise in the cost of construction design and the economic losses brought to the owner.

The design-build management mode is selected [21]. After the project is approved, the owner will contract the design, construction, material and equipment procurement, and other tasks of the project to a general contractor, who will be responsible for all the organization and management of the project construction and finally hand over the construction results to the project owner. Adopting this mode can make the design and construction combine organically, which is beneficial to the contractor to control the progress and cost. Due to the simple contractual relationship between the owner and the contractor, the owner has less organization and coordination, so he has less control over the project. At the time of signing the general contract both contract terms and contract price are difficult to be accurately determined. The increase of uncertainty makes the contractor demand higher risk compensation and leads to higher contract price or cause more contract disputes in the future. The implementation of design-construction mode has higher quality requirements for general contracting units, which are generally rich in capital, strong in technology and coordination, and have greater benefits and risks.

6. Conclusion

In the analysis of the engineering management model, this study makes full use of rough set theory, simplifies the evaluation index, increases the objectivity of weight calculation, and provides a useful reference for the analysis of management model evaluation research. On the basis of analyzing the defects of traditional evaluation methods, a project management model based on Hilbert space vector norm is proposed, and a new evaluation method is established. It can help organizations to normalize project management activities that are difficult to quantify according to a series of criteria and identify weak links, thus helping organizations to improve management capacity and level. This model is a characteristic evaluation model constructed according to the actual situation of big science engineering, which is mainly applicable to the evaluation of similar project management ability.

Compared with traditional evaluation methods, this model has the following advantages:

(1) It has good data processing function, including qualitative data and nonqualitative data, and has a strong promotion prospect

(2) Through index analysis, the evaluation objects can be compared horizontally and vertically

(3) Through index analysis, the contribution rate of each index to the total index can be obtained, problems and gaps can be found, and the management environment can be improved with a targeted approach, which has strong applicability

However, the evaluation system of engineering management mode in this study has few index samples and limited reduction of index samples. Therefore, in the future research, we should constantly improve the evaluation index, deeply study the reduction function of rough set theory on evaluation index, improve the evaluation index of engineering management model, and promote the accuracy of evaluation results.

Data Availability

The labeled dataset used to support the findings of this study are available from the author upon request.

Conflicts of Interest

The author declares that there are no conflicts of interest.

References

[1] X. Chen, "Content analysis and optimization measures of civil engineering project management," *Management and Technology of Small and Medium-sized Enterprises (Mid-day)*, vol. 09, pp. 25–27, 2021.

[2] M. Betts and P. Lansley, "Construction Management and Economics: A review of the first ten years," *Construction Management & Economics*, vol. 11, no. 4, pp. 221–245, 1993.

[3] R. Pietroforte and T. P. Stefani, "ASCE journal of construction engineering and management: Review of the years 1983-2000," *Journal of Construction Engineering and Management*, vol. 130, no. 3, pp. 440–448, 2004.

[4] O. Abudayyek, A. Dibert-DeYoung, and E. Jaselskis, "Analysis of trends in construction research: 1985-2002," *Jouranl of Comtruction Engineering and Management*, vol. 130, no. 3, pp. 433–439, 2004.

[5] L. Crawford, J. Pollack, and D. England, "Uncovering the trends in project management: Journal emphases over the last 10 years," *International Journal of Project Management*, vol. 24, no. 2, pp. 175–184, 2006.

[6] M. Hough, "Computing trends for civil Engineers," *Journal of Computing in Civil Engineering*, vol. 10, pp. 45–47, l997.

[7] J. Becker, M. Kugeler, and M. Rosemann, "Process management," *Journal of Computing in Civil Engineering*, vol. 10, pp. 27–32, 2003.

[8] R. Sacks, B. A. Dave, and L. Koskela, "Analysis framework for the interaction between lean construction and building information modelling," *Proceedings for the 17th Annual Conference of the International Group for Lean Construction*, vol. 7, pp. 90–93, 2009.

[9] R. Sacks and L. Koskela, "Interaction of lean and building information modeling in construction," *Construction Engineering And Management*, vol. 136, no. 9, pp. 968–980, 2010.

[10] S. L. Christopher, "Implementation of integrated project delivery on Department of Navy Military construction

Hindawi
Security and Communication Networks
Volume 2024, Article ID 9897623, 1 page
https://doi.org/10.1155/2024/9897623

Retraction

Retracted: A New Method for Inverter Diagnosis of Electric Locomotive Using Adversarial Neural Networks

Security and Communication Networks

Received 8 January 2024; Accepted 8 January 2024; Published 9 January 2024

This article has been retracted by Hindawi following an investigation undertaken by the publisher [1]. This investigation has uncovered evidence of one or more of the following indicators of systematic manipulation of the publication process:

(1) Discrepancies in scope

(2) Discrepancies in the description of the research reported

(3) Discrepancies between the availability of data and the research described

(4) Inappropriate citations

(5) Incoherent, meaningless and/or irrelevant content included in the article

(6) Manipulated or compromised peer review

The presence of these indicators undermines our confidence in the integrity of the article's content and we cannot, therefore, vouch for its reliability. Please note that this notice is intended solely to alert readers that the content of this article is unreliable. We have not investigated whether authors were aware of or involved in the systematic manipulation of the publication process.

Wiley and Hindawi regrets that the usual quality checks did not identify these issues before publication and have since put additional measures in place to safeguard research integrity.

We wish to credit our own Research Integrity and Research Publishing teams and anonymous and named external researchers and research integrity experts for contributing to this investigation.

The corresponding author, as the representative of all authors, has been given the opportunity to register their agreement or disagreement to this retraction. We have kept a record of any response received.

References

[1] Y. Shi, C. Chen, and Y. Luo, "A New Method for Inverter Diagnosis of Electric Locomotive Using Adversarial Neural Networks," *Security and Communication Networks*, vol. 2022, Article ID 5606328, 10 pages, 2022.

Hindawi
Security and Communication Networks
Volume 2022, Article ID 5606328, 10 pages
https://doi.org/10.1155/2022/5606328

Research Article

A New Method for Inverter Diagnosis of Electric Locomotive Using Adversarial Neural Networks

Yingchun Shi,[1,2] Chunyang Chen,[1] and Yu Luo [1]

[1]*School of Traffic & Transportation Engineering, Central South University, Changsha 410075, China*
[2]*School of Electronic Engineering, Hunan College of Information, Changsha 410200, China*

Correspondence should be addressed to Yu Luo; 174201008@csu.edu.cn

Received 7 April 2022; Accepted 15 May 2022; Published 1 June 2022

Academic Editor: Fang Liu

In order to improve the fault diagnosis accuracy of the electric locomotive inverter, this article combines the adversarial neural network to construct the electric locomotive inverter diagnosis system. Moreover, at the data level, this article compares and analyzes three methods of data expansion based on single-sample processing, data expansion based on image front and background separation, and data expansion based on an adversarial neural network. In addition, this article adopts a new feature extractor and increases the penalty cost of small samples being misclassified. Finally, this article uses the LBP operator to extract the image texture features to distinguish and detect the different shapes of the rotor windings and build an intelligent system to verify the effect of the proposed system model. The experimental research shows that the inverter diagnosis system for electric locomotives based on the proposed adversarial neural network has a good practical effect.

1. Introduction

As the rear stage of the electric traction converter, the electric traction inverter converts the DC signal into an AC signal with a controllable frequency and amplitude so as to realize the speed control of the traction motor. The traction inverter consists of several IGBT modules with integrated diodes. Due to the high reliability and stability of the diode and the less electrical and thermal stress it bears, the faults of the traction inverter are mainly IGBT faults. The IGBT fault can be divided into IGBT open-circuit fault, IGBT short-circuit fault, and IGBT gate signal intermittent loss fault. IGBT short-circuit faults often generate extremely large currents in a very short period of time, causing serious damage to the system. Therefore, it is difficult to diagnose IGBT short-circuit faults online. Some auxiliary protection circuits are often used to prevent the occurrence of IGBT short-circuit faults or series fast fuses can convert short-circuit faults into open-circuit faults. The intermittent loss of IGBT gate signal is mainly caused by factors such as poor contact between the drive circuit and the control circuit, line aging, and electromagnetic interference. It is relatively difficult to diagnose online, and it can be regarded as an open-circuit fault and subsequent offline diagnosis can be performed. Therefore, this article mainly studies the IGBT open-circuit fault of electric traction inverter.

The high-speed train can run on the railway mainly by the drive of the electric motor, and the electric motor that drives the train forward is called the traction motor. The traction motor system of a high-speed train consists of multiple power configuration units, each of which includes electrical equipment such as transformers, rectifiers, and inverters, as well as mechanical equipment such as traction motors, gear boxes, and driving wheels. In the CRH type EMU, the energy of the train comes from the alternating current in the overhead catenary. It first uses the pantograph to receive the current, then transmits it to the main transformer through the line to reduce the voltage, and then rectifies and inverts through the converter to provide energy for the traction motor. The wheels are driven by gear transmission to make the train move forward at high speed. At present, China already has the world's largest high-speed railway network, with high-speed trains galloping along the railways from the icy and cold alpine regions to the hot and

rainy tropical regions. Therefore, the train needs to be able to run stably in harsh environments such as severe cold, high temperature, sand, and dust. In such a complex operating environment, the traction motor system of high-speed trains has undergone various tests, and some failures will inevitably occur. Common traction motor system faults include traction motor interturn short circuit, broken rotor bars, stator voltage and current sensor faults, speed sensor faults, converter IGBT component faults, and sensor faults. The research on fault detection and diagnosis for these common faults can not only ensure the good working condition of the train but also avoid serious losses caused by faults during operation, which is of great significance to ensure the safe and stable operation of high-speed trains.

In this article, an adversarial neural network is used to construct an inverter diagnosis system for electric locomotives, so as to improve the real-time performance of inverter diagnosis of electric locomotives.

2. Related Work

In order to ensure the normal operation of the inverter, it is necessary to carry out real-time monitoring and online diagnosis [1]. In the inverter fault, the short circuit and open circuit of the power device are the most frequent faults of the inverter. A short-circuit fault will generate a large short-circuit current instantaneously. Usually, the diagnosis of a short-circuit fault is mainly realized through hardware circuits, or a fast fuse is connected to the bridge arm to convert the short-circuit fault of the power tube into an open-circuit fault, and the open-circuit fault diagnosis method is used [2]. When an open-circuit fault occurs in the power tube of the inverter, the system can still operate under abnormal conditions, but it will lead to distortion of the output waveform and unbalanced voltage on the DC side. Therefore, the existing research on inverter fault diagnosis mainly focuses on the open-circuit fault diagnosis research [3]. Inverter fault diagnosis methods can be divided into current-based diagnosis methods and voltage-based diagnosis methods according to different detection quantities. Literature [4] takes the inverter three-phase current signal as the characteristic parameter, first uses wavelet analysis to denoise the signal, then obtains the fault feature vector through Fourier transform to statistics the current signal, and constructs a neural network model to realize fault diagnosis. Literature [5] discusses the current vector trajectory slope method and the current vector instantaneous frequency method. The former judges the fault location by the slope of the current vector trajectory, and the latter judges whether the fault occurs or not by setting the literature threshold according to the instantaneous frequency of the current vector under the fault condition is 0 but cannot locate the fault. Literature [6] can diagnose single-phase open-circuit faults and single-pipe open-circuit faults according to the obtained spectrum components by performing a double Fourier transform on the DC side bus current. While the current-based approach simply measures the load current without adding additional sensors, it is susceptible to load effects. Literature [7] configures a large number of voltage sensors in the circuit, compares the inverter phase voltage, motor phase voltage, motor line voltage, or motor neutral point voltage with the normal state, and diagnoses open-circuit fault devices according to the voltage deviation. Literature [8] establishes a neural network for sampling the output voltage of the converter to realize fault diagnosis. When analyzing the working state of the inverter circuit, it is necessary to consider both the control transition and the condition transition of the circuit. The control transition refers to the topology change of the power electronic circuit caused by the control signal of the power tube, and the conditional transition refers to the topology change of the power electronic circuit caused by the change of the state of the circuit itself leading to the change of the on-off state of the uncontrollable device. Most of the inverter diagnosis methods are based on the traditional switching function model. The traditional switching function model can only describe the control transition of the circuit, and it is difficult to accurately describe the condition transition that may occur under fault conditions, so the accuracy of the described fault circuit state characteristics cannot be guaranteed. Literature [9] considers the condition changes of the circuit and uses the output current as the identification vector to establish a hybrid logic dynamic model to realize the open-circuit fault diagnosis of the inverter. However, similar to most previous models, this inverter model does not consider the influence of clamp diodes on the circuit, and the freewheeling effect of clamp diodes cannot be ignored in practical situations.

Literature [10] proposed a converter fault diagnosis model based on the rough set decision table. Based on the acquisition of the three-phase output current energy value, the decision table was established, and the rough set method was used to simplify the decision table, which not only can diagnose faults but also has good performance. Adaptability: literature [11] used a combination of wavelet analysis and neural network diagnosis method for the rectifier fault of HXDl heavy-haul freight locomotive. First, the fault feature vector of the rectifier output voltage waveform was extracted by wavelet analysis, and then the BP neural network was improved based on a genetic algorithm. The algorithm establishes the correspondence between the fault feature vector and the fault mode. Literature [12] proposes a fault diagnosis method for analog circuits that combines optimal wavelet packets and extreme learning machines. Based on the degree of feature deviation, wavelet bases are selected to participate in feature extraction, and then extreme learning machines are introduced to discriminate fault types. There is a clear advantage in time. Literature [13] studies the converter fault diagnosis method based on the knowledge base, extracts the fault features from the data of various types of faults obtained in advance, establishes the knowledge base, and inputs the data of the unknown fault type into the knowledge base for comparison. Get a diagnosis. Literature [14] comprehensively uses two methods of principal component analysis and support vector machine for fault diagnosis of power electronic rectifier. First, the principal component analysis method is used to extract the fault eigenvalues of the three-phase rectifier, and then the model

established by the support vector machine is used and realizes fault diagnosis.

When using quantitative analysis to diagnose faults, it is necessary to establish a system model first and then use the model to analyze and calculate various indicators of the research object. In the model-based fault diagnosis method, the mathematical model of the system is used to obtain the expected data of the system, and the deviation between the actual operating state and the expected state of the system is judged by the residual between the expected data and the observed input and output data. Fault diagnosis is made by analyzing the residual signal [15]. Generally speaking, such methods include the state estimation method, Parameter Estimation method, and Parity Space method. The fault diagnosis method based on state estimation mainly uses observers or filters to estimate the state of the system and then compare the system state with the constructed system health or fault model for fault diagnosis [16]. The basic principle of fault diagnosis based on parameter estimation is that if a fault occurs, the process parameters of the system will change, and the changes of process parameters will also affect the parameters of the system model. Therefore, by observing the system model, according to the changes in the system parameters for fault diagnosis [17], the fault diagnosis method based on equivalence space first establishes the mathematical relationship between the system input and output and then diagnoses the fault by checking whether the input and output values obtained from the system sensors satisfy the equivalence relationship obtained by the mathematical model. In the analytical redundant fault diagnosis method, the difference value obtained after the consistency test of multiple variables is called the residual signal [18]. When the system is in a healthy state, the residuals should have zero mean, and the occurrence of faults will cause deviations in the residuals, so the deviation of the residuals is used to diagnose whether the system has faults. The consistency check in analytical redundancy is usually to compare the observed signal obtained by the sensor with the estimated value from the mathematical model and obtain the residual to diagnose the fault of the system [19].

3. Processing of Sample Imbalance Problem Based on Adversarial Neural Network

In classical supervised machine learning, the number of samples of each category of training samples is generally similar or equal, but when applied to real-world scenarios, the problem of sample imbalance often occurs. For example, there are far more positive samples than negative samples in the rotor qualification test in this article. When these problems arise, the training model robustness will definitely suffer.

In order to reduce the impact of underfitting caused by unbalanced samples, an adversarial neural network is constructed through the dynamic game between the recognizer and the generator, and the sample capacity of the negative samples is expanded. At the data level, it achieves a balanced effect with positive samples while increasing the diversity of negative samples.

The sample image is analyzed with the rotor windings in the foreground and the background, including the hooks on the commutator and other nonwinding areas. By separating the front and background of the image, a separate rotor winding and background part are obtained, and then the two parts are randomly combined, and a new sample image can be obtained by combining the image enhancement method. The common image front and background separation techniques include the background difference method, optical flow field method, and frame difference method. Since the overall detection scheme adopted in this article is a single static image, which lacks the frame information before and after the image, only some experimental improvements and summaries are made on the background difference method.

The background difference method usually refers to a method that first assumes that the background is static, then uses the obtained image and the background image to perform a difference operation, and finally realizes the target recognition in the detection area by combining with threshold segmentation. This article has carried out two experimental analyses on this.

The Gaussian mixture model (GMM) is estimated using the weighted sum of the Gaussian model established in advance on the probability density distribution of sample data. Then, a common statistical method of projecting the probability of belonging to the corresponding class. In the field of image processing, the Gaussian distribution model is used to model each pixel on the image, and the model parameters are optimized and updated through the expectation–maximization algorithm, which can effectively overcome certain influences caused by illumination changes and is mostly used for moving target detection.

In the mixed Gaussian background modeling, the image background information is represented by the probability density of the repeated pixel sample values, and the target pixels are analyzed by methods such as differential statistics. Based on the assumption that image pixels are independent of each other, the image pixels are randomly generated in the sequence image, and the Gaussian distribution model is used to describe the regularity of image pixel color distribution. After that, multiple Gaussian distributions are weighted and superimposed in combination with different weights so as to realize the overall modeling of the image.

The mixed Gaussian distribution model was established based on the rotor winding image, the pixel samples at time t obey the mixed Gaussian distribution, and the corresponding probability density function is as follows:

$$P(X_t) = \sum_{i=1}^{n} W_{i,t}\eta\left(X_t, \mu_{i,t}, \tau_{i,t}\right),$$

$$\eta\left(X_t, \mu_{i,t}, \tau_{i,t}\right) = \frac{1}{\left|\tau_{i,t}\right|^{1/2}} e^{-1/2\left(x_t-\mu_{i,t}\right)^T \tau_{i,t}^{-1}\left(x_t-\mu_{i,t}\right)}, \quad (1)$$

$$\tau_{i,t} = \sigma_{i,t}^2 I.$$

In the above formula, n is the total number of Gaussian distribution modes established by the model, $W_{i,t}$ is the

weight of the ith Gaussian distribution at time t, and the sum of the n modes is 1. At time t, $\eta(X_t, \mu_{i,t}, \tau_{i,t})$ is the corresponding ith Gaussian distribution, where the mean is $\mu_{i,t}$, the covariance matrix is $\tau_{i,t}$, the variance is $\sigma_{i,t}$, and I is the three-dimensional standard identity matrix.

Generally speaking, the steps to achieve image front and background separation based on the Gaussian mixture model are as follows:

① The algorithm initializes the Gaussian model and compares the deviation of the first k Gaussian models with the image pixel X. If it can satisfy the 3 σ criterion, it is a distribution model that can match it, and the value of k is generally 3~6:

$$\left|X_t - \mu_{i,t-1}\right| \le 3\sigma_{i,t-1}. \tag{2}$$

When the matching pattern satisfies the requirements of the background condition, it means that the pixel belongs to the background; otherwise, the opposite is true.

② The algorithm updates the weights of the matching patterns. $M_{i,t} = 1$, if the pattern matches successfully; otherwise, it is 0. The algorithm then normalizes the weights of all modes, and α is the learning rate.

$$W_{i,t} = (1-\alpha)W_{i,t-1} + \alpha M_{i,t}. \tag{3}$$

For the unmatched model, no change is made to its standard deviation and mean u, and the parameter update method of the successfully matched Gaussian model is performed according to the following formula:

$$\begin{aligned} \rho &= \alpha \cdot \eta\left(X_t \mid \mu_k, \sigma_k\right), \\ \mu_t &= (1-\rho)\mu_{t-1} + \rho X_t, \\ \sigma_t^2 &= (1-\rho)\sigma_{t-1}^2 + \rho\left(X_t - \mu_t\right)^T\left(X_t - \mu_t\right). \end{aligned} \tag{4}$$

③ If the matching fails, the algorithm replaces the current pixel value with the mean value for the Gaussian model with the smallest weight and replaces the standard deviation with the larger value. Then, the algorithm sorts each pattern in descending order of W/α^2 size and selects the first N patterns as the image background, and N needs to satisfy the following formula. Among them, the parameter T represents the proportion of the background ($0.5 < T < 1$).

$$N = \arg\left\{\min\left(\sum_{k=1}^{n} w_k > T\right)\right\}. \tag{5}$$

The algorithm repeats the above steps to perform matching detection between X_t and the first N Gaussian models. If the match is successful, it means that the pixel is the background point; otherwise, it is the foreground point.

In the image processing open-source library OpenCV, the GrabCut segmentation algorithm uses the Gaussian mixture model to easily separate the front and the background. For the rotor winding image experiment, the results are shown in Figures 1 and 2.

Since the detected image is intercepted at the same position, the algorithm directly uses the missing picture as the background image and then combines the unilateral image and other differential operations to obtain the foreground image, that is, the image of the rotor winding part. Next, the algorithm uses other images and the obtained foreground image to perform a difference operation to obtain a new background image and then combines different foreground images and background images to obtain a new sample image through image enhancement.

The specific operation process is shown in Figure 3.

Through the separation and fusion of the front and the background of the rotor winding image, we combine the image enhancement technology to obtain a new negative sample image. The experimental results show that the new sample is still different from the original sample, but it cannot meet the diversity needs well.

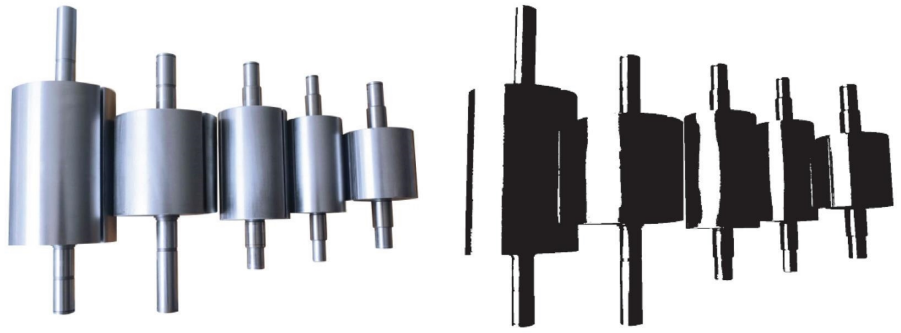
Adversarial neural network (GAN) is a deep learning model based on unsupervised learning based on the idea of game theory. The model framework mainly includes a Generative Model and a Discriminative Model, and an ideal output result is obtained through the mutual game learning of these two models. At present, GAN is mostly used for image generation, and it is also involved in semantic segmentation and data enhancement.

Taking image generation as an example, the basic principle of GAN can be understood as building a generative network G (Generator) and a recognition network D (Discriminator). Among them, G is a network that generates pictures, the input is random noise z, and the corresponding output is G(z). D is a network for judging the true and false pictures, the input is a true and false picture x, and the output D(x) represents the probability of judging that x is a real picture. If the result is 1, it means that the probability that x is a real picture is 100%. On the contrary, if the output is 0, it means that x can never be a real picture; it must be a simulated picture generated by noise. In the model training process, the goal of generating network G is to use noise to simulate as much as possible to generate real pictures, which are used to deceive the discrimination network D. The goal of D is to try to distinguish the image generated by the G network in the input x from the real image. G and D constitute a dynamic zero-sum game process. Ideally, G can generate images G(z) that are hard enough for D to discriminate between real and fake, so $D(G(z)) = 0.5$ at this time. Finally, a suitable generative model G can be obtained, which can be used to generate pictures similar to real pictures, and the recognizer cannot identify true and false.

The above is the core principle of GAN, and the mathematical expression of its objective function is as follows:

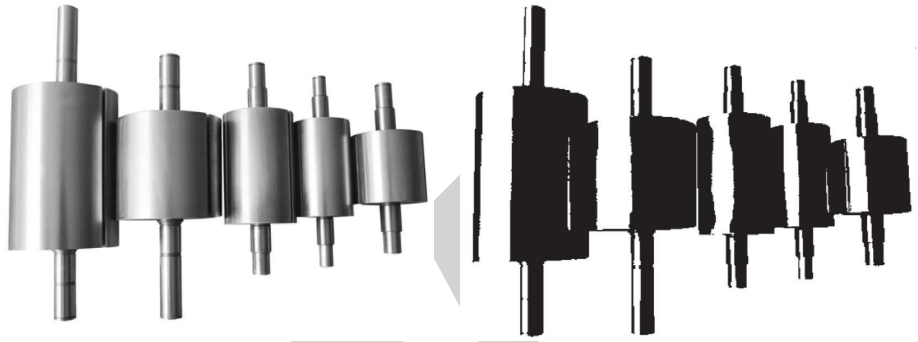
$$\begin{aligned} \min_G \max_D V(D,G) = {} & E_{X-P_{\text{data}}(x)} \log D(x) \\ & + E_{X-P_G(x)} \log\left(1 - D(G(z))\right). \end{aligned} \tag{6}$$

Among them, x represents the real image, z is the input of the G network, which represents the randomly generated noise, and G(z) represents the image generated by the generator simulation. D(x) represents the probability that



(a) (b)

Figure 1: Background separation of bright pieces. (a) Bright parts. (b) Foreground separation map.



(a) (b)

Figure 2: Background separation of dark objects. (a) Dark parts. (b) Foreground separation map.

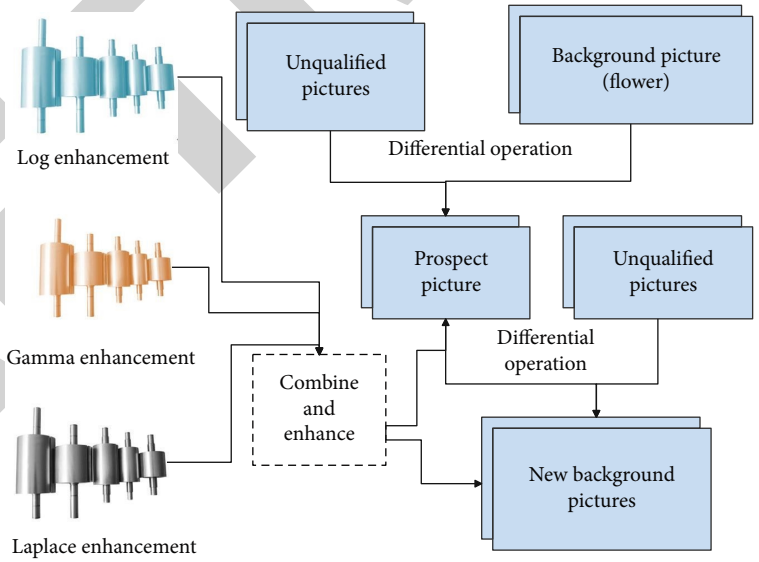


Figure 3: Process of generating negative samples.

the recognition module judges whether the real picture is real. For a real image x, the closer the value of D(x) to 1, the stronger the recognition network's ability to identify the authenticity of the image, while $D(G(z))$ represents the probability that the recognition network judges whether the image generated by the generator is real.

The goal of the G network is to increase the value of $D(G(z)$ as much as possible; that is, G should hope that the difference between the image generated by training and the real image is getting smaller and smaller. However, the goal of the D network is to discriminate between real and fake pictures; that is, as the recognition ability of the D network

increases, $D(x)$ should be larger, and $D(G(z))$ should be smaller. With continuous training, ideally, the above equation converges to an equilibrium state. The schematic diagram of the action of the adversarial network is shown in Figure 4.

When the GAN model network is first trained, the model first partially trains the D network and then trains the G network. According to the objective function, the stochastic gradient is added to obtain the maximum value when training the D network, and the minimum value is obtained by subtracting the stochastic gradient when training the G network. The whole training process is carried out alternately in two stages, and finally, a dynamic balance is achieved. The schematic diagram of model training is shown in Figure 5.

In order to improve the extraction of image features, DCGAN is obtained by combining GAN and CNN, which replaces the previous G network structure and D network structure with a convolutional neural network in structure. In order to improve the quality of generated samples and the speed of model convergence, DCGAN has also made some changes in the structure of the convolutional neural network:

① For the pooling layer, the discriminative network D is replaced with strided convolution, while the generation network G chooses the microstepped magnitude convolution.

② In order to speed up the model convergence and avoid the overfitting problem, batch normalization is used in both the generative model G and the discriminant model D, and the fully connected hidden layer is removed at the same time so that the network becomes a fully convolutional network.

③ In order to better fit the model, in the G network, except for the output layer of the last layer, which uses Tanh, all other layers use ReLU as the activation function. In the D network, all layers use Leaky ReLU as the activation function.

④ In the generative network G, a neural network model similar to deconvolution is used, and upsampling is performed through the transposed convolutional layer operation, while the discriminant network D only uses an ordinary convolutional neural network for feature extraction.

The structure of the generative network G in DCGAN is shown in Figure 6.

The structure of the recognition network D in DCGAN is shown in Figure 7.

Combined with the rotor winding picture analysis, the modified DCGAN network structure is used to expand the insufficient negative samples. Among them, the specific configuration of the parameters is as follows: the input image size is $160 * 160$, the learning rate is 0.0002, the batch size is 32, the iteration is 1000 times, and the output image size is the same as the input size.

The cost-sensitive method refers to adjusting the attention of the optimization model to small samples by adding a penalty function to the objective function, which is generally used to deal with the problem of imbalanced samples from the algorithm level. The common forms are those based on a cost-sensitive matrix and based on a cost-sensitive vector. In common classification problems, it is assumed that there are N types of samples in the training set, and the cost of misclassification of different categories is represented in a cost-sensitive matrix cost of NN. cost$[i, j]$ represents the penalty cost of misclassifying the object of category i to the object of category j, and the optimal state is achieved when the sum of the cost matrix is the smallest [20].

$$\begin{bmatrix} \cos t(1,1) & \cos t(1,2) & \cdots & \cos t(1,N) \\ \cos t(2,1) & \cos t(2,2) & \cdots & \cos t(2,N) \\ \vdots & \vdots & \ddots & \vdots \\ \cos t(N,1) & \cos t(N,2) & \cdots & \cos t(N,N) \end{bmatrix}. \tag{7}$$

Among them, $\cos t(i, j) \in [0, \infty)$. When $j = i$, $\cos t(i, j) = 0$, which means that there is no misclassification.

The penalty method based on the cost-sensitive vector is for a single sample. For sample (x_n, y_n), we take a K-dimensional cost-sensitive vector $\cos t_n$, where $\cos t_n \in [0, \infty)$, the value of the k-th dimension represents the penalty cost of being wrongly identified as the k-th class. The cost-sensitive vector is combined with the samples, and iterative learning is performed with the form $(x_n, y_n, \cos t_n)$ as the input. Relatively speaking, the cost-sensitive matrix method is a special form of the cost-sensitive vector method; that is, the misclassification penalty vector is set to be the same for all samples of a certain class.

Usually, the use of cost-sensitive methods to deal with the problem of sample imbalance requires specifying a cost-sensitive matrix or vector first, and the key is to set the misclassification penalty or misclassification weight. In actual use, the size of the weight in the cost-sensitive matrix or vector is often specified according to the proportion of the sample and other information. For example, if it is assumed that the training samples are divided into three categories, namely, category a, category b, and category c, and the corresponding number of samples is x: y: z, the corresponding cost-sensitive matrix is as follows [21]:

$$\cos t = \begin{bmatrix} 0 & \frac{y}{y+z} & \frac{z}{y+z} \\ \frac{x}{x+z} & 0 & \frac{z}{x+z} \\ \frac{x}{x+y} & \frac{y}{x+y} & 0 \end{bmatrix}. \tag{8}$$

4. Inverter Diagnosis System of Electric Locomotive Based on Adversarial Neural Network

The system adopts the C/S (client/server) structure system, in which the auxiliary inverter fault diagnosis host is the client and the vehicle diagnosis host is the server, and the

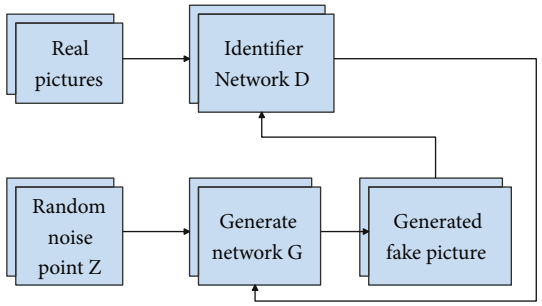


Figure 4: Schematic diagram of the role of the adversarial network.

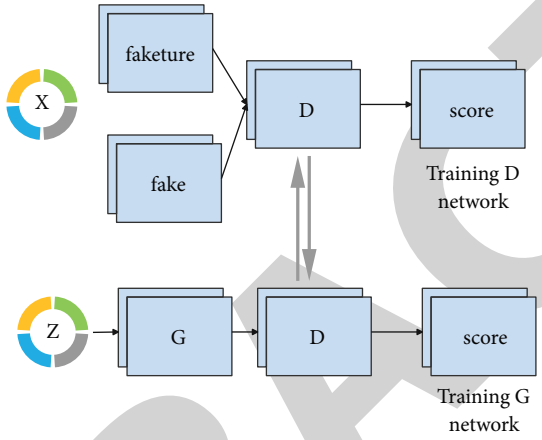


Figure 5: Schematic diagram of model training.

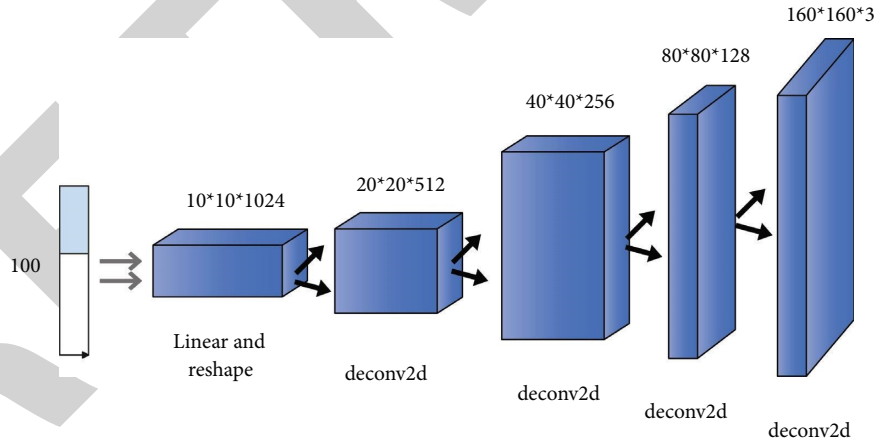


Figure 6: Structure diagram of the generation network.

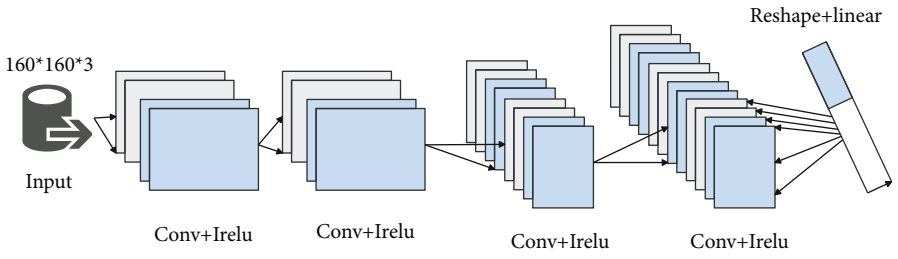


Figure 7: Structure diagram of the recognition network.

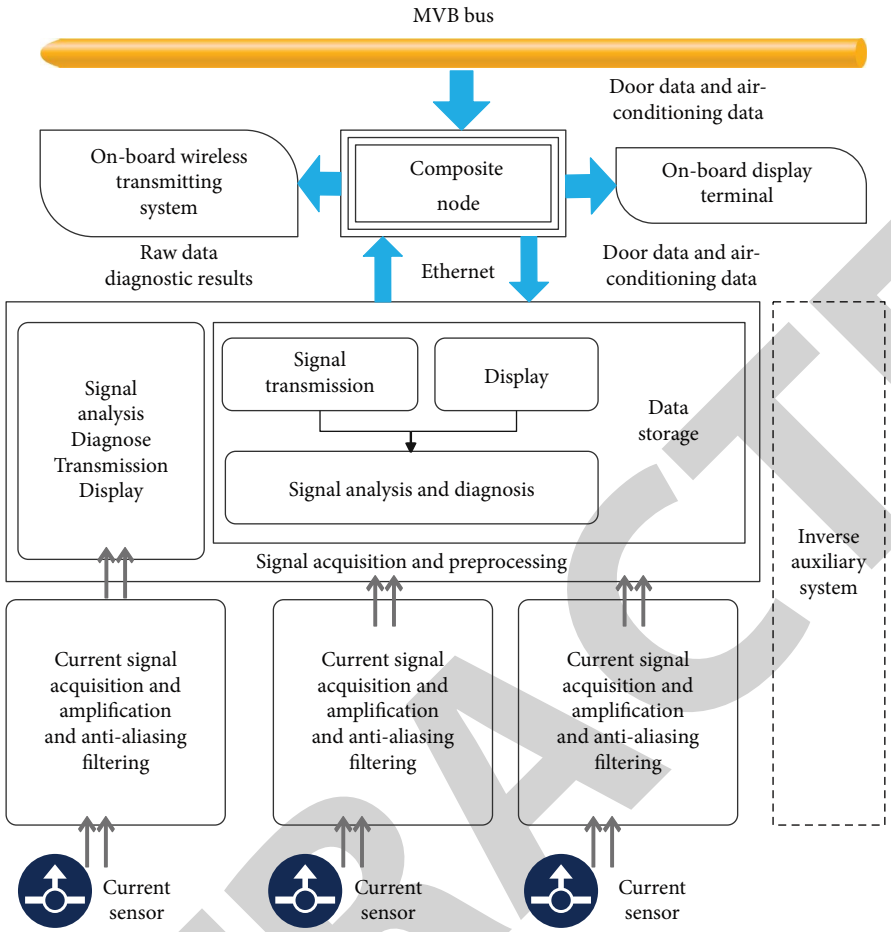


Figure 8: Design of the overall structure of the system.

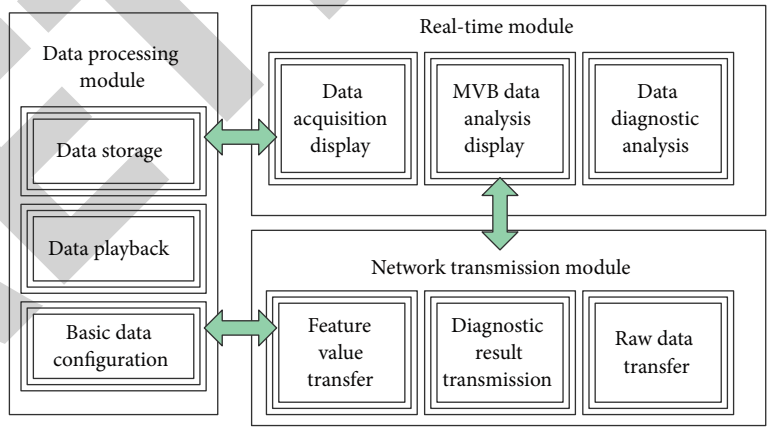


Figure 9: System functional module design diagram.

two communicate through the TCP protocol. The overall structure design of the auxiliary inverter diagnosis system is shown in Figure 8.

The system can be divided into three functional modules: real-time module, data processing module, and network transmission module. The functional module design diagram is shown in Figure 9.

After obtaining the above system model, the effect of the system model is verified, and the system structure is constructed through computer simulation, and the inverter image recognition and fault diagnosis effects of the system in this article are verified, and the results shown in Tables 1 and 2 are obtained.

From the above research, it can be seen that the electric locomotive inverter diagnosis system based on the

Table 1: Image recognition effect of electric locomotive inverter diagnosis system based on adversarial neural network.

Number	Image identification
1	91.05
2	89.38
3	88.04
4	93.08
5	92.76
6	91.12
7	87.84
8	87.04
9	91.50
10	89.30
11	87.12
12	92.74
13	89.09
14	89.45
15	88.52
16	88.22
17	89.04
18	93.57
19	89.62
20	88.61
21	89.34
22	93.81
23	93.51
24	90.52
25	90.40
26	92.35
27	87.53
28	87.71
29	93.55
30	87.37
31	93.05
32	92.64
33	88.22
34	93.70
35	87.99
36	92.73
37	93.21
38	89.81
39	89.72
40	93.53
41	91.63
42	93.86
43	91.75
44	90.51
45	90.15
46	89.74
47	91.50
48	92.37
49	90.00
50	90.24
51	87.02
52	88.68
53	91.70
54	90.89
55	87.12
56	89.24
57	91.74
58	93.80
59	92.63
60	91.13

Table 2: Fault diagnosis effect of electric locomotive inverter diagnosis system based on adversarial neural network.

Number	Troubleshooting
1	88.52
2	73.35
3	76.80
4	81.33
5	74.68
6	73.03
7	84.10
8	74.50
9	76.14
10	75.11
11	77.12
12	77.14
13	84.14
14	78.97
15	71.55
16	79.53
17	74.54
18	79.83
19	80.24
20	71.23
21	86.85
22	75.94
23	78.62
24	78.88
25	79.77
26	75.54
27	86.27
28	74.06
29	81.43
30	86.93
31	77.21
32	85.88
33	74.03
34	85.92
35	75.74
36	83.62
37	82.98
38	84.23
39	80.39
40	76.79
41	79.02
42	76.71
43	81.35
44	81.65
45	76.28
46	79.32
47	73.11
48	71.89
49	85.87
50	84.12
51	86.74
52	75.31
53	73.40
54	76.97
55	78.09
56	71.72
57	75.70
58	72.25
59	77.66
60	85.75

Hindawi
Security and Communication Networks
Volume 2024, Article ID 9829563, 1 page
https://doi.org/10.1155/2024/9829563

Retraction

Retracted: Prediction and Analysis of the Physical Test Scores Based on BP Neural Network and Principal Component Analysis Algorithm

Security and Communication Networks

Received 8 January 2024; Accepted 8 January 2024; Published 9 January 2024

This article has been retracted by Hindawi following an investigation undertaken by the publisher [1]. This investigation has uncovered evidence of one or more of the following indicators of systematic manipulation of the publication process:

(1) Discrepancies in scope
(2) Discrepancies in the description of the research reported
(3) Discrepancies between the availability of data and the research described
(4) Inappropriate citations
(5) Incoherent, meaningless and/or irrelevant content included in the article
(6) Manipulated or compromised peer review

The presence of these indicators undermines our confidence in the integrity of the article's content and we cannot, therefore, vouch for its reliability. Please note that this notice is intended solely to alert readers that the content of this article is unreliable. We have not investigated whether authors were aware of or involved in the systematic manipulation of the publication process.

In addition, our investigation has also shown that one or more of the following human-subject reporting requirements has not been met in this article: ethical approval by an Institutional Review Board (IRB) committee or equivalent, patient/participant consent to participate, and/or agreement to publish patient/participant details (where relevant).

Wiley and Hindawi regrets that the usual quality checks did not identify these issues before publication and have since put additional measures in place to safeguard research integrity.

We wish to credit our own Research Integrity and Research Publishing teams and anonymous and named external researchers and research integrity experts for contributing to this investigation.

The corresponding author, as the representative of all authors, has been given the opportunity to register their agreement or disagreement to this retraction. We have kept a record of any response received.

References

[1] J. Qu, "Prediction and Analysis of the Physical Test Scores Based on BP Neural Network and Principal Component Analysis Algorithm," *Security and Communication Networks*, vol. 2022, Article ID 5210810, 12 pages, 2022.

Hindawi
Security and Communication Networks
Volume 2022, Article ID 5210810, 12 pages
https://doi.org/10.1155/2022/5210810

Research Article

Prediction and Analysis of the Physical Test Scores Based on BP Neural Network and Principal Component Analysis Algorithm

Jiale Qu

Sports Institute, Inner Mongolia University, Hohhot 010021, China

Correspondence should be addressed to Jiale Qu; 111983018@imu.edu.cn

Received 4 April 2022; Revised 27 April 2022; Accepted 6 May 2022; Published 31 May 2022

Academic Editor: Fang Liu

College students' physical fitness test can comprehensively evaluate students' physical health level from many aspects such as students' body shape, quality, function, and sports ability. Through the analysis and prediction of college students' physical fitness test results, it can be used to understand the actual physical quality of college students, formulate the evaluation standard of students' physical health level, and assist physical education teachers to formulate reasonable teaching plans. For students with different physical quality, different training plans can be formulated to improve their actual physical quality. Aiming at this background, this paper puts forward a method based on BP neural network and principal component analysis algorithm of college students test score prediction algorithm, the BP neural network, and principal component analysis of machine learning algorithm successfully applied to physical test comprehensive performance prediction, implements the college students test transcript accurate prediction, and can effectively assist PE teachers to develop reasonable teaching plan. For students with different physical quality, different training plans can be formulated to improve their actual physical quality.

1. Introduction

In 2019, the arrival of novel coronavirus made us deeply aware of the importance of the human self-immune system. Strengthening physical exercise to improve the own immunity can effectively prevent the invasion of bacteria and viruses. The novel coronavirus outbreak is a warning to all of us humans, especially the younger generation of college students today. With good physical quality, people can put more energy on daily life, study, and work, which is also the basis of contemporary college students' study and life, but also one of the necessary elements to ensure the all-round development of students. College students are the future pillars of our country, and whether they can grow up healthily is related to the future of our nation. The Ministry of Education requires colleges and universities to carry out physical fitness tests for college students every year and report the test data, so as to have a comprehensive understanding of the physical development of college students today [1].

College students' physical fitness test will comprehensively evaluate students' physical health level from the aspects of students' physical form, quality, function, and sports ability, which is a very effective educational means to promote the healthy development of students' physical fitness and encourage students to actively carry out physical exercise and also the evaluation standard of students' physical health level. As the main base for cultivating high-quality talents, colleges and universities are facing a harsh test [2]. It is an important task of physical education teaching in colleges and universities to cultivate college students' interest in physical exercise and make them participate in sports consciously and move forward to lifelong sports. At present, exercise has become an important measure used in many countries to improve the physical health level, and maintaining a moderate amount of daily exercise is beneficial to the health of people of all age groups. Exercise can effectively enhance physical fitness and improve psychological quality; at the same time the human muscles will be more developed and more powerful. Colleges and universities have always paid too much attention to the intellectual development factors of college students and ignored their physical condition. With the improvement of people's daily living standards, the material life of college students has become richer, thus with lack of exercise, and some students'

physical quality has decreased. Unideal physical quality will not only affect the study and life of college students, but also affect their future work in the society.

The analysis and prediction of the physical fitness test results can be used to understand the actual physical condition of college students. The annual physical fitness test can make students deeply aware of their own physical fitness changes. Physical fitness test can make college students deeply realize the importance of physical exercise and encourage them to strengthen exercise to improve their physical health level. Physical fitness test is an important means for teachers to understand students' physical quality. The results of college students' physical fitness test can help the sports management department of universities to set up scientific and reasonable courses and develop the most effective training mechanism. Therefore, this paper uses the physical fitness test data over the years for analysis, and the analysis results are used to assist physical education teachers to develop reasonable teaching plans. For students with different physical quality, different training plans can be formulated to improve their actual physical quality.

Based on this background, in order to realize the prediction and analysis of college students' physical education test scores, this paper proposes an algorithm combining BP neural network and principal component analysis (PCA), which establishes a dynamic model, and realizes the analysis and prediction of physical education test scores. The full text is divided into four chapters. Chapter 1 introduces the research background and research necessity and the chapter arrangement of the paper; Chapter 2 mainly analyzes some research work on the test and analysis of sports performance. The feasibility of BP neural network and principal component analysis in sports exercise test was also discussed; Chapter 3 mainly introduces the theory and modeling process of BP neural network and principal component analysis. A model and algorithm based on BP neural network and principal component analysis algorithm is proposed; Chapter 4 mainly involves the specific implementation of the model and algorithms proposed in Chapter 3 and applied to the actual physical test performance analysis and prediction, validation of the algorithm, analyzing the experimental results and the errors, and arrival at a conclusion. The experiments show that the BP neural network and principal component analysis algorithm can realize the analysis and prediction of body test results, are consistent with the reality, and have good results.

2. State of the Art

Today's society is full of challenges and competition, so the society has put forward higher requirements for the basic quality of talents. There are always many problems in how to cultivate high-quality talents with all-round development in colleges and universities [2]. The important task of physical education in colleges and universities is to cultivate the interest of college students through physical exercise, so that they can consciously participate in sports and maintain it for life. In many countries, exercise has become an important tool to improve physical health.

The study of how to enhance students' physical quality is a great project by all countries around the world. The United States is a very developed country in science, technology, and economy, and it is also one of the earliest countries in the world to pay attention to the study of national physical fitness. In the mid-twentieth century, the AAHPER Association took the lead in developing an efficient physical education evaluation index, adding four items: standing long jump, sit-up, softball throwing, and 50-meter return running to the student physical fitness test. The physical fitness study in the United States combines the physical education courses in colleges and universities and implements a very distinctive fitness program in every school. Japan is the country with the most complete and earliest survey and research data on adolescent physique. Since 1898, Japan has accumulated a large number of data and conducted research. Japan is recognized as one of the more authoritative countries in the world in the field of testing and evaluation of adolescent physical fitness. The Japanese people are leading the way in studying adolescent body shape and bone development, combining their physical fitness with study, life, and work. In particular, Europe has established a committee called "urofield," whose main task is to coordinate the test management of student physical fitness in various countries, check the results of each test, and recommend the whole process of the test and the final results of the test [3]. British physical monitoring in colleges and universities started later than United States and Japan, but its monitoring level has reached the world advanced level, especially in single project testing. The use of national sports monitoring standards, the students' body composition and exercise ability evaluation and monitoring, has reached the degree of automation. The Australian Football League has successfully applied the neural network algorithm in machine learning to the selection of tournament players, predicting the athletic ability of the participants, including anthropometric, mental, and skill estimation, and selecting the best players, thus increasing the possibility of competition victory [4]. The results of this study show that neural networks can better assist recruitment managers to identify talents. Machine learning algorithms have been successfully applied to NBA games to collect historical data of games and predict whether the basketball team can win according to the results of data analysis. It can effectively avoid accidents and adjust the order of game players in time, so as to increase the possibility of victory [5]. Wang platinum et al. used BP neural network algorithm to estimate the development status of folk custom sports events in some parts of China from two aspects of male and female characteristics. The results show that neural network can better predict the future development of traditional sports [6]. Wang Ji'an usage of BP neural network algorithm is relatively stronger, self-fault tolerance and self-training learning ability as well as good advantages, are useful in constructing model, athletes performance prediction, neural network model for sports performance prediction model research provides extremely extensive development space, and neural network in prediction and analysis is very popular [7]. Kerstin Witte uses principal component analysis to study the sports coordination of

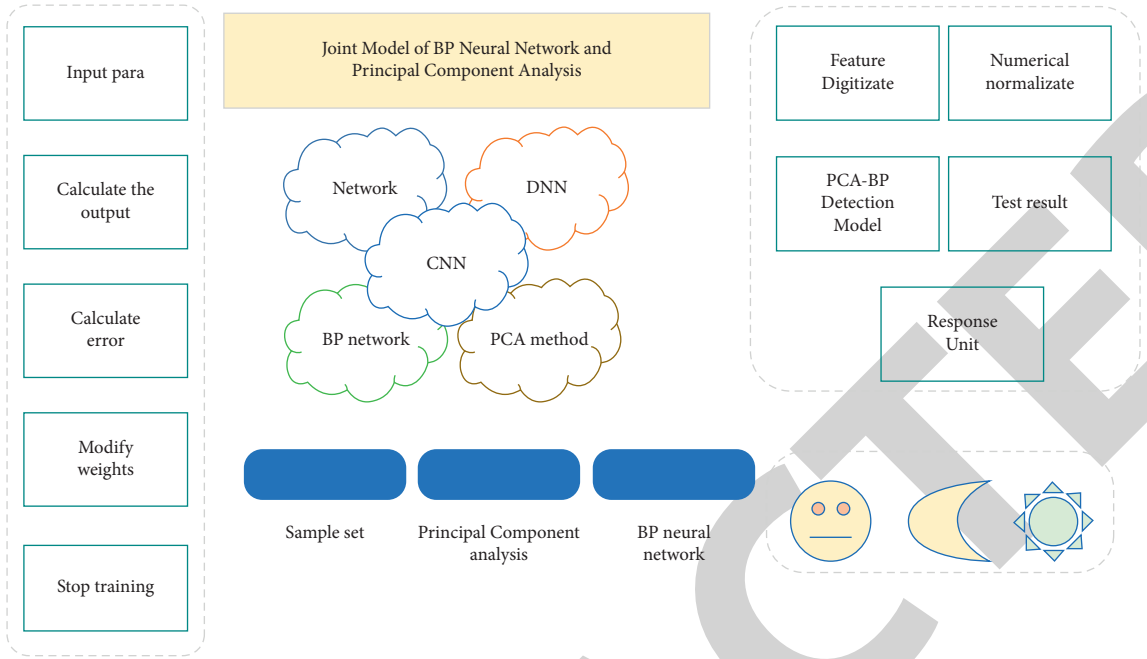


Figure 1: Flowchart of PCA methods.

rehabilitation, triathlon, and horse riding in sports science [8]. The results show that the principal component analysis can effectively characterize people's coordination during movement in a whole. The principal component analysis algorithm is used to decompose the complex movement mode of skiing into the main movement components, determine the standard posture and main movements of the skiers, and assist the coach in training and preaching [9, 10].

To sum up, all countries attach great importance to the study of college students' physique. College students are the future and hope of a country, and their physical condition is a problem that we should pay common attention to. The analysis and research of machine learning data in the field of sports are widely involved both at home and abroad, which provides great help to people's life, physical health, and national competitions. In order to analyze and deal with the historical data of college students' physical fitness test scores, classify management students and put forward targeted training plans suitable for students' own physical quality, so as to assist physical education teachers to better develop reasonable teaching plans. This paper analyzes the historical data of the current college students' sports performance test, draws samples, and uses radar maps to visualized data, which intuitively reflects the distribution of each student's scores. Then, the correlation analysis and principal component analysis methods in the machine learning algorithm are used to preprocess the physical fitness test data, eliminate the mutual influence between the attributes of the data, and cover the original attribute information with the new principal component attributes, and the analysis process is simplified and the prediction time is saved. Finally, the BP neural network algorithm was used to establish the college student sports performance prediction model, and the model was used for performance analysis and prediction, so that the physical fitness test data over the years could play a greater role and provide better help for teachers to make teaching plans.

3. Methodology

3.1. Principal Component Analysis Method. One of the biggest challenges in data processing is data multiple-complexity. Principal component analysis is a commonly used technique used to reduce the dimensionality of datasets to explore and simplify some kind of complex relationship between variables. Principal component analysis was first proposed by Pearson in 1901 and developed by Hotelling in 1933, with the main idea being to represent the majority of the original variables with a few components via dimensionality reduction techniques [11]. The flow of the algorithm using the principal component analysis is shown in Figure 1.

It can transform multiple original variables with strongly correlated properties into several unrelated variables, and the calculated several variables without correlation are the main components [12]. The goal of the principal component is to use a smaller set of unrelated variables instead of a large number of correlated variables, while retaining the raw data information as much as possible. The principal component is a linear combination of the original variables, whose model is shown in Figure 2.

The principal component reflects most of the characteristics of the original variables and can remove strong correlations between the original variables. The principal component is a linear combination of the original variables, with the first one explaining the most variance to the first known variable, while the second one ranks second for the original variable variance interpretation and is orthogonal

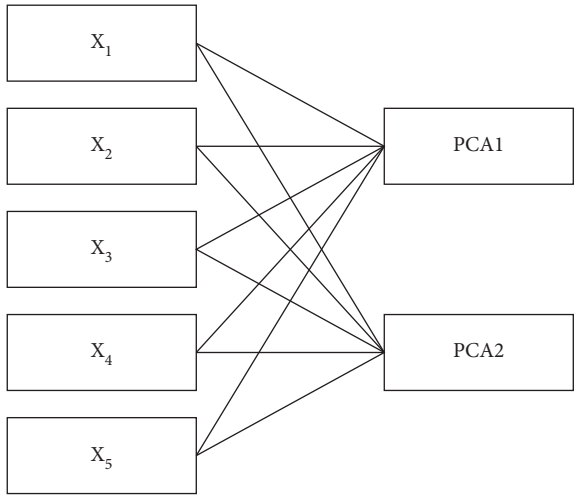


Figure 2: Methods and model for principal component analysis.

to the first principal component, that is, completely irrelevant [13]. And so on, the remaining principal components are all related in orthogonal relationships. It is assumed that there are P variables in the original data, respectively, $x_1, x_2, \ldots, x_p$, and the new p mutually independent principal component variables are formed through linear combination. The mathematical model expression is as follows:

$$\begin{cases} y_1 = u_{11}x_1 + u_{12}x_2 + \ldots + u_{1i}x_i + \ldots + u_{1p}x_p \\ y_2 = u_{21}x_1 + u_{22}x_2 + \ldots + u_{2i}x_i + \ldots + u_{2p}x_p \\ \vdots \\ y_i = u_{i1}x_1 + u_{i2}x_2 + \ldots + u_{ii}x_i + \ldots + u_{ip}x_p \\ \vdots \\ y_p = u_{p1}x_1 + u_{p2}x_2 + \ldots + u_{pi}x_i + \ldots + u_{pp}x_p \end{cases}. \tag{1}$$

The model changes to the matrix form as shown in formula:

$$y = \begin{bmatrix} u_{11} & u_{12} & \cdots & u_{1p} \\ u_{21} & u_{22} & \cdots & u_{2p} \\ \vdots & \vdots & \vdots & \vdots \\ u_{p1} & u_{p2} & \cdots & u_{pp} \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_p \end{bmatrix} = Ux. \tag{2}$$

The sum of the squares of the principal component coefficient is 1, as shown in formula:

$$u_{i1}^2 + u_{i2}^2 + \ldots + u_{ip}^2 = 1. \tag{3}$$

Next, in order to obtain the principal component value of y_p, calculate the principal component coefficient. The covariance matrix is first calculated from the raw data as shown in equation

$$\text{cov} = \frac{1}{n}\sum_{i=1}^{n}(x_1 - \overline{x})(y_1 - \overline{y}). \tag{4}$$

Since the data has been normalized processed, the variance of the original data s^2 should be one. See formula

$$s^2 = \frac{1}{n}\sum_{i=1}^{n}(x_1 - \overline{x})^2 = 1. \tag{5}$$

Change formula (5) to (6),

$$\sum_{i=1}^{n}(x_1 - \overline{x})^2 = ns^2 = 1. \tag{6}$$

The formula is

$$r = \frac{\sum_{i=1}^{n}(x_i - \overline{x})(y_i - \overline{y})}{\sqrt{\sum_{i=1}^{n}(x_1 - \overline{x})^2}\sqrt{\sum_{i=1}^{n}(y_i - \overline{y})^2}} = \frac{\sum_{i=1}^{n}(x_i - \overline{x})(y_i - \overline{y})}{n} = \text{cov}. \tag{7}$$

From formula (7), the correlation coefficient matrix of the original data is actually equivalent to the covariance matrix. The eigenvalues of the covariance matrix represent the variance of the principal components, while the eigenvalues and principal component coefficients μ_{pp} are calculated by the correlation coefficient matrix and the eigenvalues y are calculated by $y = x\mu^T$. Theoretically according to the principal component contribution to choose less principal components instead of the original data, generally selected contribution is 90% of the number of principal components. This will inevitably lead to missing data, resulting in inaccurate experimental results. So in this paper, we will choose the same original number of principal components, so we will not throw the original data information and also can remove the strong correlation between the original variables on the model training. Next, the neural network model was established using eight unrelated new variables, which increased the persuasion of the model accuracy, while excluding the influence of the data factors on the model establishment and parameter optimization.

3.2. BP Neural Network. Artificial neural networks, also known as neural networks, have originated in neurophysiology [14]. Neural network is composed of a large number of neural cells, which is a simplified and abstract with simulation of the human brain. Neural network is a kind of machine learning intelligent algorithm to imitate the brain; it has its own unique nonlinear information processing ability, which can be stored in the neural network through adaptive and autonomous learning for information, repeated learning and training, applied in intelligent control, image recognition, combination optimization computing, and speech recognition, etc. Neural networks contain many types, such as perceptron, BP neural network, radial base network, self-organized mapping network, etc.

Among the numerous models of neural networks, the BP neural network model is the most widely used representative neural network. It is a supervised learning algorithm based on the error-square MSE as the objective function and a multilayered network with weights trained on the nonlinear differentiable function [15]. The basic structure of the BP neural network is shown in Figure 3.

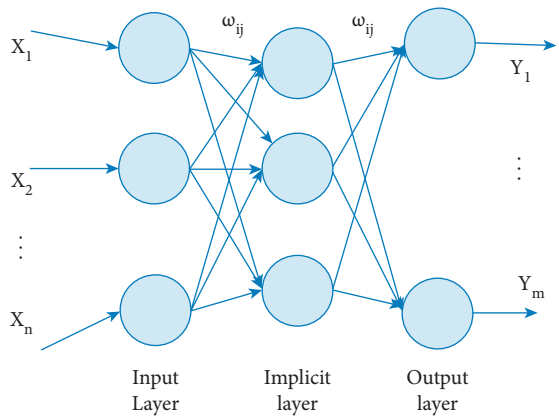


Figure 3: B P Neural network basic model structure.

The BP neural network mainly consists of three parts: input layer, implied layer, and output layer, where X_i refers to the input value of the BP neural network, W_{ij} and W_{jk} are the weight of the neural network, and Y_i refers to the output value of the BP neural network. It can also be seen from the above figures that, in the BP neural network model, the network input value is taken as the independent variable of the function, and the network output value is taken as the dependent variable of the function.

The algorithm flow of BP neural network is shown in the figure, mainly including forward propagation and backpropagation. The specific implementation process is as follows.

(1) Forward propagation of the data:

Internet patterns between neural networks are formed by the interconnections of neurons, and the initial weights between each connection are randomly assigned by the computer. The forward propagation stage of the data signal refers to the process of the original data signal passing through the implied layer from the input layer to the output layer; that is, the output of the upper node serves as the input of the lower node.

As shown in Figure 4, each neuron cell has a corresponding computational weight. The output value of the input layer in the implied layer is obtained by the input value, connection weight, and threshold value, and the calculation method is shown in formula

$$\text{net1}_k = \sum_{i=1}^{n} w_{ik} y_i + b_k = w_{1k} y_1 + w_{2k} y_2 + \ldots w_{nk} y_n + b_k. \tag{8}$$

During the process of prediction, applying the activation function processing can obtain better prediction accuracy. There are many kinds of activation functions, such as step function, Sigmoid function, tanh function, and ReLU function. This paper uses the Sigmoid function to activate the output information. The output value of the input layer is activated by the activation function to (f (net1) k). The implied layer family is obtained by formula

$$z_k = f\left(\text{net1}_k\right) = \frac{1}{1 + \exp\left(-\text{net1}_k\right)}. \tag{9}$$

Next, the implied layer data acts as the input layer to pass the data to the output layer. The output value net2_j is the connection weight v_{kj} between the hidden layer value and the hidden layer and the output layer. The weighted sum plus the threshold is still obtained as shown in formula

$$\text{net2}_j = \sum_{k=1}^{n} v_{kj} z_k + b_j = v_{1j} z_1 + v_{2j} z_2 + \ldots + v_{nj} z_n + b_j. \tag{10}$$

Formula (11) activates the output value to obtain the data for the final output layer.

$$z_k = f\left(\text{net2}_j\right) = \frac{1}{1 + \exp\left(-\text{net2}_j\right)}. \tag{11}$$

(2) Error backpropagation

When the signal is transmitted to the output layer, the error function is used to detect whether the training process of the neural network ends. The neural network is stopped by satisfying the error function limit value or reaching the set maximum number of iterations. Training is stopped when the output error function is less than the predetermined value. If the condition is not met, the error is backpropagated. The error function (E) is used to measure the error size between the actual output code and the desired output O_j, as shown in formula

$$E = \frac{1}{2}(d - o)^2 = \frac{1}{2}\sum_{j=1}^{n}\left(d_j - o_j\right)^2. \tag{12}$$

The error signal from each layer was used to adjust the weights of connections between neurons. Equation (13) simulates the process of error backpropagation.

$$E = \frac{1}{2}\sum_{j=1}^{n}\left(d_j - o_j\right)^2 = \frac{1}{2}\sum_{j=1}^{n}\left(d_j - f\left(\sum_{k=1}^{n} v_{kj} z_k\right)\right)^2. \tag{13}$$

The error decreases along the gradient by constantly adjusting the connection weights and thresholds. After calculating the change value of the weight connection value Δv_{kj} between the implied layer and the output layer, update each connection weight and see formulas (14) and (15).

$$\Delta v_{kj} = -\eta \frac{\partial E}{\partial \text{net2}_j} z_k. \tag{14}$$

$$v_{kj} = v_{kj} + \Delta v_{kj}. \tag{15}$$

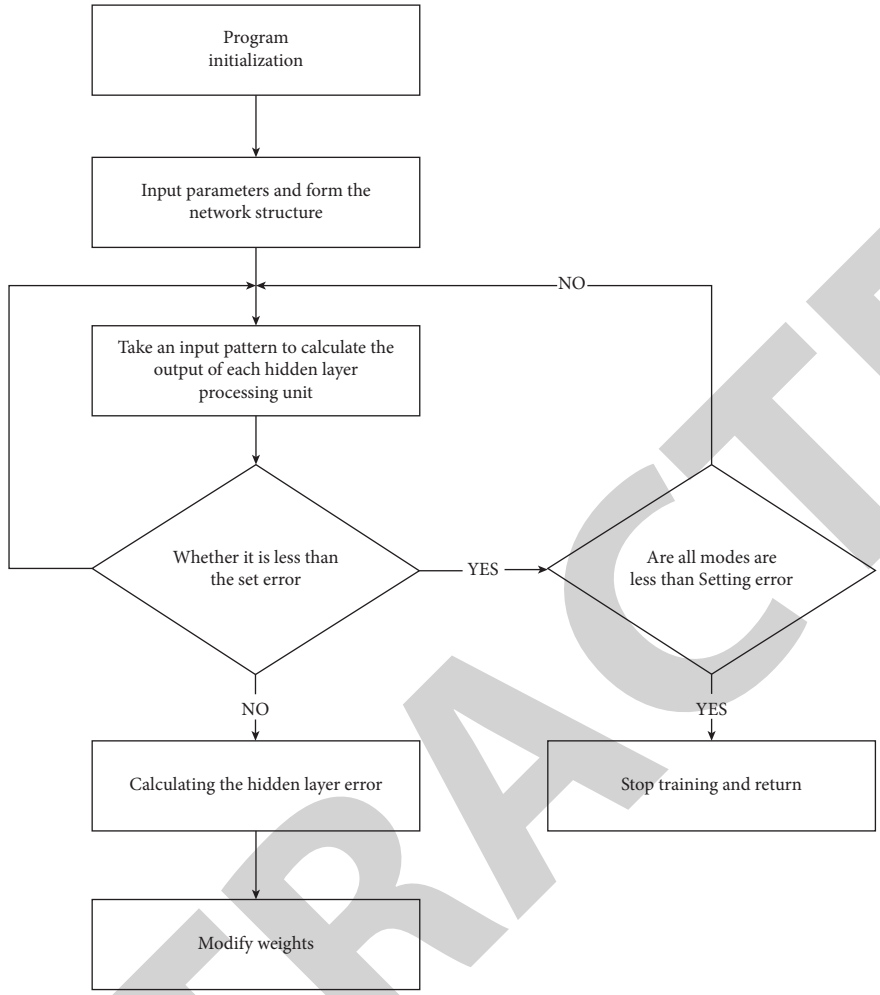


Figure 4: Training process of the BP neural network.

Adjust the connection weight between the input layer and the hidden layer as above. When all weights are readjusted, the signal forward propagation will continue. When the model reaches the convergence criterion, the training is stopped, the model is established, and the model parameters are adjusted to optimize the model. The established model is used to predict the physical fitness test data, calculate the error size between the predicted value and the actual value to verify the feasibility of the model, and then apply the model.

3.3. Predictive Model Based on the BP Neural Network and Principal Component Analysis Algorithm. Physical fitness test data were preprocessed and standardized to eliminate strong correlations between the data using principal component analysis. After transforming the raw data by using the principal component analysis method, the BP neural network is used to build the model. The overall process is as shown in Figure 5.

Before selecting the actual results of college students' sports test as the original data and using principal component analysis, we need to standardize the original data to eliminate the impact of different dimensions of variables on the analysis results. We then chose the first few principal components where the cumulative variance contribution is no less than 85% after dimensionality reduction as a new learning sample of the neural network.

4. Result Analysis and Discussion

4.1. Overview of the Physical Fitness Test Data. The physical fitness test dataset used in this institute is composed of students in the 2016–2019 academic year. The dataset contains the physical fitness test records of all students in the university within four years, including the measurement results of instruments and equipment, the score of individual tests, additional points, and the final comprehensive score, and the total data of more than 80,000 pieces.

The analysis of the dataset used can be performed by using the data visualization analysis technology, and one of the sampled student information can be represented in Figure 6, and from the figure, the actual physical condition of the student can be even more clearly observed.

The physical fitness tests in the dataset are as follows:

(1) Height (H) and weight (W): Height and weight are the required basic items in the physical fitness test.

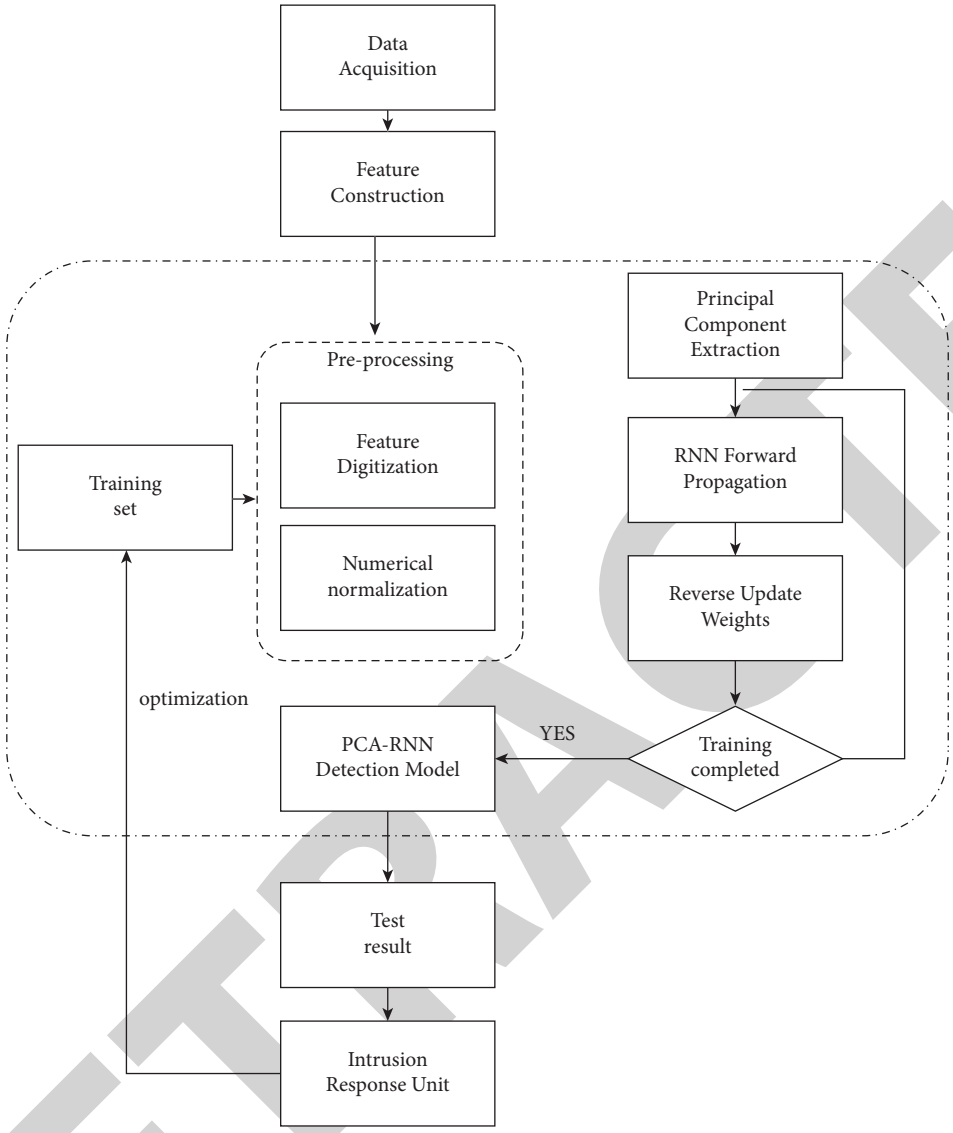


Figure 5: Physical measurement analysis and prediction model based on principal component analysis and BP neural network.

These two tests can judge whether a person's growth and development tend to be normal. The change of human body size is one of the important criteria reflecting the health of a person's basic body.

(2) Spirometry (VC): Spirometry refers to the maximum deep breath after the maximum deep inhalation. This process represents the maximum functional activity of human lungs at a time and reflects the potential ability of respiratory function in the lung. This activity volume is an important indicator used to evaluate the function of human respiratory system.

(3) 50-meter sprint (S): 50-meter sprint is a common international "displacement speed" test project. It measures students' physical speed quality through short distance and high intensity running, including movement speed and reaction speed.

(4) Standing long jump (SLJ): Standing long jump is a long jump that does not start from a standing position without any support run. This process is mainly used to measure the explosive force of the lower limb muscles of the human body when jumping forward. The explosive force of the human body depends on the strength of the human body itself, which is one of the inaccessible factors in daily life.

(5) Sitting forward flexion (SR): Sitting anterior flexion is used to measure the maximum range of activity of the trunk, waist, and other joints of the human body at rest. The measurement is mainly used to reflect the elasticity and extension of the body's joints, muscles, and ligaments, as well as the level of body flexibility.

(6) Endurance items (SP): Endurance items are measured in middle and long distance running. Due to the different physique of boys and girls, the project distance measurement is different, including 1000 meters for boys and 800 meters for girls. Middle and long distance running is a kind of exercise mode to cultivate students' endurance quality, but also an aerobic metabolism

Figure 6: Drawing four-year test data for a sample of students. (a) Students with perfect grades. (b) Students with individual weaknesses. (c) Students reach to the passing score nearly. (d) Students with lowest scores.

project, which is mainly used to test students' endurance and body oxygen supply function.

(7) Strength project (PP): Strength test is the number of corresponding items completed in one minute. For the difference of physical requirements between male and female students, boys conduct pull-up project, while girls perform sit-up project. Both pull-ups and sit-ups are methods used to measure muscle endurance and strength. The measured results of the strength test can provide a better understanding of the students' physical muscle strength and endurance.

4.2. Implementation of the Body Measurement Algorithm Based on the BP Neural Network and Principal Component Analysis. The 2016 physical fitness test data were selected to build the model, with 80% of the student sample as training set and the remaining 20% as test set for model evaluation. The scoring criteria and methods are different for boys and girls, so the test data were separated to build separate models for prediction. Continuous tuning optimized the model using 80% of the training set, and the final model parameters are shown in Table 1.

Table 1: Physical fitness test predicted model parameters.

Parameter name	Parameter values
Number of neurons in the input layer	8
Number of neurons in the output layer	1
Number of neurons in the hidden layer	11
Threshold	0.005
Learning rate	0.1
Maximum iteration number	1.0*e*10
Training algorithm	rprop+
Error function	sse
Activation function	Logistic

As shown in Table 1, the threshold serves as the conditional value for training stopping, which indicates the predetermined value in the error function. The maximum

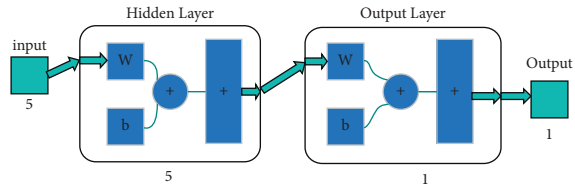


Figure 7: The Matlab neural network toolbox.

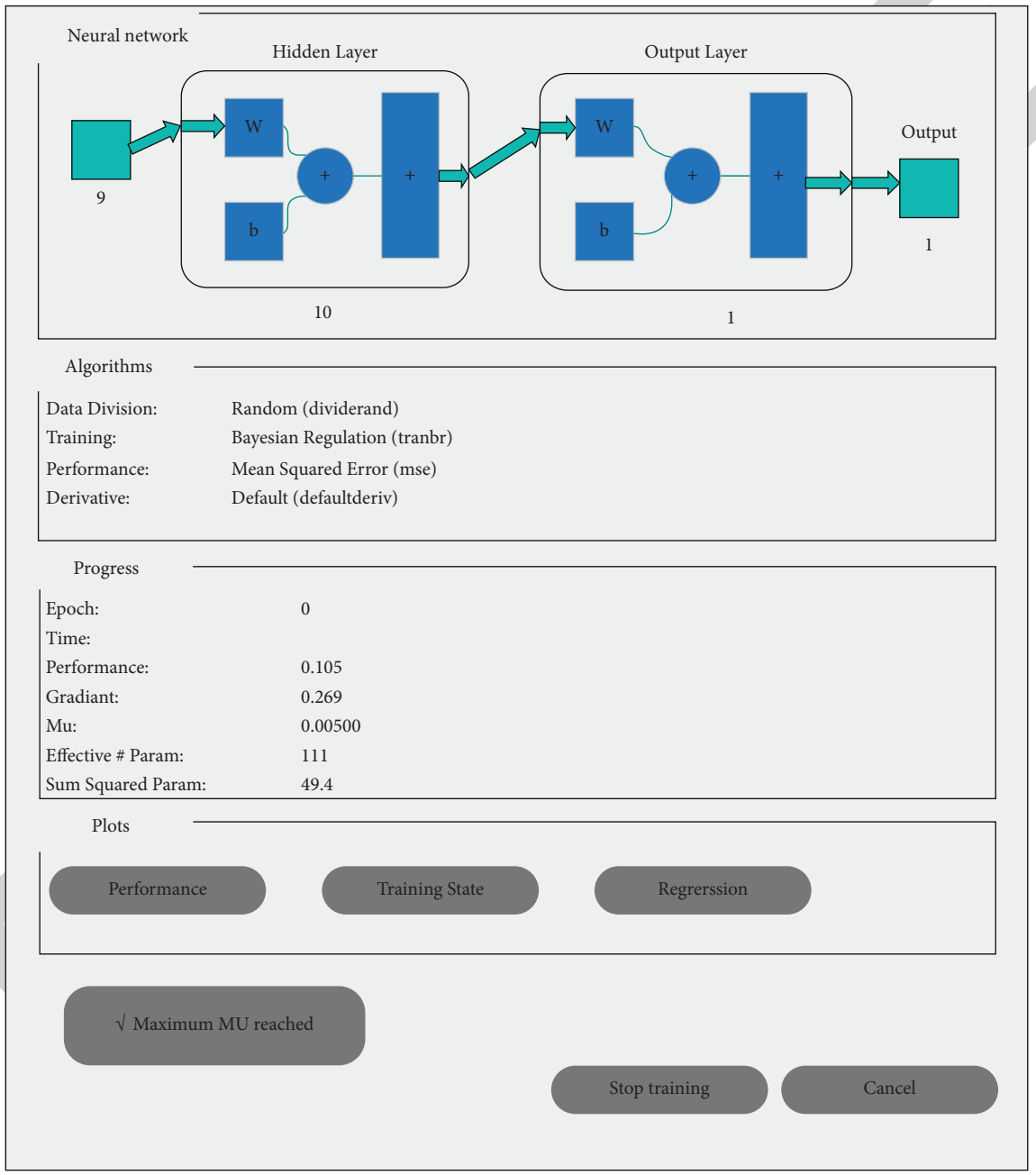


Figure 8: Neural network training process.

number of iterations forces the training to stop when the predetermined value is never reached and the iteration cannot stop. The algorithm "rprop+" used for training is a weighted error backpropagation algorithm, namely, the BP neural network algorithm. The error function "SSE" was used to calculate the magnitude of the error at the end of the forward propagation. The activation function uses the parameter "logistic" for the Sigmoid activation function. The number of neurons in the hidden layer is determined by the mean square error (MSE) and formula

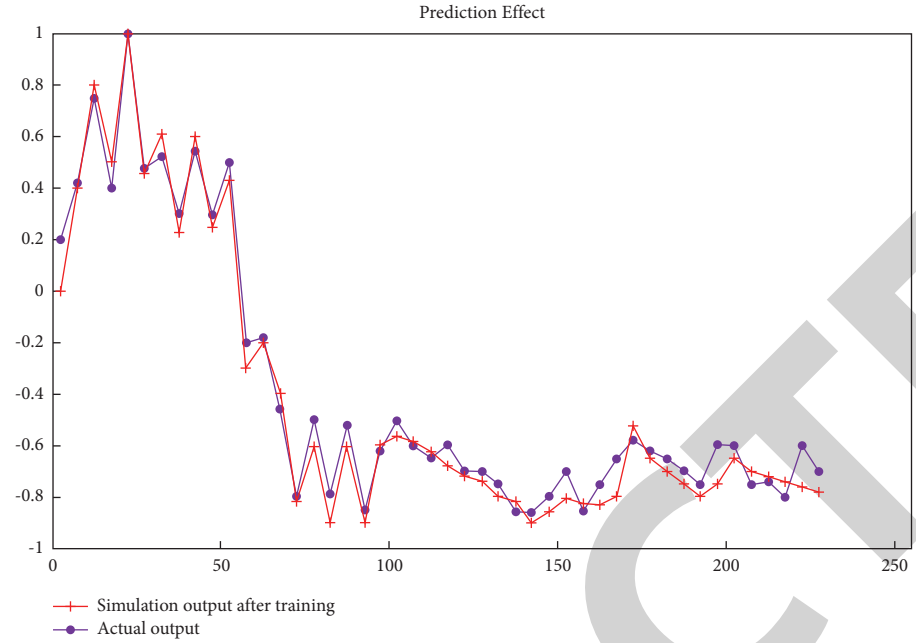


Figure 9: Neural network training fitting effect.

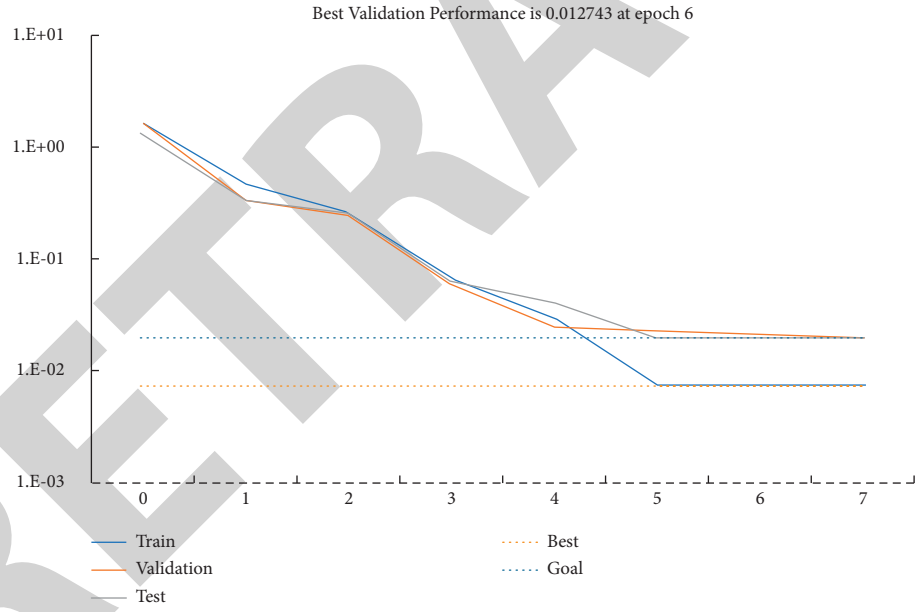


Figure 10: Performance curves for the BP neural network training.

$$h = \sqrt{m+n} + a. \tag{16}$$

m is the number of input neurons, h is the number of output neurons, and a is a constant ranging from 1 to 10, so the value of the number of hidden layers h ranges from 4 to 13. Therefore, the model building process is conducted for the number of different hidden layers, and the mean square error (MSE) is used to compare the accuracy of the model prediction. Mean square error (MSE) is calculated by absolute error (AE), and the absolute error is the difference between the actual output value and the model predicted value as shown in formulas (17) and (18).

$$AE = o_i - o_j. \tag{17}$$

$$\text{MSE} = \frac{1}{n}\sum_{i=1}^{n}\left(o_i - o_j\right)^2. \tag{18}$$

Mean square error (MSE) method effectively avoids the problem that positive and negative errors cannot be added and can be used to evaluate the accuracy of model prediction. The smaller the value of MSE, the stronger the ability of the model to fit the experimental data, but the value of MSE cannot be 0, which proves that our established model is overfitted. Through the size of MSE under

the model of each number of hidden layers, the number of neurons in the hidden layer was finally determined to be 11. The setup of the neural network using Matlab is shown in Figure 7, and the training process is shown in Figure 8.

Then, 80% of the data after the principal component analysis was brought into the function to build the neural network model and evaluate the accuracy of the model using the data from the test set. The test set data not involved in the model training process were brought into the model for prediction, respectively, and finally the prediction results of male and female students were combined to observe the prediction performance of the overall model. After sampling individual samples to evaluate the test results, the model prediction performance is further observed from the overall data. The visual results show that the model prediction performance proposed in this paper is very high, which has certain practical value for the prediction of comprehensive physical fitness test performance in the future.

The sample of 40 students was randomly selected in the test set of the 2016 data, and the difference between the actual value of these 40 students and the predicted value of the model is shown in Figure 9. Shown are the predicted versus actual values of a random sample of 40 students in the test set. The real line in the figure is the actual value, and the dashed line is the predicted value. It is obvious that these two lines have a high coincidence rate, and only individual samples can see the obvious error. The results show that the physical fitness test of the prediction model is very accurate and has a good performance.

Figure 10 shows the performance curve of the neural network training, indicating the variance changes. After several cycles, the network achieves convergence with the mean variance of 0.0070188 and 0.0098638, which are less than the set expected error target of 0.001. The whole curve drops faster, which indicates the appropriate learning rate. Error can reflect the reliability of the prediction results, and the absolute error (AE) value close to 0 means that the prediction is very accurate.

5. Conclusion

College students' physical fitness test mainly evaluates their physical condition and training effect through the test results of various items, which is a very sound and effective strategy and can urge college students to actively participate in sports training. College PE teachers can provide students with the most scientific training plan according to the test results, so as to continuously enhance their own physical fitness. In order to better analyze the physical education test results of college students and to predict them, this paper proposes a comprehensive performance prediction model of physical fitness test to successfully apply machine learning algorithms such as BP neural network and principal component analysis to the prediction of physical fitness test. The performance prediction model to predict the comprehensive performance reduces the performance calculation time and solves the problem of inconsistent scoring standards due to manual calculation over the years. Compared with the traditional calculation method, the physical fitness test results play greatest value. Compared with the annual test results of the student, the child labor can reflect whether the student's physical fitness is improved and whether the corresponding training plan provided by the teacher is reasonable and effective. At the same time, it provides guidance for the adjustment of the training plan and the teachers' scientific formulation of the teaching plan. The results show that the comprehensive performance prediction model is highly accurate and can serve the physical education teaching very well.

Data Availability

The labeled datasets used to support the findings of this study are available from the author upon request.

Conflicts of Interest

The author declares no conflicts of interest.

Acknowledgments

This work was supported by the Inner Mongolia University.

References

[1] B. Zhao, "Performance analysis and prediction of the world's top male athletes in Decathlon," *Sports Culture Guide*, vol. 3, p. 4, 2013.

[2] F. Wang, "Research and analysis of physical fitness test management system of baoshan university," *Yunnan University*, vol. 3, pp. 76–79, 2017.

[3] F. Zhe, *Research on European Sports Development Mode Reform*, East China Normal University, Shanghai, China, 2013.

[4] Duncan, "Data mining in sports," 2010.

[5] B. Loeffelholz, E. Bednar, and K. W. Bauer, "Predicting NBA games using neural networks," *Journal of Quantitative Analysis in Sports*, vol. 5, no. 1, p. 7, 2009.

[6] B. Wang, X. Li, and Y. Sun, "BP neural network model-based urbanization process traditional sports cultural development e," *The Open Cybernetics & Systemics Journal*, vol. 9, no. 1, pp. 3005–3010, 2015.

[7] J. Zhou, W. U. Guilin, and Y. U. Shengsheng, "Algorithm of BP neural network-based face detection," *Computer Engineering*, vol. 30, 2004.

[8] K. Witte, N. Ganter, C. Baumgart, and C. Peham, "Applying a principal component analysis to movement coordination in sport," *Mathematical and Computer Modelling of Dynamical Systems*, vol. 16, no. 5, pp. 477–488, 2010.

[9] B. Natàlia, G. Jacob, J. Casimiro et al., "Cardiorespiratory coordination after training and detraining: a principal component analysis approach," *Frontiers in Physiology*, vol. 7, 2016.

[10] P. Federolf, R. Reid, M. Gilgien, P. Haugen, and G. Smith, "The application of principal component analysis to quantify technique in sports," *Scandinavian Journal of Medicine & Science in Sports*, vol. 24, no. 3, pp. 491–499, 2014.

Hindawi
Security and Communication Networks
Volume 2024, Article ID 9850571, 1 page
https://doi.org/10.1155/2024/9850571

Retraction

Retracted: Network Interconnection Security Buffer Technology for Power Monitoring System

Security and Communication Networks

Received 8 January 2024; Accepted 8 January 2024; Published 9 January 2024

This article has been retracted by Hindawi, as publisher, following an investigation undertaken by the publisher [1]. This investigation has uncovered evidence of systematic manipulation of the publication and peer-review process. We cannot, therefore, vouch for the reliability or integrity of this article.

Please note that this notice is intended solely to alert readers that the peer-review process of this article has been compromised.

Wiley and Hindawi regret that the usual quality checks did not identify these issues before publication and have since put additional measures in place to safeguard research integrity.

We wish to credit our Research Integrity and Research Publishing teams and anonymous and named external researchers and research integrity experts for contributing to this investigation.

The corresponding author, as the representative of all authors, has been given the opportunity to register their agreement or disagreement to this retraction. We have kept a record of any response received.

References

[1] J. Wang, J. Wu, W. Tao, W. Zhu, and W. Qiu, "Network Interconnection Security Buffer Technology for Power Monitoring System," *Security and Communication Networks*, vol. 2022, Article ID 6371062, 11 pages, 2022.

Hindawi
Security and Communication Networks
Volume 2022, Article ID 6371062, 11 pages
https://doi.org/10.1155/2022/6371062

Research Article

Network Interconnection Security Buffer Technology for Power Monitoring System

Jifeng Wang, Jinyu Wu, Wenwei Tao, Wen Zhu, and Weijie Qiu

China Southern Power Grid Co., LTD, Huangpu District, Guangzhou, Guangdong 510623, China

Correspondence should be addressed to Jinyu Wu; wujinyu0301@163.com

Received 7 March 2022; Revised 14 April 2022; Accepted 22 April 2022; Published 30 May 2022

Academic Editor: Zhiping Cai

In recent years, the risk of malicious attacks on power monitoring systems has increased, and there have been many attacks on power systems in the world. Aiming at the network interconnection security problem of the core control system, the concept of "security buffer" is introduced, and a network security buffer method forpower monitoring system is proposed, which is composed of three parts: paradigm check, behavior analysis, and dynamic conversion and jointly realizes the multilevel security inspection of interconnection requests. Experimental verification results show that the proposed method has a protective effect on malicious attacks of power monitoring system.

1. Introduction

In recent years, an increasing number of security incidents have happened to the industrial control system, especially to the power monitoring system. In 2010, Stuxnet invaded the Iranian nuclear power station, disabling 20 percent of centrifuges and severely impeding the implementation of Iran's nuclear power plan. Stuxnet was a destructive worm specifically targeting the industrial control system. It aimed to attack the PLC, and data acquisition and supervisory systems of Siemens, steal its system permission, and further maliciously changed control parameters. In 2015, the Black Energy left more than half of Ukraine without power. In 2018, TSMC's machine equipment was used for blackmail, which got its chip production in trouble. Frequent industrial control security incidents have attracted extensive attention from home and abroad. China and European and American countries have included the industrial control system in their national strategies [1–3].

Some studies have been conducted targeting network security of industrial control systems. The studies comprise two aspects: on the one hand, the learning algorithm is used to train the model and detect the attack behavior based on extracted data features or traffic characteristics. The literature [4, 5] used SVM to model the flow interval and the length of data packets for the network traffic of industrial control system and designed an intrusion detection system; Zhao Guicheng [6] proposed building a behavior model based on function code and start address in Modbus protocol and applying SVM algorithm to the analysis of abnormal behavior. Zhu et al. [7] designed and achieved a multiclass SVM algorithm for the intrusion detection in the perspectives of function code or behavior characteristics; Li Wei et al. [8] proposed a SCADA system intrusion detection approach, which sets out intrusion detection rules by the white list and based on analysis of behavior protocol; Parvania et al. [9] presented a behavior-based intrusion detection system for communication behaviors and protocol specifications of smart grid system by means of statistical analysis of traditional network features and specification-based detection. However, as the attack has turned to slow penetration, statistics of network flow cannot satisfy the demand. At present, there are also some scholars who propose the addition of relevant parameters (such as control command) and semantic descriptions (such as trusted measured values) to the detected characteristics to detect system attacks such as wrong command injection and tampering messages. On the other hand, protocols are subject to the uniform description by protocol analysis in order to detect noncompliant protocols. Suda et al. [10] put

forth an intrusion detection algorithm of time-series features extracted based on time characteristics of series, which extracts effectively the time series features by recurrent neural network (RNN); by virtue of time series loop structure of RNN, and the temporal dependence of samples, Yan Binghao et al. [11] proposed an intrusion detection model based on deep recurrent neural network (DRNN) and region adaptive synthetic oversampling algorithm. But the jobs give little consideration for the behavioral interdependence among control commands. The protocol descriptions, which are either too complicated to popularize or less expressive to explain complex protocols and have slow protocol analysis problems, are unsuitable for the scenes of the power monitoring system.

Therefore, the concept of "security buffer" is introduced to this paper, and a network security buffer method for power monitoring systems is proposed. A security buffer is a memory area that is used between the input and output devices and the CPU to store safety data. It enables the low-speed input/output devices and the high-speed CPU to work in coordination, avoiding the low-speed input/output devices from taking up the CPU and freeing up the CPU so that it can work efficiently. The method is composed of three parts: paradigm check, behavior analysis, and dynamic conversion and jointly realize the multilevel security check on network requests. The paradigm check module examines message format and filters data packets that fail to meet the standard message specification; the behavior analysis module analyzes the sequence of packets and blocks request sequence targeting multiple packets' abnormal behaviors; the dynamic conversion module utilizes format conversion or confusion to implement data structure changes and unload the attacker's attack modes such as buffer overflow attacks.

Compared with existing works, the main contributions and innovations of this paper are as follows:

(1) A unified description language for defining interconnection protocol packets of power monitoring systems is given, which supports the description and parsing of complex heterogeneous protocols and provides a basis for subsequent unified analysis.

(2) Introducing the idea of redundant heterogeneity and adding a dynamic conversion function in the security buffer, which can prevent attackers from trying to speculate the normal working mode and then carry out precise attacks by dynamically adjusting the conversion strategy.

(3) Experimental evaluation of the proposed method shows that the proposed method has a high accuracy rate of detecting multipacket anomalous behavior and the proposed dynamic conversion strategy is effective for offloading buffer overflow attacks.

The other parts of this paper are organized as follows: Section 1 introduces problematic scenes that this method targets; Section 2 deals with detailed design of the method; Section 3 makes an assessment of the proposal by experiment; at last, Section 4 concludes the paper and discusses work to be done next.

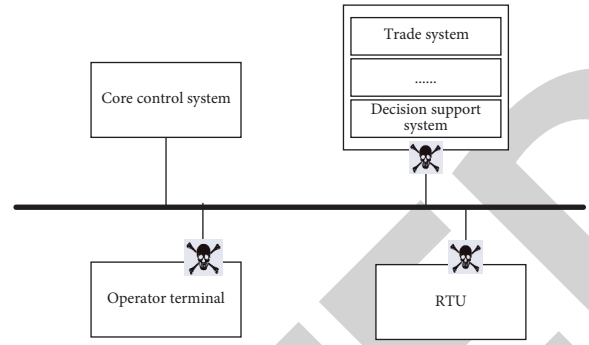


Figure 1: Security threats to the network interconnection of power monitoring system.

2. Problematic Scenes

With computers, communication equipment, measurement and control units as basic tools, the power monitoring system provides a basic platform for real-time data acquisition, switch status detection, and remote control of power generation, transmission, transformation, and distribution systems. The system, together with detection and control equipment, can make up any complex supervisory system.

The network interconnection of power monitoring system is mainly exposed to the following security risks, as shown in Figure 1:

(1) The network architecture of the current power monitoring system is relatively simple. Equipment and core control system are directly accessible through network protocols by operators and at data acquisition places, which provides a springboard for attackers to use the vulnerability of the core control system to attack the system and then destroy the power security. For the primary technological means, hackers exploit vulnerabilities of application protocols in the power monitoring system and create attack load elaborately, triggering buffer overflow vulnerability; then they inject attack loads such as viruses and Trojan horses into the core control system, thus undermining the system security.

(2) The current power monitoring system and other systems on the main network side are accessible. Attackers can first break through other systems, and then use this springboard to scan vulnerabilities of the core control system, operating system, and middleware; then, they use the vulnerabilities to launch brute force attack and remote code injection and finally destroy the security of the core control system.

Therefore, it poses a great risk by directly exposing the core control system of the power monitoring system to operators, data acquisition points, or other business systems. For this reason, this paper proposes a security buffer before the core control system to offload the attacks towards the core control system and secure it.

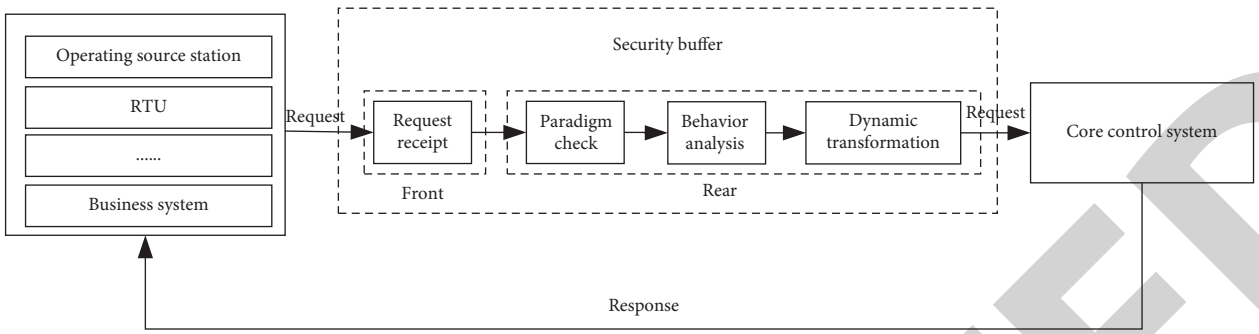


Figure 2: Architecture of network interconnection security buffer technology for the core control system of power monitoring system.

Table 1: Descriptions of XML-based Internet protocol packet paradigm for the power system.

Tag	Meaning	Remarks
<data></data>	Protocol packet	None
<filed></filed>	Field	The field includes two attributes: name of the attribute field and length (in bytes); if the field is a fixed value, it is written directly in the tag
<rule></rule>	Rule	There are three types of rules: 1 (0 : 1024) indicating: 0 ≤ value ≤ 1024; 2 [a,b,c] means that the value can be a, *b*, or *c*; 3 (like '%1') indicates that the field is restricted to those ending with 1;
![CDATA[]	Special tags	Information in [ ] is passed on in the integrity by the parser to the applications, without parsing any control marks in this message.

3. Method Design

3.1. How It Works. Based on the above analysis, this paper presents a network interconnection security buffer technology for the core control system of power monitoring system. This method adds a security buffer between the core monitoring system and other systems or operating terminals to defend against malicious attacks. The method architecture is shown in Figure 2. The security buffer deploys three main functional modules: paradigm check, behavior analysis, and dynamic conversion.

3.2. Paradigm Check. Paradigm check is to examine the protocol specifications of network interconnection packets of the power monitoring system. This section offers a packet paradigm, which supports uniform descriptions of varied network interconnection protocol packets of IEC 104, IEC, and 101 power monitoring systems. The paradigm can be used to define specifications for the Internet protocol data, i.e., rules for the analysis and check of request packets. The data packet will continue to be carried forward depending on the subsequent analysis of the request packet and the check that the packet matches protocol data specification.

3.2.1. XML-Based Uniform Description of Internet Protocols. To support checks of more Internet protocol data specifications, this paper presents a multiprotocol packet paradigm based on the extensible markup language (XML), which is applied for the uniform description of various Internet protocol data specifications of the power system. The descriptions of the XML-based Internet protocol packet paradigm for the power system are shown in Table 1.

Table 2: Example packet paradigm of the XML-based IEC 104 protocol.

<data>Tag
<filed name = "Boot_character" length = "1">68*H*</filed> <filed name = "APDU_Length" length = "1"> <rule>![CDATA[(0 : 253)]</rule> </filed> <filed name = "Control1″ length = "1"></filed> <filed name = "Control2″ length = "1"></filed> <filed name = "Control3″ length = "1"></filed> <filed name = "Control4″ length = "1"></filed> <filed name = "Type" length = "1"></filed> <filed name = "Determiner" length = "1"></filed> <filed name = "TransferReason" length = "1"></filed> <filed name = "DataAddr" length = "2"></filed> <filed name = "MessageBody" length = " APDU_length-10"></filed> </data>

Taking "68 0E 00 00 00 00 64 01 06 00 01 00 00 00 00 14" (master call request that master station sends to slave station in the mainstream IEC 104 protocol of current power system) as an example, a packet paradigm for the XML-based IEC 104 protocol is presented, as shown in Table 2.

The security buffer administrator gives a uniform description of the specifications for Internet protocol data based on the paradigm above. The protocol data specification file may be named by "protocol name.xml", e.g., IEC104.xml, and the captured request packets are subsequently analyzed and checked according to the rules in the specification.

3.2.2. Packet Analysis and Format Check. Like traditional Internet protocols, the Internet protocol packets of the

Table 3: Paradigm check algorithm for request packets.

Input: Request data, protocol name. XML file
Output: 1 and compliant packets/0, discard noncompliant packets; "1" indicates the request packet meets the protocol data specification, and "0" means noncompliance
1 input RequestData
2 analyze protocol name.XML, and generate data structure "S" and rule "R"
3 analyze and unify format of RequestData according to the structure of "S"
4 for $i = 1$ to n/* traverse the rule set "R" * /
5 for $j = 1$ to m/* traverse the set "S" and search the corresponding field based on the field name in the rule set*/
6 if S[j].name = R[i].name/* compare the fields, if the field names are the same*/
7 The field if conforms to the protocol rule defined by the user
8 i++
9 else data frame is discarded, return 0/* discard the data in case of inconformity*/
10 end if
11 else j++
12 end if
13 end for
14 end for
15 output the parsed data structure "S" in the format defined in Table 2
16 return 1

power system are encapsulated top-down in a sequence of the application layer, transport layer, network layer, data link layer, and physical layer. Therefore, the analysis and format check of Internet data of power system mainly consists of analyzes and checks of the network layer, transport layer, and application layer, which are shown as follows.

The capture time of data packets shall be saved prior to protocol analysis, as the control behavior sequence in the power monitoring system is sensitive to time.

<filed name = "time"></filed>

Analysis of network layer mmainly to check the source IP address (SourIP) and the destination IP address (DesIP) on the network layer of packets. The identity information of visitors can be acquired through IP address detection, which provides support for access control and intrusion detection. The information below is saved:

<filed name = "SourIp" ></filed>

<filed name = "DesIp"></filed>

Check of transport layer mainly to examine the source port number (SourPort) and the destination port number (DesPort). Different applications usually use different ports for communication. Port check may help discover some application's connection and access to the target application resources. The following information is saved after analysis:

<filed name = "SourPort" ></filed>

<filed name = "DesPort" ></filed>

Analysis and check of application layer: it is the focus of check on the request packet paradigm, which mainly examines protocol information on the application layer, including the function codes and field values that represent the control behavior.

The paradigm check algorithm of request packets is shown in Table 3. The Internet protocol data specification defined based on the paradigm in 3.2.1 (e.g., IEC104.xml) is first parsed to construct the set $S = \{S1,S2,S3,\ldots,Sm\}$, where Sj $\{j = 1,\ldots,m\}$ represents a field in the protocol in the form of a key-value pair of name and value, i.e., Sj = (name, value), and a rule set $R = \{(R1,R2, R3,\ldots,Rn\}$ is generated as well, where Ri$\{i = 1,\ldots,n\}$ is the specification in the protocol data, representing the specification requirements of a particular field; then the captured request packets are formatted according to S for unification, and finally S is checked according to R to see, for example, whether the function code is compliant and whether the value of the data is out of the range of values.

The master station sends the master call request "68 0E 00 00 00 00 64 01 06 00 01 00 00 00 00 00 00 14" to the slave station, which is subject to algorithm check before output in the format, as shown in Table 4.

The compliant request packets through analysis and check on the application layer, plus the information field extracted from the transport and network layers are saved based on the XML paradigm shown in Table 2, and noncompliant packets are directly discarded.

3.3. Behavior Analysis

3.3.1. Extraction of Behavior Sequence. The indexes of control behavior sequence mainly focus on the control operation interaction process between every two devices on the network of power monitoring system. For the purpose of real-time monitoring and calculation, it is necessary to depend on the analysis result of request packets over a period of time. As stated in Section 3.2, a compliant request packet that has passed paradigm check corresponds to an XML file, whose format is shown in Table 4. Through the time window of time span, we captured the packet analysis result corresponding to

Table 4: Paradigm check output files.

<filed name = "Boot_character" length = "1">68H</filed>
<filed name = "APDU_Length" length = "1">0*E*</filed>
<filed name = "Control1" length = "1">00</filed>
<filed name = "RandomNumber" length = "1">04</filed>
<filed name = "Control2" length = "1">00</filed>
<filed name = "Control3" length = "1">00</filed>
<filed name = "Control4" length = "1">00</filed>
<filed name = "Type" length = "1">64</filed>
<filed name = "Determiner" length = "1">01</filed>
<filed name = "TransferReason" length = "1">06</filed>
<filed name = "DataAddr" length = "2">00 01</filed>
<filed name = "MessageBody" length = " APDU_Length-10">00 00 00 00 14</filed>

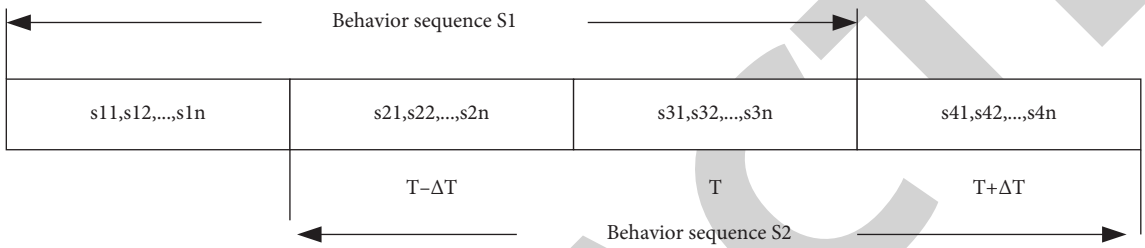


Figure 3: Principle of the incremental window extraction mechanism.

this period of time and extracted a phased behavior sequence. At the time of extraction of behavior sequence, it is necessary to extract the source IP (SourIP), destination IP (DesIP), source port (SourPort), destination port (DesPort), application layer protocol) (Proto), and function code that represents control behavior (Control) and capture time (time).

The IP address and port number at both ends of the control behavior sequence and the protocol type are used as identifiers to distinguish the control behavior sequence. The packets in the time window are grouped according to the quintuple of identification fields (<SourIP>, < DesIP >, < SourPort >, < DesPort >, <Proto>), and all control behaviors are sorted according to time to obtain the behavior sequence [<Controlk>] ranked by control operations, thus obtaining the characteristic data of the control behavior sequence.

<SourIP>,<DesIP>,<SourPort>,<DesPort >,<Proto>: [<Controlk>].

This characteristic data embody the features of control behaviors in a period of time.

When the time window strategy is used to capture packets, to avoid mis-segmentation of multiple single control operations of a continuous related control behavior, the extraction accuracy of the control behavior sequence can be improved based on the partition length "T" and the incremental window of "ΔT" length. The principle of the incremental window extraction mechanism is shown in Figure 3:

3.3.2. Abnormal Behavior Recognition. The information acquired in power monitoring systems may have problems such as inconspicuous data labels and the noisy samples. Given that One-Class Support Vector Machine (OCSVM) algorithm has the features of not requiring neither any algorithm for modeling nor abnormal samples and being robust to noisy samples during training, this paper introduces OCSVM, which has significant advantages over other unsupervised learning methods, to identify the anomalous behavior of network interconnection in power monitoring systems.

The basic idea of OCSVM is to apply the training samples of the same class, map the input space of the training samples into a high-dimensional space by a kernel function to find the optimal classification hyperplane, maximize the distance from the hyperplane to the origin, and to obtain the probability density region of the data in the feature space. Check whether the new input sample point is in the region of the training data point; corresponding quadratic programming problems are shown in formulas (1) and (2).

$$\min_{\omega,\xi_i,\rho} \frac{1}{2}\|\omega\|^2 + \frac{1}{\nu l}\sum_{i}^{l}\xi_i - \rho. \tag{1}$$

Thus

$$\Phi(x_i)\omega \geq \rho - \xi_i, \xi_i > 0, i = 1, \ldots, l. \tag{2}$$

where the training samples $x_1, x_2, \ldots, x_l \in X$, l is the total number of training samples, $\Phi: X \longrightarrow H$ is the mapping of the original feature space to the high-dimensional space, and ω and ρ are the normal vector and compensation of the desired hyperplane in the feature space, respectively. $\nu \in (0,1]$ is the upper limit of the marginal error score and the lower limit of the support vector fraction, and ξ_i is the relaxation variable.

A decision function that represents classification hyperplane is finally obtained as below:

$$f(x) = \operatorname{sgn}(\Phi(x)\omega - \rho). \tag{3}$$

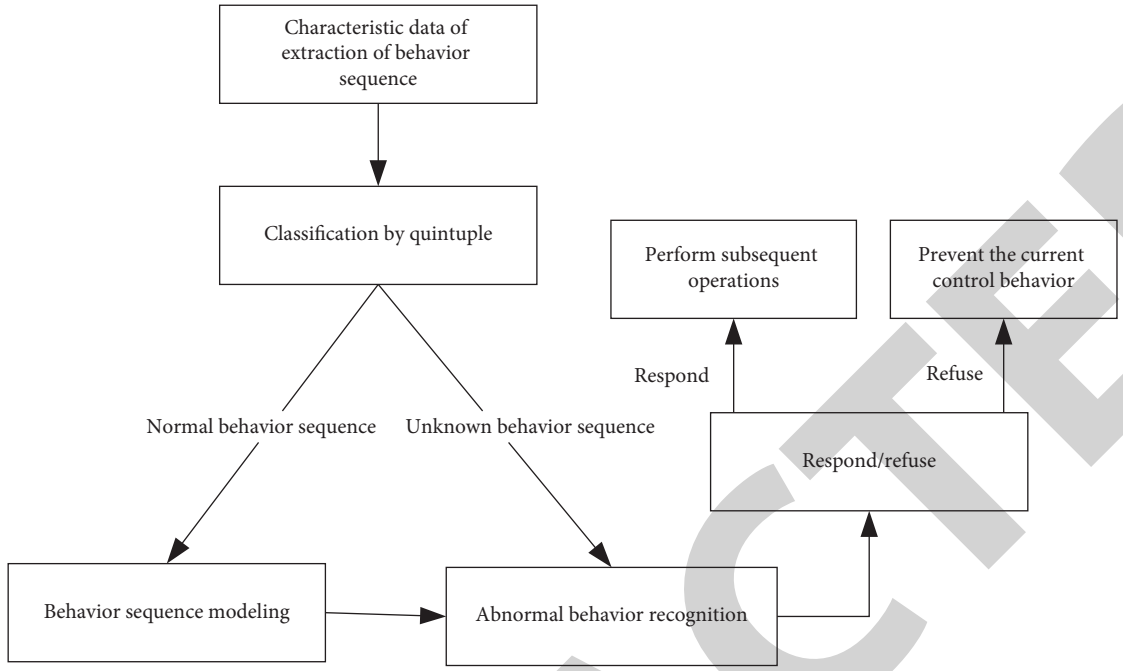


Figure 4: Recognition process of abnormal behavior.

With the Lagrangian function and the Gaussian kernel function introduced, the dual problem of the objective quadratic programming problem can be obtained as below:

$$\min_{\alpha} \frac{1}{2} \sum_{i}^{l} \sum_{j}^{l} \alpha_i \alpha_j K\left(x_i, x_j\right). \tag{4}$$

Thus

$$0 \le \alpha_i \le \frac{1}{vl}, i = 1, \ldots, l \sum_{i}^{l} \alpha_i = 1. \tag{5}$$

where, $K(x_i, y_j)$ is the kernel function, and the vectors that satisfy $0 \le \alpha_i \le 1/vl$ are called support vectors; the final decision function obtained is shown as Formula (6), in which NSV is the number of support vectors.

$$f(x) = \operatorname{sgn}\left(\sum_{i}^{NSV} \alpha_i K\left(x_i, x_j\right) - \rho \right). \tag{6}$$

The process of building an abnormal behavior recognition model based on OCSVM is shown in Figure 4. First, the extracted behavior sequence feature data are classified according to the quintuple, and the behavior sequence si (that is, $\text{Control}_k >$ above) is obtained by time window partition as the data set "S". The sequence si in S is vectorized and transformed into a feature vector x_k of specified k dimension to generate a training sample set X. The OCSVM model is obtained according to X training. When the unknown type of behavior sequence s' is obtained, it is vectorized to generate x', and the resulting feature vector is substituted into the training model to check whether the output x ' is a normal behavior; thus, the recognition of abnormal behavior sequences is achieved. The specific algorithm is shown in Table 5.

When getting the detection result, the security buffer decides whether the current control behavior is allowed or blocked depending on the result; and if not, this packet is discarded.

3.4. Dynamic Conversion. After analyzing the behavior, the data information carried by the packet will be subject to dynamic conversion. Generally, attacks are a pattern of attacks that are carefully designed by the attacker to make the attack successful after he or she is familiar with the system. Therefore, this paper designs and introduces a dynamic conversion module to the security buffer to converse transmitted data according to a predefined policy, so that the attack mode is changed and the data entering the system does not make an attack on the system, which is equivalent to an effective defense against the corresponding attack. By reference to the idea of "redundant heterogeneity", which refers to the use of multiple functionally or performance-equivalent heterogeneous components in parallel, multiple conversion policies are designed in the dynamic conversion module. A policy is selected randomly each time, and the policies are updated from time to time so that the dynamic conversion module itself can remain effective.

3.4.1. Format Conversion of Protocol Data. After a parsed request packet is obtained, select a number randomly from the parsed request packet. The positions of the front and back fields are swapped centering on the "random number" to transform the protocol data format. The reason for random number is to ensure security and prevent tampering

Table 5: Abnormal behavior recognition algorithm.

Input: a Training set of normal behavior sequence S and a unknown behavior sequence *s*'
Output: 1/0, 1 represents s', belonging to normal behavior, and 0 indicates abnormal behavior
1 read the training set of normal behavior sequence *S*
2 The constructed vector model transform it into k-dimensional feature vector x_k to generate the training sample set X
3 train the OCSVM model based on the training sample set
4 vectorize the unknown behavior sequence *s*' to obtain the feature vector *x*'
5 substitute *x*' into OCSVM model and check whether *x*' is normal behavior
6 If it is normal behavior of the model
7 output 1
8 else output 0

Table 6: Format conversion algorithm of protocol data.

Input: Data output from paradigm check
Output: OutData after structural adjustment
1 read data, saved as InData in array format
2 get the array length
3 generate a random, with the random < length
4 create a new array OutData[length]
5 OutData = reverse (InData, random)/ * swap positions of the contents in the front and back according to the random
6 add a new field to the converted data (<filed name = "RandomNumber">random</filed>: Describing the specific value of the generated random)
7 output OutData

Table 7: Format of converted data structure.

<filed name = "Control3" length = "1">00</filed>
<filed name = "Control4" length = "1">00</filed>
<filed name = "Type" length = "1">64</filed>
<filed name = "Determiner" length = "1">01</filed>
<filed name = "TransferReason" length = "1">06</filed>
<filed name = "DataAddr" length = "2">00 01</filed>
<filed name = "MessageBody" length = " APDU_Length-10">00 00 00 00 14</filed>
<filed name = "Control2″ length = "1">00</filed>
<filed name = "Boot_character" length = "1">68*H*</filed>
<filed name = "APDU_Length" length = "1">0*E*</filed>
<filed name = "Control1" length = "1">00</filed>
<filed name = "RandomNumber" length = "1">04</filed>

Table 8: Redundancy-based data obfuscation algorithm.

Input: Data output from paradigm check
Output: OutData after redundancy is added to the control domain
1 input data, and extract the control field action in the data
2 action is an eight-digit number, with storage location is 76543210 from low to high; the eight-digit number is divided into four parts, i.e., 76,54,32, and 10, which are, respectively, the first, the second, the third, and the fourth bytes in the 32-digit number
3 generate a random 32-digit number "ActionPro", each digit of which is random; two maximum digits are taken from each byte
4 The first two bits of each byte are sequentially spliced together to form a new data
5 data mod 7 = *z*
6 then, starting from the zth bit of each byte (from left to right), the numbers 76,54,32, and10 in aciton are stored sequentially, generating AcitonPro
7 write AcitonPro back to the data to generate OutData
8 output OutData

attacks during data transmission. The specific algorithm is shown in Table 6.

To take data in Table 4 as an example, if the random is 04, the format of converted data in the application layer is shown in Table 7.

The corresponding packet changes to "00 00 64 01 06 00 01 00 00 00 00 14 00 68 0E 00 05".

3.4.2. Data Obfuscation. An attacker may modify the control fields in the application layer protocol to achieve illegal control of the device or host. Therefore, protection can be provided by adding redundant bits of data. For example, the type identifier of the behavior in IEC 104 is a 1 byte 8-digit number; it can be converted into 32 bit. The specific algorithm is shown in Table 8.

Table 9: Obfuscated data.

<filed name = "Boot_character" length = "1">68*H*</filed>
<filed name = "APDU_Length" length = "1">0*E*</filed> <filed name = "Control1" length = "4">54 80 C0 30</filed> <filed name = "Control2" length = "4">54 80 C0 30</filed> <filed name = "Control3" length = "4">54 80 C0 30</filed> <filed name = "Control4" length = "4">54 80 C0 30</filed> <filed name = "Type" length = "1">64</filed> <filed name = "Determiner" length = "1">01</filed> <filed name = "TransferReason" length = "1">06</filed> <filed name = "DataAddr" length = "2">00 01</filed> <filed name = "MessageBody" length = " APDU_Length-10">00 00 00 00 14</filed>

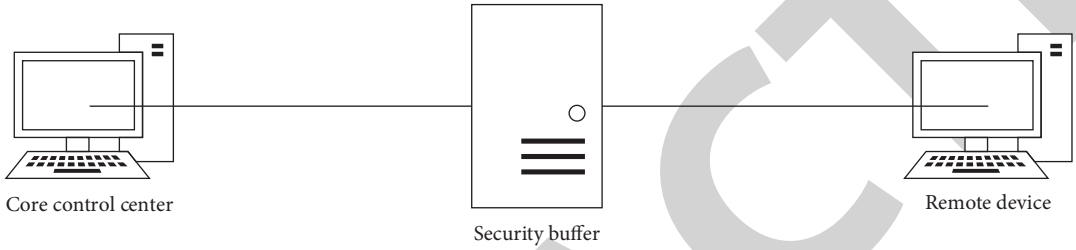


Figure 5: Experimental topology.

Still taking the data in Table 4 as an example, the random 32 bit number is 56 82 C2 32; when the control domain is obfuscated, the converted data format in the application layer is as shown in Table 9.

The corresponding packet changes to "68 0E 54 80 c0 30 54 80 C0 30 54 80 C0 30 54 80 C0 30 64 01 06 00 01 00 00 00 00 14".

It should be noted that the implementation of conversion policies affects the performance of the power system to a certain extent; thus, the policies can be dynamically increased or decreased depending on the specific scenario and different security protection requirements.

4. Experimental Evaluation

4.1. Experimental Environment. We performed simulation experiments on three computers with Windows10, Intel Core i7-9700F, 3.0 GHz CPU, and 32 GB memory, in which one was used as a security buffer functional computer to implement and deploy paradigm check module, behavior analysis module, and dynamic transformation module; one to build Ubuntu16.04 virtual machine to simulate the attacked core control center; and one as a remote device to launch an attack on the target computer. The experimental topology is as shown in Figure 5.

4.2. Effect of Behavior Analysis. In this experiment, we used OCSVM as the learning algorithm for security buffer behavior analysis. Based on UNSW-NB15 data set, we simulated the control behaviors under various scenarios including remote control, remote signaling, remote regulation, and telemetry in the power monitoring system, a total of 1500 sequences of control behavior under normal operation conditions, to give normal sequence model training. Meanwhile, for the common types of attack on the core control systems, and considering the difficulty in obtaining abnormal sequences, abnormal control behavior sequences generated by several attack types such as random operations, repetitive instructions, inversion of time series, and unknown commands were stimulated in the experiment based on construction, clipping, swapping, and falsification for normal behavior sequences. Abnormal behavior sequences and some normal behavior sequences are selected to generate a test set.

The experiment adopted precision and recall as indexes to test the effect of the behavior analysis method proposed in this paper. The computing method is as below [15, 16]:

$$\text{precision} = \frac{\text{true positive}}{\text{predicted positive}} \times 100\%. \quad (7)$$

$$\text{recall} = \frac{\text{true positive}}{\text{total positive}} \times 100\%. \quad (8)$$

We applied Gaussian radial basis function in the OCSVM modeling, in which the parameter gamma indicates degree of nonlinear mapping [17, 18]. The upper bound of modeling error nu[0,1] is the upper limit of the marginal error score and the lower limit of the fraction of support vector. This parameter is used to adjust the precision of the model description of the sample distribution. To make the model contain as many samples as possible, it is necessary to set the upper bound of this error at a low level; and if there is too much noise in the data set, nu may be heightened properly to avoid serious overfitting. Generally, nu is 0.1. To describe the model precisely, $u = 0.01$ was selected as a matched group. Gamma is 0.5 by default. Based on the value, we expanded the value range as a matched group.

Test the behavior analysis effect of the experiment according to the formulas (7) and (8); Figure 6 displays changes of precision along with gamma, and Figure 7 shows changes of recall with gamma.

According to the above experimental results, the behavior analysis method proposed in this paper put in a good performance on precision, which can be above 90 with the changes of gamma's value, but the recall remains to be improved. Considering the difficulty in obtaining and marking malicious samples in the actual power monitoring system, abnormal behavior identification based on OCSVM is still an effective and feasible solution.

To further test the effectiveness of OCSVM, it was compared with the unsupervised learning methods K-Means clustering algorithm [19] and PCA algorithm [20], where gamma = 0.5 and nu = 0.1, as shown in Table 10. As can be seen from Table 10, OCSVM has significant advantages over other methods in terms of accuracy and recall and is suitable for the security protection system of power monitoring systems.

4.3. Effect of Dynamic Conversion. The experiment demonstrates buffer overflow attack, granting common users root privileges to the core control systems and displays the effect of attack uninstallation by dynamic conversion strategy. For the purpose of better exhibition of the effect, the address randomization of the virtual machine in the core control center of the simulation was shut down during the experiment, the StackGuard protection scheme was disabled at the time of code compile, and nonexecutable stacks were turned off.

In the experiment, we compiled stack.c first as a program on the virtual machine of the core control center. The function of the program is to create a 24 byte memory buffer and later transmit data to the buffer via the strcpy() function. Since the strcpy() function does not check the bounds, there is a vulnerability of buffer overflow. What comes next was to compile the program exploit.c that uses stack.c. The main function of the program is to put a piece of shellcode[] (refer to Table 11, more than 24 byte) in the memory, compute its address in the memory, and then work out the return address of stack.c in the program call stack. Through data transmission, exploit.c is sent to the virtual machine at the core control center. When stack.c is executed on the virtual machine, shellcode[] will be saved in the buffer, and due to overflow, the address of shellcode[] will overlay the return address, and the codes in shellcode[] are executed instead.

Normal users on the virtual machine of the core control center can obtain root privilege to the control host by executing exploit.c and then stack.c, until # appears on the command line, as shown in Figure 8.

The dynamic conversion strategy used in the experiment is to swap the contents before and after a certain position in the array. As shown in Table 12, the content of shellcode[] changes, and the contents before and after "50" have their positions swapped.

The code execution results after dynamic conversion is shown in Figure 9. When the stack.c program is executed

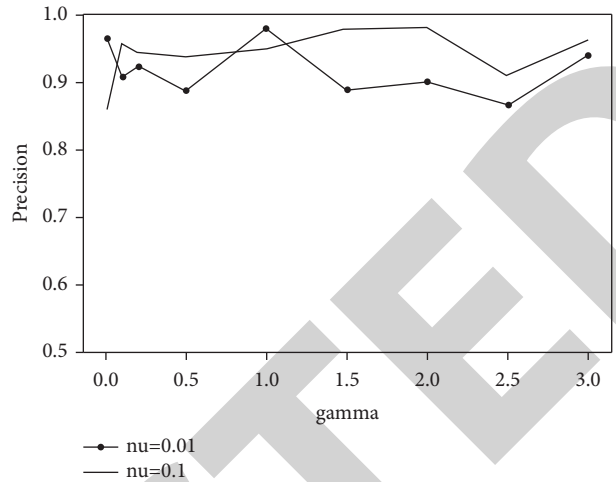


Figure 6: Changes of precision with gamma.

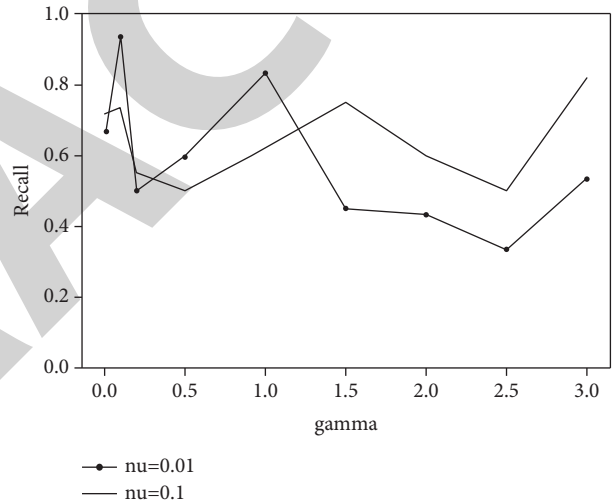


Figure 7: Changes of recall with gamma.

Table 10: Methods comparison.

Methods	Precision	Recall
K-means	0.746	0.375
PCA	0.875	0.428
OCSVM	0.936	0.5

Table 11: Shellcode[] codes.

Char shellcode[] =			
"\x31\xc0"	/*xorl	%eax,%eax	*/
"\x50"	/*pushl	%eax	*/
"\x68""//sh"	/*pushl	$0 × 68732f2f	*/
"\x68""/bin"	/*pushl	$0x6e69622f	*/
"\x89\xe3"	/*movl	%esp,%ebx	*/
"\x50"	/*pushl	%eax	*/
"\x53"	/*pushl	%ebx	*/
"\x89\xe1"	/*movl	%esp,%ecx	*/
"\x99"	/* cdq		*/
"\xb0\x0b"	/*movb	$0 × 0b,%al	*/
"\xcd\x80"	/* int	$0 × 80	*/

```
[09/02/21]seed@VM:~/host$ gcc -o exploit exploit.c
[09/02/21]seed@VM:~/host$ ./exploit
31 c0
50 68
2f 2f
73 68
68 2f
62 69
6e 89
e3 50
53 89
e1 99
b0 b
cd 80
[09/02/21]seed@VM:~/host$ ./stack
#
```

Figure 8: Common users successfully obtain the root privilege.

Table 12: Codes after dynamic conversion.

Char shellcode[] =			
"\x53"	/* pushl	%ebx	*/
"\x89\xe1"	/* movl	%esp,%ecx	*/
"\x99"	/* cdq		*/
"\xb0\x0b"	/* movb	$0 × 0b,%al	*/
"\xcd\x80"	/* int	$0 × 80	*/
"\x50"	/* pushl	%eax swap the contents front and back based on this flag bit	*/
"\x31\xc0"	/* xorl	%eax,%eax	*/
"\x50"	/* pushl	%eax	*/
"\x68" "//sh"	/* pushl	$0 × 68732f2f	*/
"\x68" "/bin"	/* pushl	$0x6e69622f	*/
"\x89\xe3"	/* movl	%esp,%ebx	*/

```
[09/02/21]seed@VM:~/host$ gcc -o exploit exploit.c
[09/02/21]seed@VM:~/host$ ./exploit
53 89
e1 99
b0 b
cd 80
50 31
c0 50
68 2f
2f 73
68 68
2f 62
69 6e
89 e3
[09/02/21]seed@VM:~/host$ ./stack
Returned Properly
```

Figure 9: Attack uninstallation.

once again on the host of the control center, returned properly will appear on the command line, indicating that stack.c is successfully executed; the return address fails to leap to the other memory space, which shows that the conversion strategy takes effect.

5. Conclusion

This paper puts forward a network interconnection security buffer method targeting the core control system of power monitoring system to address the network interconnection security in the power monitoring of core control system. This method adds a security buffer between the core control system for power monitoring and the other system or the operating terminal. Three functional modules such as paradigm check, behavior analysis, and dynamic conversion are deployed in the security buffer to make multilevel security inspection of interconnection request packets. Among them, a unified description language is given for defining interconnection protocol packets of power monitoring systems, which supports the description and parsing of complex heterogeneous protocols, OCSVM in behavior analysis has significant advantages over other unsupervised learning methods and can be effectively adapted to the power monitoring system environment, by introducing the idea of redundant heterogeneity and adding a dynamic conversion function in the security buffer, the conversion policy can be dynamically adjusted to prevent attackers from trying to speculate the normal working mode and then carry out precise attacks. This method can uninstall attacks against the core control system and secure the system. The proposal increases a security buffer, which can exert a certain influence on the instantaneity of the power monitoring system and may make a few erroneous judgments on the identification of malicious behaviors. In the future, we will study more effective behavior analysis algorithms to guarantee the real-time performance of the power monitoring system and further improve the security protection capability of the system.

Data Availability

The labeled data set used to support the findings of this study is available from the corresponding author upon request.

Conflicts of Interest

The author declares no competing interests.

Acknowledgments

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

References

[1] F. Alrimawi, L. Pasquale, and B. Nuseibeh, "On the automated management of security incidents in smart spaces," *IEEE Access*, vol. 7, Article ID 111513, 2019.

[2] F. Alrimawi, L. Pasquale, D. Mehta, N. Yoshioka, and B. Nuseibeh, "Incidents are meant for learning, not repeating: sharing knowledge about security incidents in cyber-physical systems," *IEEE Transactions on Software Engineering*, vol. 48, no. 1, pp. 120–134, 2022.

[3] D. Schlette, M. Caselli, and G. Pernul, "A comparative study on cyber threat intelligence: the security incident response perspective," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 4, pp. 2525–2556, 2021.

[4] M. A. A. Mutha and M. R. R. Tuteja, "Secure and efficient approach for mul-tilayer cyber security based on intrusion detection system," *International Journal of Advent Research in Computer and Electronics*, vol. 2, no. 2, pp. 33–37, 2015.

Hindawi
Security and Communication Networks
Volume 2024, Article ID 9847896, 1 page
https://doi.org/10.1155/2024/9847896

Retraction

Retracted: Performance Evaluation Method of Online Supply Chain Finance Logistics Enterprises Based on GARCH-VAR

Security and Communication Networks

Received 8 January 2024; Accepted 8 January 2024; Published 9 January 2024

This article has been retracted by Hindawi following an investigation undertaken by the publisher [1]. This investigation has uncovered evidence of one or more of the following indicators of systematic manipulation of the publication process:

(1) Discrepancies in scope

(2) Discrepancies in the description of the research reported

(3) Discrepancies between the availability of data and the research described

(4) Inappropriate citations

(5) Incoherent, meaningless and/or irrelevant content included in the article

(6) Manipulated or compromised peer review

The presence of these indicators undermines our confidence in the integrity of the article's content and we cannot, therefore, vouch for its reliability. Please note that this notice is intended solely to alert readers that the content of this article is unreliable. We have not investigated whether authors were aware of or involved in the systematic manipulation of the publication process.

Wiley and Hindawi regrets that the usual quality checks did not identify these issues before publication and have since put additional measures in place to safeguard research integrity.

We wish to credit our own Research Integrity and Research Publishing teams and anonymous and named external researchers and research integrity experts for contributing to this investigation.

The corresponding author, as the representative of all authors, has been given the opportunity to register their agreement or disagreement to this retraction. We have kept a record of any response received.

References

[1] T. Xia and J. Yang, "Performance Evaluation Method of Online Supply Chain Finance Logistics Enterprises Based on GARCH-VAR," *Security and Communication Networks*, vol. 2022, Article ID 4500430, 9 pages, 2022.

Hindawi
Security and Communication Networks
Volume 2022, Article ID 4500430, 9 pages
https://doi.org/10.1155/2022/4500430

Research Article

Performance Evaluation Method of Online Supply Chain Finance Logistics Enterprises Based on GARCH-VAR

Ting Xia[1] **and Junxuan Yang**[2]

[1]*School of Finance, Guangdong University of Finance and Economics, Guangzhou 510320, China*
[2]*School of Economics & Management, Tongji University, Shanghai 200092, China*

Correspondence should be addressed to Junxuan Yang; 1510311@tongji.edu.cn

Received 1 March 2022; Revised 4 April 2022; Accepted 18 April 2022; Published 30 May 2022

Academic Editor: Zhiping Cai

In recent years, China's core enterprises have been plagued by high operating costs, difficult bank loans, and other practical problems in the supply chain. As a new financing model emerged in recent years, it has opened up new markets in finance and logistics industry and brought new ideas and vitality to all parties in the supply chain. Since the strengthening of supervision, the operation of the industry has gradually changed to the direction of normalization. The study of online loan interest rate fluctuation is helpful to understand the source and characteristics of online loan risk, which has important reference significance for China's Internet lending market. The measurement of interest rate risk can help to monitor market risk in time and improve financial supervision. This paper takes the online loan interest rate under the background of supervision as the research object, combining theoretical analysis and empirical research to explore the characteristics of interest rate fluctuations and the reasons behind the P2P online loan, and discusses the online loan business model. Based on the influencing factors of interest rate fluctuation, this paper analyzes the main characteristics of network loan interest rate from the aspects of interest rate trend interval distribution, regional distribution, and background distribution. This paper adopts the daily closing price data of domestic R insurance company to establish the daily logarithmic return rate series of stock prices. The results show that (1) GARCH-VAR model can effectively reflect the stock price fluctuation and market risk degree of the insurance company; (2) the company's VAR showed a trend of first rise and then slight decline, with the highest VAR in 2018; and (3) the interpretation of VAR value should be combined with financial indicators. The increase in net profit rate will also lead to the decline of VAR value in the next period. Based on this, countermeasures and suggestions for market risk management are proposed for insurance companies.

1. Introduction

With the continuous development of the financial system and social security system, the insurance industry, as a part of it, has become more and more important. The outbreak of the global financial crisis in 2008 led to the violent turbulence of the international financial market and the huge impact on the financial systems of various countries, which directly affected the survival and development of financial and insurance institutions [1–3]. For example, the global insurance giant American International Group was on the verge of bankruptcy due to a huge capital gap. At present, central banks of various countries keep cutting interest rates, and the global finance has entered the era of low interest rate. The stable development of insurance industry is deeply affected by the basic variable of interest rate [4]. Low interest rate leads to the reduction of investment yield and increases the spread loss risk. The valuation of financial assets is distorted, and insurance companies are facing increasingly severe market risks. As China's economy steps into the new normal and the rise of the mixed business model, the control of financial risks is particularly important [5–7].

Risk measurement is the first step of market management, and the VAR model is also one of the classic measurement methods [8]. Generally speaking, there are four measures of market risk: sensitivity analysis is reflected by changes in expected portfolio value caused by changes in some market risk factors. Among them, the common market

risk factors of gap analysis and duration analysis are interest rates. Capital asset pricing model is a very classic measure of market risk, which is developed based on Markowitz's portfolio theory [9, 10]. The calculation of the commonly used method mainly depends on the historical data to calculate the VAR value, that is, to calculate the VAR of all financial assets in the portfolio and the income distribution of the entire portfolio [11–15].

Online supply chain finance is to realize the interconnection of the information systems of financial institutions and the upstream and downstream enterprises of the core enterprises in the supply chain through Internet technology under the condition of information to reduce the financial loss. [16, 17]. Compared with traditional supply chain finance, online supply chain finance has more efficient information communication, more accurate management process, and more controllable financial risks [18–20]. Compared with traditional supply chain finance dominated by logistics enterprises, online supply chain finance has a wider scope of credit, no longer limited to large enterprises, and dynamic pledge to fill positions more timely and transparent process. It can be seen from the above analysis that the domestic research studies on online supply chain finance are still in its infancy, and the main research contents are mode characteristics and functions, while the research on the performance evaluation of logistics enterprises in online supply chain finance is rarely involved. This paper takes online supply chain finance led by logistics enterprises as the entry point to study its performance evaluation indicators and methods [21]. It is expected to provide help for the promotion and application of this new online supply chain finance model in reality.

In the dynamic pledge mode of online supply chain finance led by logistics enterprises, financing enterprises apply for financing to the cooperative bank of the online platform through the electronic warehouse receipt provided on the online platform of logistics enterprises [22]. Online supply chain finance dominated by logistics enterprises, creditor enterprises, and debtor enterprises adopts collection mode. Banks sign contracts on the online supply chain finance platform provided by logistics enterprises and, on this basis, provide financial services to supply chain related enterprises through e-commerce. [23, 24]. Making the financing process more convenient online financial supply chain in the process of cargo circulation is not a bank in the ownership of the goods. On the contrary, the online platform provides the first choice of credit investigation list for enterprises in the supply chain of benign competition and credit investigation system construction [25–27].

The contributions of this paper are as follows. This paper adopts the daily closing price data of domestic R insurance company to establish the daily logarithmic return rate series of stock prices. The proposed combined algorithm results in online supply chain financial logistics enterprise performance evaluation.

2. Related Works

As can be seen from the above literature review, since the research of supply chain finance on the performance evaluation of logistics enterprises is relatively few, this paper summarizes the viewpoints of predecessors from three aspects: logistics supply chain enterprises, financial evaluation supply chain, and financial performance evaluation index system. Doan and Bui [28] believed that the evaluation of enterprise credit risk in supply chain finance is inseparable from the evaluation of enterprise operation ability, profitability, debt paying ability, and development ability. Meucci and Carrotani [29] believed that supply chain finance should not only pay attention to its performance management but also pay attention to the liquidity of supply chain finance and the visualization of supply chain. Yagi believed that supply chain finance should not only pay attention to its performance management but also pay attention to the liquidity of supply chain finance and the visualization of supply chain. The performance evaluation of logistics enterprises in the implementation of supply chain finance is carried out from the aspects of logistics operation ability, supply chain dynamic management ability, online platform operation ability, and financial operation ability. In particular, the financial operation ability of logistics enterprises is projected by the indicators of transaction efficiency and allocation efficiency. Elmanizar et al. [30] established a performance evaluation system for small- and medium-sized enterprises under the supply chain finance mode from the aspects of financial evaluation, customer evaluation, internal business process, and growth with balanced scorecard, in which customer complaint rate reflects product reliability and supply chain node interaction reflects learning and growth [31].

The direction of supply chain finance evaluation mainly involves supply chain finance risk evaluation, credit evaluation, supply chain performance evaluation, and so on [32]. However, there are few research studies on the financial performance evaluation of supply chain, and the financial research of supply chain performance evaluation is even more scarce. Therefore, this study hopes to supplement the problems we are facing [33]. Although there are few direct studies on the performance evaluation of supply chain finance, the comprehensive evaluation of other aspects of supply chain finance can also understand the study of supply chain financial performance evaluation from the side [34] With the development of supply chain finance, order financing based on supply chain relationship also appears in large numbers to authenticate the property rights of collateral [35]. There is an increasing demand for third-party institutions for value evaluation and supervision and control and for providing evaluation warehousing and monitoring services for inventory and receivables financing. Warehousing and logistics enterprises have become relatively standardized and developed. Conditions for the development of supply chain financial services are ripe. Warehousing and logistics enterprises should connect with banks and other financial

institutions, increase the supply chain finance business model with small- and medium-sized enterprises and core enterprises, and vigorously develop supply chain finance business. Enterprises have unique advantages in participating in supply chain finance financing, while the professional service advantages of logistics enterprises determine that their responsibilities in the supply chain are different from those of finance and enterprises. Therefore, it is necessary to study supply chain finance based on their own characteristics [36].

From the above analysis, we know that the above methods have studied performance evaluation of logistics enterprises in online supply chain finance. However, some problems still exist. For example, no scholar has applied the GARCH-VAR model to this field till now, so the research here is still a blank, which has great theoretical research and practical application value for logistics enterprises.

This paper consists of five parts. The first and second parts give the research status and background. The third part is the digital image-based crack repair model of ancient ceramics. The fourth part shows the experimental results. The experimental results of this paper are introduced and compared and analyzed with relevant comparison algorithms. Finally, the fifth part concludes the full paper.

3. Performance Evaluation of Supply Chain Finance Based on GARCH-VAR

3.1. Supply Chain Finance Performance Evaluation Index System. For any enterprise, capital is the source of its life; financing is a way to revitalize the enterprise capital, improve the effective utilization rate of capital, and obtain profits. With the emergence of modern new production organization mode, supply chain financing has become a research hotspot. However, enterprises must have their own unique conditions to conduct supply chain financing. Therefore, those who are most affected by stress and have the ability to take the most drastic and effective action for change are the most likely to achieve the best performance. This paper will establish the supply chain financial performance evaluation index system of warehousing and logistics enterprises from four dimensions, that are the pressure dimension, action dimension, ability dimension, and driving factor dimension. The whole system of the method is given in Figure 1.

In the process of establishing specific three-level indicators, financial indicators are selected as the standard of financial indicators of listed companies, while nonfinancial indicators of warehousing and logistics enterprises refer to high-frequency indicators and other referable standards formulated by the country or industry. According to the characteristic index of logistics enterprises, this paper chooses different methods to determine the weight of the index system and finally uses the analytic hierarchy process (AHP) to determine the financial performance evaluation index system.

3.2. GARCH-VAR Model. Although ARCH is a very simple volatility description model, it usually needs a lot of parameters to describe the volatility of return rate. And the fit effect of volatility is not very good. Here, we will talk about an generalized ARCH model—GARCH model; the expression of GARCH (p, q) model is as follows, where the $p = q = 1$ in this paper:

$$a_t = \sigma_t \varepsilon_t, \tag{1}$$

$$\sigma_t^2 = \alpha_0 + \sum_{i=1}^{p} \alpha_i a_{t-i}^2 + \sum_{q}^{j=1} \beta_j \sigma_{t-j}^2, \tag{2}$$

where σ_t^2 represents the positive term and a_t is the noise. Let us set the parameter innovation as follows:

$$\eta_t = a_t^2 - \sigma_t^2 = a_t^2 - E\left[a_t^2 | F_{t-1}\right]\left(\sigma_t^2 = E\left[a_t^2 | F_t - 1\right]\right). \tag{3}$$

Assume that

$$E(\eta_t) = 0, \operatorname{cov}(\eta_t, \eta_{t-1}) = 0. \tag{4}$$

We have

$$\sigma_t^2 = \alpha_0 + \sum_{i=1}^{p} \alpha_i \alpha_{t-i}^2 + \sum_{j=1}^{q} \beta_j \sigma_{t-j}^2, \tag{5}$$

and

$$a_t^2 - \eta_t = \alpha_0 + \sum_{i=1}^{p} \alpha_i a_{t-i}^2 + \sum_{j=1}^{q} \beta_j \left(a_{t-j}^2 - \eta_{t-j}\right). \tag{6}$$

So, like the ARCH model, to keep stationary, the two sides will return expected:

$$\operatorname{var}(a_t) = E\left[a_t^2\right] = \frac{\alpha_0}{1 - \sum_{i=1}^{\max(p,q)} (\alpha_i + \beta_i)}. \tag{7}$$

To ensure that variance is positive, that is, variance exists and is finite,

$$\sum_{i=1}^{\max(p,q)} (\alpha_i + \beta_i) < 1. \tag{8}$$

The GARCH (1, 1) model is the most popular and useful GARCH model at present:

$$\sigma_t^2 = \alpha_0 + \alpha_1 a_{t-1}^2 + \beta_1 \sigma_{t-1}^2 \left(\alpha_1 \beta_1 \geq 0, \alpha_0 > 0, \alpha_1 + \beta_1 < 1\right). \tag{9}$$

Why can the GARCH model better describe volatility aggregation. Because a large a_{t-1}^2 or σ_{t-1}^2 can well describe volatility clustering,

$$K_a = (K_\varepsilon + 3) E\left[\sigma_t^4\right] \frac{\left(1 - (\alpha_1 + \beta_1)\right)^2}{\alpha_0^2} - 3 \frac{(K_\varepsilon + 3)\left(1 - (\alpha_1 + \beta_1)^2\right)}{1 - 2\alpha_1^2 - (\alpha_1 + \beta_1)^2 - K_\varepsilon Q_1^2} - 3, \tag{10}$$

$$K_a^\phi = \frac{3 - 3(\alpha_1 + \beta_1)^2}{1 - 2\alpha_1^2 - (\alpha_1 + \beta_1)^2} - 3. \tag{11}$$

For the GARCH model, we also adopt the maximum likelihood method and the parameters we want to estimate, so there is condition likelihood:

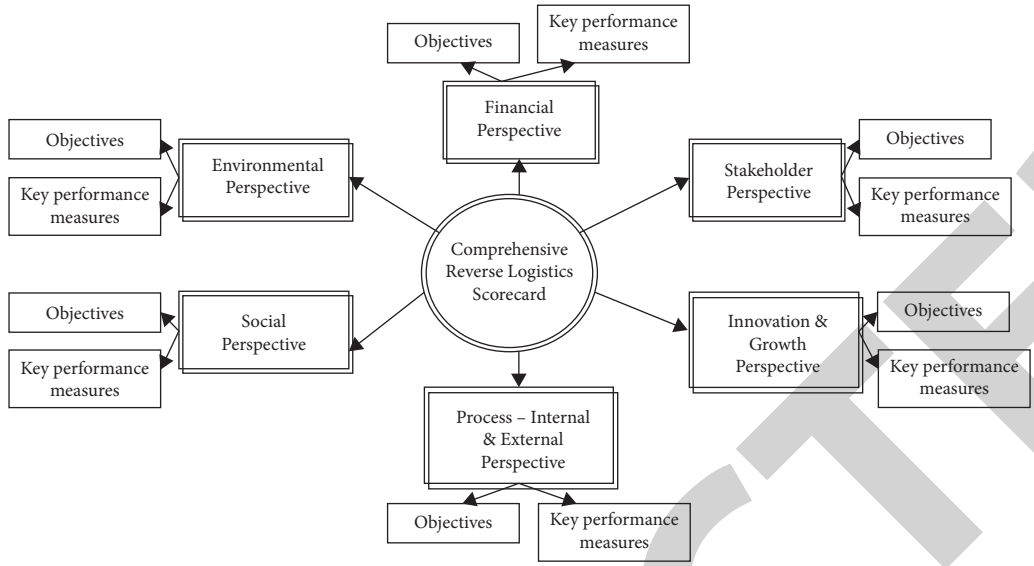


Figure 1: The whole system of the proposed method.

$$p(r_2, \ldots, r_T | r_1, \theta) = \prod_{t=2}^{T} p(r_t | \mathcal{F}_{t-1}, \theta), \tag{12}$$

$$b_{pqrs} = b_{pqrs} + V_{pqrs} \cdot \widehat{F}_{pqrs}. \tag{13}$$

It has been proved above that, compared with the normal distribution, the distribution of the random error term of the Internet financial index return rate presents a significant peak thick-tailed distribution. In order to describe the distribution characteristics more accurately, the random error terms of T and GED distributions of students in three forms are discussed, and the following results are obtained. If the sum of parameters is infinitely close to 1, it indicates that the influence of conditional variance is highly durable, and GARCH (1, 1) has high stability, which can better fit the data. Then, conditional heteroscedastic ARCH LM test is performed on the above equation to obtain the statistical results of residual sequence when the lag order $p = 3$.

The value of Internet financial products or services is lost due to market uncertainty, and the risk measurement of Internet financial market is used to measure the loss. The GARCH family model is used to model the volatility of Internet financial price index series and reflect the difference in the state and accuracy of volatility. Based on this, the AIC criterion is used to find the conditional variance of the model which can better fit the volatility. The VAR method can not only measure the risk of Internet finance but also describe the change of Internet finance income well, so it has a wide range of uses.

4. Experimental Results and Analysis

4.1. Introduction to Experimental Environment and Data Set. With the continuous development in recent years, R Insurance Company has become the representative of the mixed operation of China's insurance industry. At present, its market value is up to one trillion yuan, ranking in the forefront of large domestic insurance companies. As a large listed insurance company in China, R Insurance Company is faced with one of the major financial risks and its impact on the company's operation and even the insurance industry, which cannot be ignored.

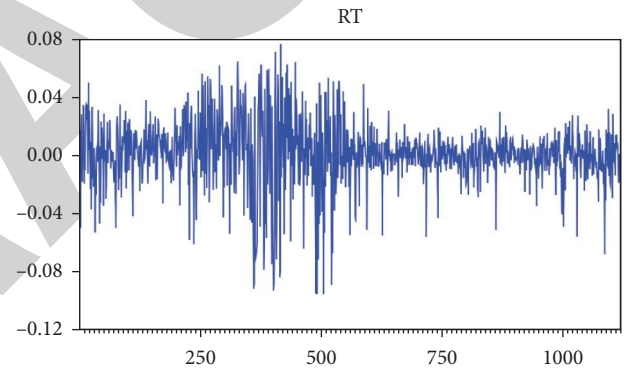
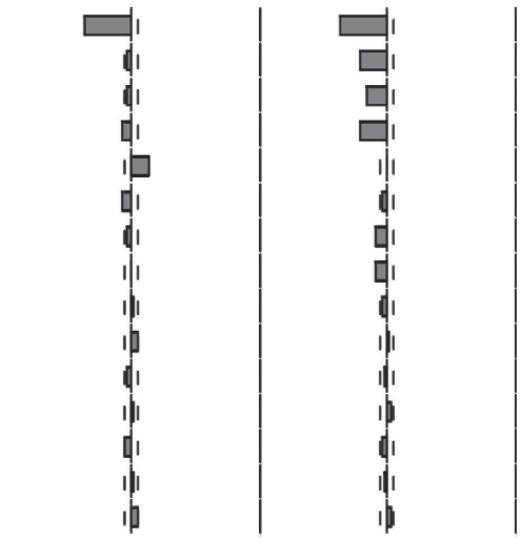


Figure 2: The stationarity results of experimental data.

Therefore, in order to avoid the influence of abnormal fluctuations of the stock market as much as possible, this paper sets the time span of the research data as January 1, 2016, to May 1, 2020, and calculates the corresponding pair based on the daily closing price P of R Insurance company rate of return. All data in this paper are from NetEase Financial website. In the descriptive analysis of the data, EVIEM8.0 software was used to depict the time series diagram of the stock return rate. According to Figure 2, the logarithmic return rate fluctuated up and down with 0 as the center value, and its fluctuation range was obvious in most of the time periods, with different fluctuations. The amplitude is concentrated in different time periods, which indicates that the time series of return rate has strong characteristics of fluctuation agglomeration.



Autocorrelation	Partial Correlation		AC	PAC	Q-Stat	Prob
		1	−0.378	−0.378	165.55	0.000
		2	−0.044	−0.218	167.79	0.000
		3	−0.029	−0.161	168.76	0.000
		4	−0.079	−0.209	175.96	0.000
		5	0.147	0.007	201.26	0.000
		6	−0.067	−0.040	206.44	0.000
		7	−0.039	−0.085	208.23	0.000
		8	−0.005	−0.083	208.25	0.000
		9	0.012	−0.042	208.42	0.000
		10	0.056	0.011	212.12	0.000
		11	−0.032	−0.010	213.36	0.000
		12	0.023	0.034	213.99	0.000
		13	−0.050	−0.025	216.90	0.000
		14	0.009	−0.024	216.99	0.000
		15	0.048	0.027	219.73	0.000

Figure 3: LR sequence autocorrelation and partial autocorrelation test results.

4.2. Experimental Results Analysis. Time series has the characteristic of autocorrelation, so the past values of variables can be used to predict their future values. To determine the mean value equation, we need to investigate the autocorrelation function (ACF) and partial autocorrelation function (PACF) of data. On this basis, we can choose the appropriate regression model and then combine with the information criterion to determine the best lag order.

Figure 3 shows the autocorrelation and partial autocorrelation test results of LR sequences. It can be seen that both ACF function and PACF function are trailing. Therefore, ARMA(1, 1), ARMA(1, 2), ARMA(2, 1), and ARMA(2, 1) were established, respectively, and AIC information criteria and lag time were compared. According to the conditional heteroscedasticity of financial logistics performance, interest rate fluctuation changes with time. Poor economic environment and low platform interest rate have become one of the unstable factors for the whole logistics enterprise. On the other hand, irrational behaviors of lenders and borrowers often occur, which also weakens the stable supply and demand mechanism of the market.

Firstly, with the continuous improvement of mobile payment application technology, the scale of its users is also increasing year by year. According to the statistics of China Internet Network Information Center of the People's Bank of China, from 2014 to 2018, the scale of Internet users increased from 300 million to 570 million, the growth rate decreased from 17% to 7%, with the growth rate dropping from 73.2 to 8.2. This means that on the one hand, the popularity of payment is increasing, and on the other hand, the competition for users in the industry is becoming increasingly fierce, as shown in Figure 4.

With the development of information technology, innovation in payment field is further evolving from payment mode innovation to payment media innovation. New technologies such as code payment, biometric payment, and NFC are emerging, and their application scope is gradually expanding. According to iResearch data statistics, in 2017, by virtue of the intelligent transformation of traditional POS machines, bank card orders accounted for 19.4% of the payment market size, Internet payment accounted for 16.8%, mobile payment accounted for 63.7% have become the absolute leader in new payment formats.

Drip travel allows merchants to offer mobile payments, such as the integration of financial closed loop in the mobile payment market rapid development at the same time, exposed the personal information leakage risk and capital risk mainly including the following several reasons: firstly, mobile banking and third-party payment platforms verify by verification code or dynamic password. Once the mobile phone is lost or stolen, there are huge security risks in customer transaction information. Second, when consumers make purchases on Taobao, the user's name, contact information, address, and consumption information will be recorded in the memory of the phone.

Many poorly managed online lending platforms usually face liquidity risks. From the rise of P2P online lending platforms to the present, online lending platforms that do not meet compliance requirements have been eliminated from the market. One side is the completion of multiple rounds of investment and financing and listed industry leading enterprises, while the other side is hovering on the edge of life and death, the face of bankruptcy at any time small platform statistics at the end of 2017, a total of 3902 problem platforms (excluding transformation), accounting for 70.9% of the total number of platforms, at least 643 in 2017. The number of problematic platforms decreased by 44.6% year on year. Among all the problematic platforms, 196 platforms lost contact and ran away, accounting for 30.5%. 160 platforms were closed without reason, accounting for 24.9%. A total of

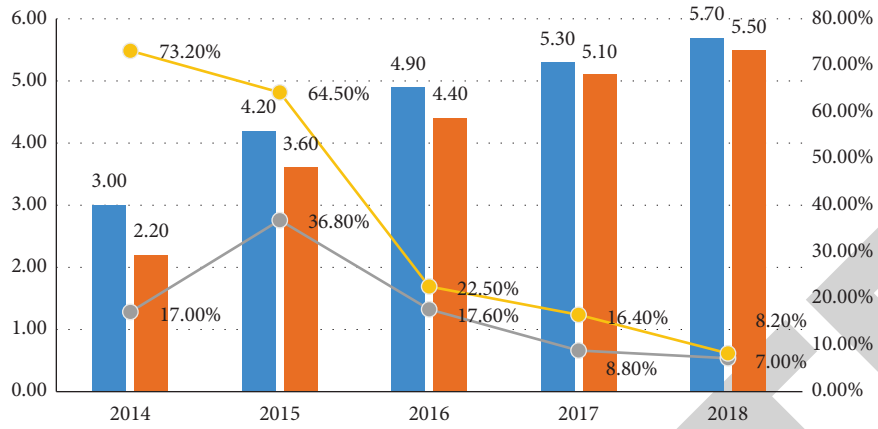


Figure 4: Size and growth of logistics supply chain from 2014 to 2018.

141 platforms closed down, accounting for 21.9%; 100 platforms are difficult to withdraw cash, accounting for 15.6%, and the rest are shown in Figure 5.

The interval distribution of interest rates can be observed from the perspective of volume and number of platforms. From the perspective of volume (Figure 6), since 2016, the transaction interest rate of most online loan orders is between 8% and 12%. The transaction interest rate of 12%–16% accounts for a small proportion, while the transaction interest rate of more than 16% declines year by year until it reaches zero. It can be seen that under the background of gradually strengthening financial supervision, online loan interest rate gradually shifts to a reasonable range, and supervision plays a significant role in regulating interest rate. In terms of the overall trend, the next highest percentage of deals was below 8%, and in early 2016 and early 2017, those below 8% squeezed even beyond the 8% to 12% range. This is closely related to macroeconomic policies and financial supervision. In the environment of deleveraging and defusing financial risks, the policy prospects of online lending industry are uncertain, and the downward pressure on interest rates is large. After 2017, the regulatory policy framework of online lending has been basically built, and market expectations have improved, and the downward pressure on interest rates has been eased.

In Figure 7, the straight line represents the distribution of the income sequence, and the scatter plot under the normal distribution curve represents the actual distribution. As can be seen from the figure, the scatter distribution on both sides of the online wave is very obvious, but the left curve near the lower end of the horizontal axis shows a scatter diagram, and the linear deviation is getting larger and larger, indicating that the production sequence has a trailing effect.

As shown in Figure 8, the overall performance from 2015 to 2019 showed a downward trend with a large fluctuation range. There were two obvious inflection points in the figure, which were divided into three stages according to the inflection points for further analysis. In the first stage, from the beginning of 2015 to the beginning of 2017, the interest rate dropped rapidly from around 14% to around 8%. Before the regulation gradually approached the reasonable range, a large number of online loan platforms implemented policies,

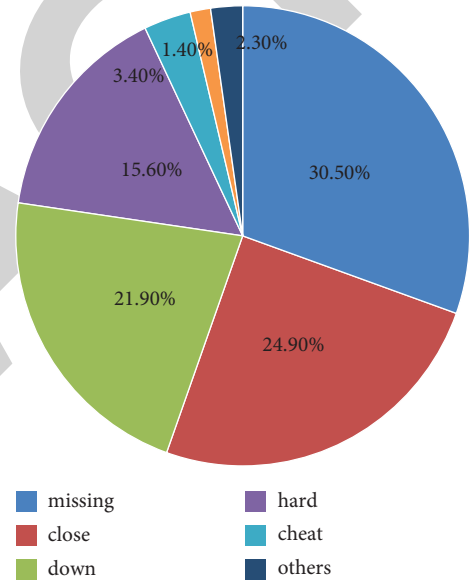


Figure 5: Composition of problem types in supply chain finance in 2020.

such as guarantee payment and high interest solicits, to expand the capital pool.

After the issuance of regulatory policies in 2015, the irregular behaviors of online lending platforms have been gradually controlled, and the artificially high interest rates have returned to a reasonable level. In addition, due to the uncertain industry outlook caused by regulation and the lack of investor confidence, the performance fluctuated greatly during this period. In the second stage, from the first quarter of 2017 to the second quarter of 2018, the performance rebounded slowly. During this period, the supervision system of the online loan industry has been basically established and the supervision goal is to promote the healthy development of the industry. In the third stage, from the third quarter of 2018 to the end of 2019, the performance fell back again. Previous regulations curbed the irregular development of online loans but failed to resolve the accumulation of risks, which showed the difficulty of reforming the financial logistics industry.

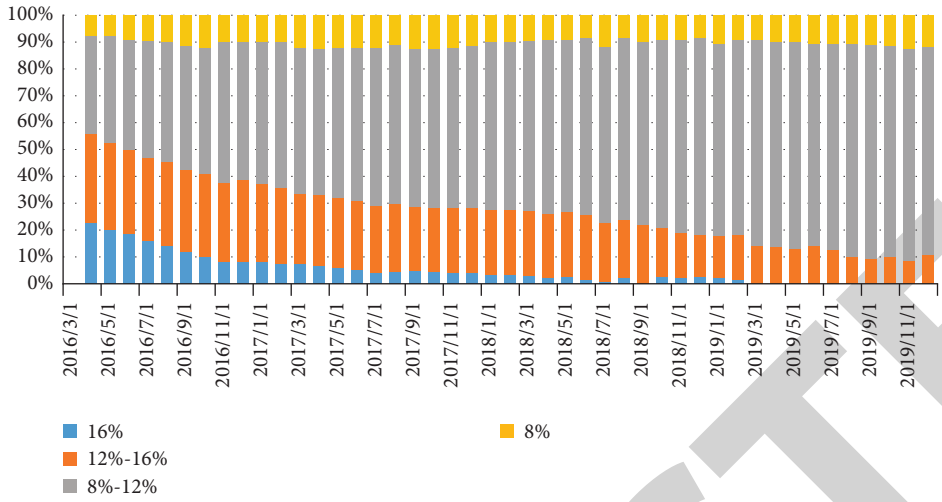


Figure 6: Logistics enterprise comprehensive performance evaluation grading.

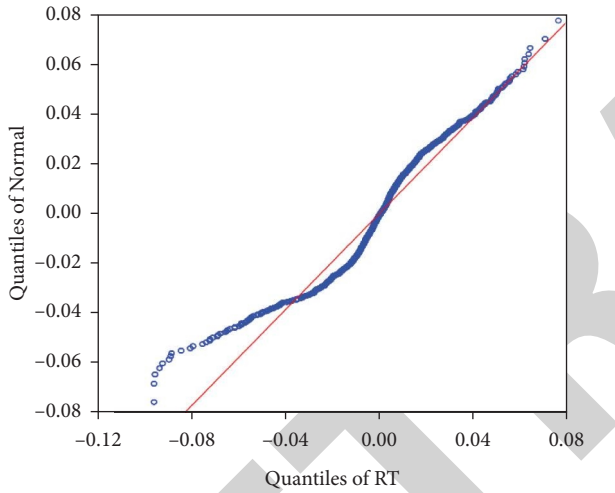


Figure 7: Supply chain finance logistics enterprise performance index QQ chart.

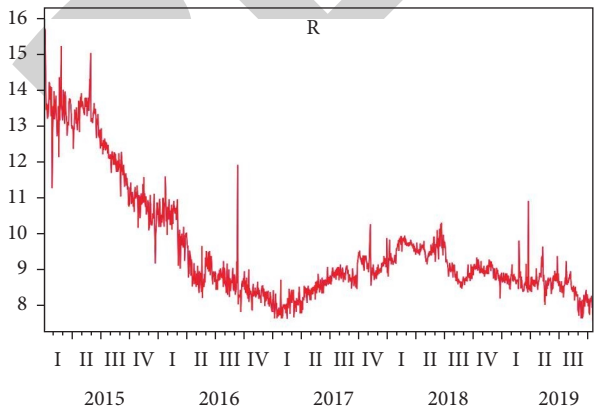


Figure 8: Performance trends of financial enterprises.

5. Conclusions

Supply chain finance, as an emerging financing method, provides a good solution to the problems of capital turnover of all parties in the supply chain, which is conducive to solving the financing difficulties of small- and medium-sized enterprises. As a key node in the supply chain, warehousing and logistics enterprises enjoy a special position. Therefore, it is necessary to study the performance of supply chain finance of warehousing and logistics enterprises, and it is of great significance to study the performance of supply chain finance of enterprises to promote better and faster development of supply chain finance of enterprises.

On the basis of literature retrieval and analysis by domestic and foreign scholars in the early stage, the research topic of supply chain financial performance evaluation of logistics enterprises is determined, and risk analysis is carried out through relevant basic theories and the operation process of supply chain financial mode of warehousing logistics enterprises. This paper innovatively takes the GARCH-VAR model as the supply chain financial performance analysis model and tries to construct a complete index system through analytic hierarchy process. The fuzzy comprehensive evaluation method is used to empirically evaluate the financial performance of the supply chain of warehousing and logistics enterprises, so as to test its applicability and operability, then analyze the problems existing in the evaluation score of the supply chain financial performance of warehousing and logistics enterprises, and put forward corresponding improvement suggestions for the problems and shortcomings of enterprises.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

[1] P. O. Junior, A. K. Tiwari, G. Tweneboah, and E. Asafo-Adjei, "GAS and GARCH based value-at-risk modeling of precious metals[J]," *Resources Policy*, vol. 75, Article ID 102456, 2022.

[2] C. Tang and K. Aruga, "Relationships among the fossil fuel and financial markets during the COVID-19 pandemic: evidence from bayesian DCC-MGARCH models," *Sustainability*, vol. 14, no. 1, p. 51, 2021.

[3] S. Chen, J. Du, W. He, and M Siponen, "Supply chain finance platform evaluation based on acceptability analysis," *International Journal of Production Economics*, vol. 243, Article ID 108350, 2022.

[4] L. Wang and Y. Wang, "Supply chain financial service management system based on block chain IoT data sharing and edge computing," *Alexandria Engineering Journal*, vol. 61, no. 1, pp. 147–158, 2022.

[5] T. L. Vu, D. N. Nguyen, T. A. Luong, and T. D. U Doan, "The impact of supply chain financing on SMEs performance in Global supply chain," *Uncertain Supply Chain Management*, vol. 10, no. 1, pp. 255–270, 2022.

[6] Y. Yang, X. Chu, R. Pang, F. Liu, and P Yang, "Identifying and predicting the credit risk of small and medium-sized enterprises in sustainable supply chain finance: evidence from China," *Sustainability*, vol. 13, no. 10, p. 5714, 2021.

[7] F. Olan, S. Liu, J. Suklan, U. Jayawickrama, and E. O. Arakpogun, "The role of Artificial Intelligence networks in sustainable supply chain finance for food *and drink industry*," *International Journal of Production Research*, pp. 1–16, 2021.

[8] Y. Wu, "Nonparametric inference of the area under ROC curve under two-phase cluster sampling," *Journal of Biopharmaceutical Statistics*, pp. 1–10, 2021.

[9] A. R. Shaik, "Significance of supply chain finance: insights from Saudi Arabia," *Uncertain Supply Chain Management*, vol. 9, no. 3, pp. 539–548, 2021.

[10] W. Yu, C. Y. Wong, R. Chavez, and M. A Jacobs, "Integrating big data analytics into supply chain finance: the roles of information processing and data-driven culture," *International Journal of Production Economics*, vol. 236, Article ID 108135, 2021.

[11] R. Reza-Gharehbagh, S. Asian, A. Hafezalkotob, and C Wei, "Reframing supply chain finance in an era of reglobalization: on the value of multi-sided crowdfunding platforms," *Transportation Research Part E: Logistics and Transportation Review*, vol. 149, Article ID 102298, 2021.

[12] H. Zhang, Y. Shi, and J. Tong, "Online supply chain financial risk assessment based on improved random forest," *Journal of Digital Information Management*, vol. 3, no. 1, pp. 41–48, 2021.

[13] X. Chen, C. Liu, and S. Li, "The role of supply chain finance in improving the competitive advantage of online retailing enterprises," *Electronic Commerce Research and Applications*, vol. 33, Article ID 100821, 2019.

[14] M. J. Lahkani, S. Wang, M. Urbański, and M Egorova, "Sustainable B2B E-commerce and blockchain-based supply chain finance," *Sustainability*, vol. 12, no. 10, p. 3968, 2020.

[15] Z. R. Marak and D. Pillai, "Factors, outcome, and the solutions of supply chain finance: review and the future directions[J]," *Journal of Risk and Financial Management*, vol. 12, no. 1, pp. 1–23, 2019.

[16] J. Chen, T. Cai, W. He et al., "A blockchain-driven supply chain finance application for auto retail industry," *Entropy*, vol. 22, no. 1, p. 95, 2020.

[17] J. Li, S. Zhu, W. Zhang, and L Yu, "Blockchain-driven supply chain finance solution for small and medium enterprises," *Frontiers of Engineering Management*, vol. 7, no. 4, pp. 500–511, 2020.

[18] S. Li and X. Chen, "The role of supply chain finance in third-party logistics industry: a case study from China," *International Journal of Logistics Research and Applications*, vol. 22, no. 2, pp. 154–171, 2019.

[19] F. Wang, L. Ding, H. Yu, and Y. Zhao, "Big data analytics on enterprise credit risk evaluation of e-Business platform," *Information Systems and E-Business Management*, vol. 18, no. 3, pp. 311–350, 2020.

[20] Z. Zhao, D. Chen, L. Wang, and C Han, "Credit risk diffusion in supply chain finance: a complex networks perspective," *Sustainability*, vol. 10, no. 12, p. 4608, 2018.

[21] E. Hofmann, U. M. Strewe, and N. Bosia, "Discussion—how does the full potential of blockchain technology in supply chain finance look like?" *Chain Finance and Blockchain Technology*, Springer, Cham, pp. 77–87, 2018.

[22] M. Du, Q. Chen, J. Xiao, H. Yang, and X Ma, "Supply chain finance innovation using blockchain," *IEEE Transactions on Engineering Management*, vol. 67, no. 4, pp. 1045–1058, 2020.

[23] Z. Wen, H. Liao, E. Kazimieras Zavadskas, and A Al-Barakati, "Selection third-party logistics service providers in supply chain finance by a hesitant fuzzy linguistic combined compromise solution method," *Economic research-Ekonomska istraživanja*, vol. 32, no. 1, pp. 4033–4058, 2019.

[24] F. Jia, C. Blome, H. Sun, Y. Yang, and B Zhi, "Towards an integrated conceptual framework of supply chain finance: an information processing perspective," *International Journal of Production Economics*, vol. 219, pp. 18–30, 2020.

[25] F. Caniato, M. Henke, and G. A. Zsidisin, "Supply chain finance: historical foundations, current research, future developments," *Journal of Purchasing and Supply Management*, vol. 25, no. 2, pp. 99–104, 2019.

[26] L. Zhao and A. Huchzermeier, *Supply Chain Finance, EURO Advanced Tutorials on Operational Research*, pp. 105–119, Springer, Cham, 2018.

[27] Z. Ali, B. Gongbing, A. Mehreen, and U Ghani, "Predicting firm performance through supply chain finance: a moderated and mediated model link," *International Journal of Logistics Research and Applications*, vol. 23, no. 2, pp. 121–138, 2020.

[28] T. T. T. Doan and T. N. Bui, "Nonlinear impact of supply chain finance on the performance of seafood firms: a case study from Vietnam," *Uncertain Supply Chain Management*, vol. 8, no. 2, pp. 267–272, 2020.

[29] C. Meucci and L. Carratoni, "Identification of the majolica polychromatic decoration by IRFC methodology," *Journal of Archaeological Science: Report*, vol. 8, pp. 224–234, 2016.

[30] H. F. Elmanizar, A. T. Nugraha, A. Yakub, H. Fitri, and B. Priyo Cahyono, "The application of agency theory in supply chain finance: a case of Indonesian manufacturing firms[J]," *International Journal of Supply Chain Management*, vol. 8, no. 3, pp. 23–32, 2019.

[31] Y. Wang, F. Jia, T. Schoenherr, and Y Gong, "Supply chain-based business model innovation: the case of a cross-border E-commerce company," *Sustainability*, vol. 10, no. 12, p. 4362, 2018.

[32] T. N. Bui, "How do financial leverage and supply chain finance influence firm performance? Evidence from

Hindawi
Security and Communication Networks
Volume 2024, Article ID 9829542, 1 page
https://doi.org/10.1155/2024/9829542

Retraction

Retracted: Model Construction of Hierarchical Polarization Characteristics Combined with Social E-Commerce Consumer Behavior

Security and Communication Networks

Received 8 January 2024; Accepted 8 January 2024; Published 9 January 2024

This article has been retracted by Hindawi following an investigation undertaken by the publisher [1]. This investigation has uncovered evidence of one or more of the following indicators of systematic manipulation of the publication process:

(1) Discrepancies in scope
(2) Discrepancies in the description of the research reported
(3) Discrepancies between the availability of data and the research described
(4) Inappropriate citations
(5) Incoherent, meaningless and/or irrelevant content included in the article
(6) Manipulated or compromised peer review

The presence of these indicators undermines our confidence in the integrity of the article's content and we cannot, therefore, vouch for its reliability. Please note that this notice is intended solely to alert readers that the content of this article is unreliable. We have not investigated whether authors were aware of or involved in the systematic manipulation of the publication process.

In addition, our investigation has also shown that one or more of the following human-subject reporting requirements has not been met in this article: ethical approval by an Institutional Review Board (IRB) committee or equivalent, patient/participant consent to participate, and/or agreement to publish patient/participant details (where relevant).

Wiley and Hindawi regrets that the usual quality checks did not identify these issues before publication and have since put additional measures in place to safeguard research integrity.

We wish to credit our own Research Integrity and Research Publishing teams and anonymous and named external researchers and research integrity experts for contributing to this investigation.

The corresponding author, as the representative of all authors, has been given the opportunity to register their agreement or disagreement to this retraction. We have kept a record of any response received.

References

[1] Q. Zhang and J. Yang, "Model Construction of Hierarchical Polarization Characteristics Combined with Social E-Commerce Consumer Behavior," *Security and Communication Networks*, vol. 2022, Article ID 9666677, 11 pages, 2022.

Hindawi
Security and Communication Networks
Volume 2022, Article ID 9666677, 11 pages
https://doi.org/10.1155/2022/9666677

Research Article

Model Construction of Hierarchical Polarization Characteristics Combined with Social E-Commerce Consumer Behavior

Quan Zhang and Jian Yang

Chuzhou Polytechnic, Chuzhou 239000, China

Correspondence should be addressed to Quan Zhang; zhangquan@chzc.edu.cn

Received 24 March 2022; Accepted 7 May 2022; Published 29 May 2022

Academic Editor: Fang Liu

In order to analyze the consumer behavior of social e-commerce, this article attempts to explore the irrational consumer behavior factors that affect the audience in the live broadcast of e-commerce Internet celebrities. This paper predicts and analyzes the consumption behavior of social e-commerce and combines the characteristics of hierarchical planning to intelligently process the system to improve the effectiveness of the system. Moreover, this paper constructs a social e-commerce consumer behavior prediction model based on hierarchical polarization characteristics, researches and analyzes multiple factors and performance, and builds an intelligent simulation model. The analysis of the test results shows that the social e-commerce consumer behavior prediction model based on the hierarchical polarization characteristics proposed in this article is effective and can play an important role in the prediction of social consumer behavior.

1. Introduction

Social networks can help social users maintain and expand personal connections. Its biggest feature is the "relationship" between people and spread through word of mouth to influence those around us who have a relationship with us. This relationship includes blood relationship, family relationship, friend relationship, neighbor relationship, colleague relationship, alumni relationship, fellow country relationship, and even netizen relationship. The essence of this "relationship" is trust, which means that the essence of social networks is the trust relationship between people. Because social networks successfully combine interpersonal relationships and word-of-mouth communication, users share product information or value-added services through social networks to create a word-of-mouth effect for corporate products or services [1].

Whether it is socialized e-commerce using social networks or other social media, social attributes are key. Social e-commerce is still an emerging field; even in the world, there is no very successful social e-commerce website. Moreover, the proportion of users sharing shopping information through social applications in my country is still relatively small. However, due to the large number of Internet users using social media and the unique shopping experience of social e-commerce, social e-commerce will be the trend of future e-commerce development. With the rise of online celebrity live broadcasts, social e-commerce has become an important type of e-commerce [2].

First of all, with the development of the Internet era, today's mobile Internet era has entered a mature period, and the value of information needs to be driven by traffic. Internet celebrities are a newly born group in this new media era, such groups often have millions or even tens of millions of fans, and they have traffic characteristics [3].

Nowadays, live broadcasting is becoming more and more common, and the transmission of information through live broadcasting can be more vivid and intuitive, and give the audience a sense of "3D interpretation." Moreover, the live broadcast method is very simple, the operation is very easy, and the threshold for becoming a self-media is relatively low. As long as you have an idea, as long as you have a mobile phone or a computer, you can live webcast. This is a creative mode of completely user-

generated content. This mode also breaks people's understanding of traditional live broadcasts, and difference and TV shopping. Moreover, in the current live broadcast field of Internet celebrities, the two-way interaction between the anchor and the audience is also a feature born with the development of new media. It is not available in the traditional TV shopping marketing model. TV shopping is just the moderator conducts one-way information transmission. Internet celebrities are a type of group with great potential and liquidity. The influence of this type of group in the new media era cannot be ignored. Internet celebrities choose the marketing model of webcast to increase the popularity and influence of platforms, brands, or individuals, and then monetize through traffic to facilitate transactions and ultimately achieve their marketing goals. This behavior can be called e-commerce Internet celebrities live streaming. ① In the live broadcast of e-commerce Internet celebrities, the audience will have a strong desire to buy, and irrational consumption behaviors are endless.

Based on the above analysis, this article conducts a predictive analysis of social e-commerce consumer behavior, combines the characteristics of hierarchical planning to intelligently process the system to improve the system's work effect, and verifies the method proposed in this article through experiments.

2. Related Work

Literature [4] equates irrational consumption behaviors with unplanned consumption behaviors and believes that consumers' rational consumption behaviors should be planned purchases of goods. If the purchased goods are not in the original plan, you can say this irrational consumer behavior has occurred. Literature [5] believes that emotions can cause irrational consumer behaviors. When irrational consumer behaviors occur, their characteristics are often impulsive and reckless. In irrational consumer behavior, consumers' emotions are considered uncontrollable. The literature [6] has great consistency in the definition of irrational consumption behaviors and believes that irrational consumption behaviors are purposeless and strongly impulsive. Literature [7] believes that individuals who make irrational consumer behaviors have a certain degree of vanity, and they want to highlight their own identity and status through their consumption power. There are also foreign researchers who believe that irrational consumption behavior has the characteristics of herding, which is manifested in the fact that consumers lack independent opinions and blindly follow the public's choices when purchasing behaviors. Literature [8] believes that some consumers have a herd mentality and believe that following the masses to purchase goods can reduce the purchase risk, but these consumers do not know their true needs. Irrational consumption means that consumers fail to carefully examine their true needs and do not consider the maximum utility of commodities.

For the research on audience users' motivation, there are many related researches on the audience users' motivation to watch the game live broadcast; of course, it is not limited to the related research on the game live broadcast field. These researches are based on various webcast platforms [9]. Research has found that users on these two social media-based webcasting platforms are often more inclined to watch the live broadcasts they follow on social media [10]. Aiming at the audience's willingness to watch the game live broadcast, the literature [11] found that emotional motivation, cognitive motivation, individual integration, social integration, and stress release are the five viewer motivations that affect the audience's watching game live broadcast. Literature [12] has conducted related research on the relationship between user needs and user viewing behavior, and the theory used is the theory of use and satisfaction. A large amount of data is collected and conducted in-depth analysis of the data, and established a model that can predict the number of barrage speeches based on the number of audiences. The research believes that analyzing user chat-related data can better understand the behavior of audience users.

In recent years, a lot of related research on anchors has also appeared. Literature [13] studied the anchors' motivation for live broadcasting. Based on the perspective of individual motivation and social capital, they found that self-expression and self-identification motivation, information propaganda motivation, and monetary gain motivation are the main factors that anchors are willing to live broadcast. There are also studies on the factors that affect the audience's use of live broadcast from the perspective of the audience. Literature [14] studies the user's willingness to use live broadcast from four perspectives, namely, the perspectives of immersion, entertainment, social interaction, and recognition. Based on the dual identity framework, relevant researches have been conducted on the factors that influence viewers' choice to continue watching live broadcasts from the perspective of individual experience and common experience. There are also studies that have begun to pay attention to the behavior of users in the live broadcast situation. Literature [15] studied the influence of the motivation of the live broadcast viewers on the live broadcast conforming behavior of the viewers.

Literature [16] found that customer fit in live broadcast can promote customers' consumption of virtual gifts. Through literature reading, we have a deep understanding of the concept of customer fit. The literature [17] believes that customer fit is a dynamic psychological process in which attitude fit positively affects behavior fit. Literature [18] proposes that customer fit is a mental state, which refers to the mental state generated by interacting with core objects in the core service relationship and co-creating customer experience. Literature [19] found that users' virtual interactive online communities have a positive impact on customer fit. Literature [20] proposes that the impact of this interaction on customer engagement is also applicable to online game scenarios.

3. Analysis of Hierarchical Plan Characteristics

The SCMA iterative decoding model of polarization code encoding is shown in Figure 1. In this system, the external information output by the polarization code decoder needs to be fed back to the SCMA detector. However, the

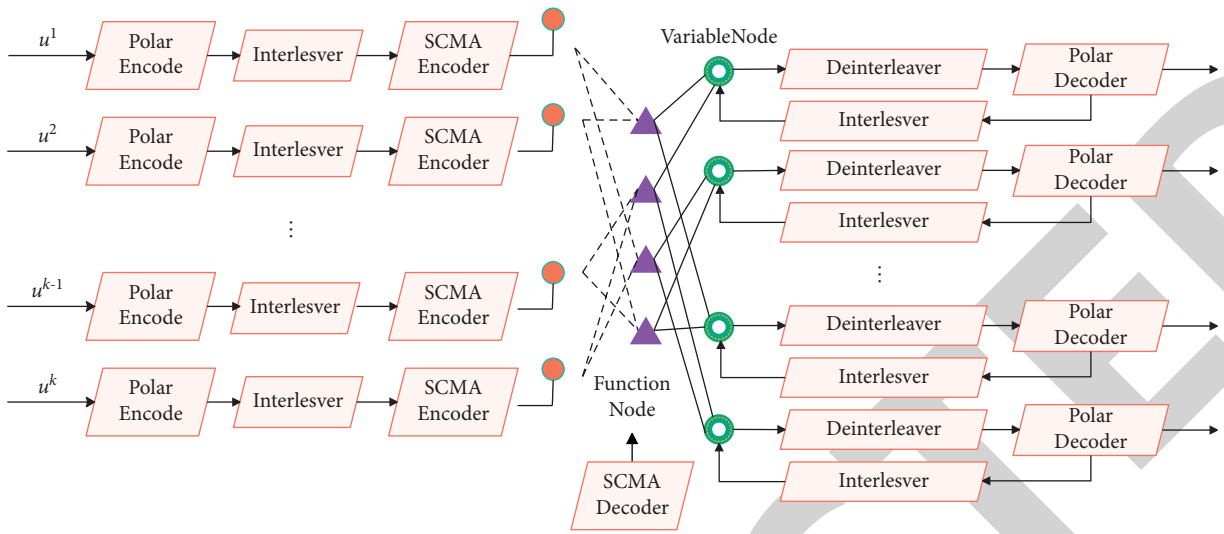


Figure 1: SCMA simplified system model encoded by polarization codes.

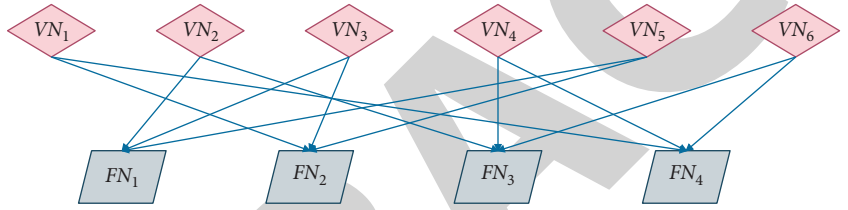


Figure 2: Factor graph corresponding to SCMA users and resource points.

SCMA detector reuses this information as a priori information to perform iterative decoding until the preset maximum number of iterations is reached or the system converges.

This article will discuss the widely discussed and published SCMA system model in which 6 user data are carried on 4 resource points. The relationship between users and resource points is represented by the factor graph in Figure 2.

In SCMA modulation, each user selects a codeword in the codebook according to the encoded bits. For example, if the modulation order of the system is M, then the bit stream of the j-th user performs multi-dimensional codeword mapping for each group of $Q = \log_2(M)$ bits. The relationship can be expressed as

$$f^j: B^{\log_2(M)} \longrightarrow \mathbf{x}^j, \mathbf{x}^j \in \chi^j. \tag{1}$$

Among them, $B = \{0, 1\}$ is a set of binary bits, χ^j is a codeword set of the j-th user, and $\mathbf{x}^j = [x_1^j x_2^j \ldots x_N^j]^T$ is an N-dimensional complex codeword, and it is satisfied that the number of 0 elements in the codeword is greater than or equal to the number of nonzero elements. Each user maps the bit group to the same N resource points and then superimposes them on the channel to form a nonorthogonal transmission signal.

According to the above modulation principle, the received signal of the SCMA system is

$$\mathbf{y} = \sum_{j=1}^{J} \operatorname{diag}\left(\mathbf{h}^j\right) \cdot \mathbf{x}^j + \mathbf{n}. \tag{2}$$

Among them, $\mathbf{y} = [y_1 y_2 \ldots y_N]^T$ is the acceptance vector of the channel, $\mathbf{h}^j = [h_1^j h_2^j \ldots h_N^j]^T$ is the channel gain between the j-th user and the base station, and $\mathbf{n} = [n_1 n_2 \ldots n_N]^T$ is a complex Gaussian white noise signal with a zero mean variance of N_0.

SCMA's MPA detection algorithm is also a belief propagation algorithm, similar to BP decoding, which is detected in an iterative manner. The main steps of the algorithm are as follows:

3.1. Joint Conditional Probability Calculation. According to the system model, the conditional probability of any resource node n can be obtained as

$$d_n\left(\mathbf{x}^i, \mathbf{x}^j, \mathbf{x}^k\right) = -\frac{1}{N_0}\left\| y_n - \left(h_n^i x_n^i + h_n^j x_n^j + h_n^k x_n^k\right)\right\|^2, \tag{3}$$

$$P\left(y_n | \mathbf{x}^i, \mathbf{x}^j, \mathbf{x}^k\right) = \exp\left(d_n\left(\mathbf{x}^i, \mathbf{x}^j, \mathbf{x}^k\right)\right). \tag{4}$$

Among them, users i, j, and k are connected to the resource node n.

3.2. Resource Node Update. According to the joint conditional probability obtained by the above steps, the edge

condition probability can be calculated by the Bayes criterion, as shown below:

$$I_{F_n}^{V_k}(\mathbf{x}^k) = P(y_n|\mathbf{x}^k) = \sum_{x'\in\mathbf{x}'}\sum_{\mathbf{x}'\in\mathbf{x}'} P(y_n|\mathbf{x}^i,\mathbf{x}^j,\mathbf{x}^k)\cdot I_{V_i}^{F_n}(\mathbf{x}^i)\cdot I_{V_j}^{F_n}(\mathbf{x}^j). \tag{5}$$

Among them, $\mathbf{x}^k \in \chi^k$, $I_{V_i}^{F_n}(\mathbf{x}^i)$, and $I_{V_j}^{E_n}(\mathbf{x}^j)$ represent the information delivered by users i and j to resource node n. In the first iteration, the probability of initializing variable nodes to resource nodes is

$$I_{V_j}^{F_n}(\mathbf{x}^j) = \frac{1}{M}, \quad \forall n \in \{1,\ldots,N\}, \forall j \in \{1,\ldots,J\}. \tag{6}$$

Among them, M is the modulation order.

3.3. Variable Node Update. The update formula for the variable node of degree 2 is

$$I_{V_k}^{F_n}(\mathbf{x}^k) = \frac{I_{F_m}^{V_k}(\mathbf{x}^k)}{\sum_{\widehat{\mathbf{x}}^k\in\mathbf{x}^k} I_{F_m}^{V_k}(\widehat{\mathbf{x}}^k)}. \tag{7}$$

In fact, the symbol probability from resource node m to variable node k is normalized.

3.4. Soft Information Calculation. When the iterative process is over, the soft information is calculated, and the soft information calculation formula for the m-th bit of the j-th user is

$$\mathrm{LLR}(b_q^j) = \ln\left(\frac{P(b_q^j=0)}{P(b_q^j=1)}\right) = \ln\left(\sum_{x'\cdot j_q^j=0} Q_j(\mathbf{x}^j)\right) - \ln\left(\sum_{x'\cdot k_q=1} Q_j(\mathbf{x}^j)\right). \tag{8}$$

Among them, there are

$$Q_j(\mathbf{x}^j) = I_{F_n}^{V_j}(\mathbf{x}^j)\cdot I_{F_m}^{V_j}(\mathbf{x}^j). \tag{9}$$

Among them, n and m are two resource nodes connected with variable node j.

The MPA detection algorithm has the best detection performance. However, this algorithm involves a large number of divisions and multiplications, the computational complexity is extremely high, and it is difficult to apply to the actual mobile communication system. Therefore, an MPA detection algorithm based on the logarithmic domain is proposed, which simplifies the four major steps of MPA detection.

3.5. Channel Euclidean Distance Calculation. Since the entire calculation process has moved from the probability domain to the logarithmic domain, this step only needs to be calculated using formula (3), and the step of shifting to the probability domain is omitted.

3.6. Resource Node Update. The algorithm takes the natural logarithm of the probability information at the resource node and then uses the Jacobi approximation to simplify the formula as

$$\begin{aligned} II_{F_*}^{V_k}(\mathbf{x}^k) &= \ln\left(I_{F_n}^{V_k}(\mathbf{x}^k)\right), \\ &= \ln\left(\sum_{x'\in x^i}\sum_{x'\in x'} P(y_n|\mathbf{x}^i,\mathbf{x}^j,\mathbf{x}^k)\cdot I_{V_i}^{F_n}(\mathbf{x}^i)\cdot I_{V_j}^{F_n}(\mathbf{x}^j)\right) \\ &= \ln\left(\sum_{x'\in\mathcal{X}'\mathbf{x}'\in\mathbf{x}'} \exp\left(d_n(\mathbf{x}^i,\mathbf{x}^j,\mathbf{x}^k) + LI_{V_i}^{F_j}(\mathbf{x}^i) + LI_{V_j}^{F_j}(\mathbf{x}^j)\right)\right) \\ &\approx \max_{x'\in\mathcal{X}',\mathbf{x}'\in\mathbf{x}'}\left(d_n(\mathbf{x}^i,\mathbf{x}^j,\mathbf{x}^k) + LI_{V_i}^{F_n}(\mathbf{x}^i) + LI_{V_j}^{F_n}(\mathbf{x}^j)\right). \end{aligned} \tag{10}$$

3.7. Variable Node Update. Same as the second step, the simplified formula is

$$\begin{aligned} LI_{V_k}^{F_n}(\mathbf{x}^k) &= \ln\left(I_{V_k}^{F_n}(\mathbf{x}^k)\right), \\ &= LI_{F_m}^{V_k}(\mathbf{x}^k) - \ln\left(\sum_{\widehat{x}^k\in\mathbf{x}^k} I_{F_m^k}^{V_k}(\widehat{\mathbf{x}}^k)\right) \\ &\approx LI_{F_m}^{V_k}(\mathbf{x}^k) - \max_{\widehat{x}^k\in\mathbf{x}^k}\left(LI_{F_m}^{V_k}(\widehat{\mathbf{x}}^k)\right). \end{aligned} \tag{11}$$

3.8. Soft Information Calculation. In the MPA algorithm, the calculation of soft information is carried out in the logarithmic domain, and then, the Jacobi approximate simplified formula is also used as

$$\begin{aligned} \mathrm{LLR}(b_m^j) &= \ln\left(\sum_{x':\, b_m=0} Q_j(\mathbf{x}^j)\right) - \ln\left(\sum_{x':\, b_m^j=1} Q_j(\mathbf{x}^j)\right) \\ &= \max_{x',j_m'=0}\left\{LQ_j(\mathbf{x}^j)\right\} - \max_{x',b_m'=1}\left\{LQ_j(\mathbf{x}^j)\right\}. \end{aligned} \tag{12}$$

Among them, there are

$$\mathrm{LQ}_j(\mathbf{x}^j) = LI_{F_n}^{V_j}(\mathbf{x}^j) + LI_{F_m}^{V_j}(\mathbf{x}^j). \tag{13}$$

Polar codes use probability domain BP decoding algorithm, while SCMA uses MPA algorithm, and the whole system has the best decoding performance.

Due to the addition of prior information, the MPA detection algorithm needs to correct the steps at the variable node update, as shown below:

$$I_{V_k}^{F_n}(\mathbf{x}^k) = \frac{P_a(\mathbf{x}^k)\cdot I_{F_m}^{V_k}(\mathbf{x}^k)}{\sum_{\widehat{\mathbf{x}}^k\in\mathbf{x}^k} P_a(\widehat{\mathbf{x}}^k)\cdot I_{F_m}^{V_k}(\widehat{\mathbf{x}}^k)}. \tag{14}$$

Among them, the prior information of the $p_a(x^k)$ detector is calculated from the external information output by the decoder, and the calculation formula is

$$P_a\left(\mathbf{x}^k\right) = \prod_{i=1}^{i=Q} P_e\left(b_i^k\right), \quad \mathbf{b}^k = f^{-1}\left(\mathbf{x}^k\right). \tag{15}$$

Among them, $p_e(b_i^k)$ cannot be obtained directly from the output of the polarization code decoder. Due to the polarization characteristics of the polarization code channel, it needs to be processed before it can be used for the calculation of a priori information. Using the generator matrix G in the encoder, when $G(I, j) = 1$, it can be calculated by the following formula:

$$P_e\left(b^k\right) = 0.5 \cdot \left(1 - \prod_{G(,,j)=1} \left(1 - 2P_{\text{Polar}}\left(b^k\right)\right)\right). \tag{16}$$

After the iteration of the SCMA detection part is completed, the soft information calculation steps are rewritten as

$$\widehat{P}\left(b_q^j = i\right) = \sum_{\mathbf{x}^j : b_q^j = i} Q_j\left(\mathbf{x}^j\right), \quad i \in \{0, 1\}. \tag{17}$$

Then, it is normalized, and you can get

$$P\left(b_q^j = 0\right) = \frac{\widehat{P}\left(b_q^j = 0\right)}{\widehat{P}\left(b_q^j = 0\right) + \widehat{P}\left(b_q^j = 1\right)}. \tag{18}$$

The probability value output by the detector is passed as the channel probability to the polarization code decoder for iterative decoding. The algorithm details are shown in Table 1. Among them, the code length of the polarization code is L, $\mathbf{x}_l^k$ represents the l-th SCMA symbol of the k-th user, and I, I_{SCMA}, and I_{Poar} represent the number of system iterations, the number of SCMA iterations, and the number of iterations of the polarization code, respectively. $f(\cdot)$ and $g(\cdot)$ have been introduced in the BP decoding algorithm of the probability domain polarization code in chapter 2.

Iterative decoding in the logarithmic domain means that the polarization code uses the original BP or min-sum-based BP decoding algorithm, while the SCMA uses the max log-MPA algorithm. In this algorithm, the variable node update formula is

$$\begin{aligned} \text{LI}_{V_i^{F_i}}\left(\mathbf{x}^k\right) &= LI_{F_m}^{V_k}\left(\mathbf{x}^k\right) - \ln\left(\sum_{\widehat{x}^i \in X^k} P_a\left(\widehat{\mathbf{x}}^k\right) \cdot I_{F_m}^{V_k}\left(\widehat{\mathbf{x}}^k\right)\right) \\ &\approx La\left(\mathbf{x}^k\right) + LI_{F_m}^{V_k}\left(\mathbf{x}^k\right) - \max_{\widehat{x}^k \in \mathbf{x}^k}\left(La\left(\widehat{\mathbf{x}}^k\right) + LI_{F_m}^{V_k}\left(\widehat{\mathbf{x}}^k\right)\right). \end{aligned} \tag{19}$$

Among them, $La(\mathbf{x}^k)$ is the logarithm and prior probability of the SCMA symbol. Through the external information output by the polarization code decoder, we get

$$La\left(\mathbf{x}^k\right) = \sum_{i=1}^{Q} L_e^T\left(b_i^k\right), \quad \mathbf{b}^k = f^{-1}\left(\mathbf{x}^k\right). \tag{20}$$

Among them, $L_e^T(b_i^k)$ represents the prior information of the i-th bit of the k-th user, which is obtained by processing the external information output by the decoder:

Table 1: Evaluation of the performance improvement effect of the consumption behavior prediction model.

Number	Performance improvement	Number	Performance improvement
1	83.50	16	78.31
2	68.52	17	67.43
3	74.92	18	75.57
4	65.41	19	68.46
5	72.93	20	74.46
6	74.54	21	71.99
7	70.08	22	72.24
8	81.10	23	65.99
9	82.52	24	64.41
10	68.18	25	81.58
11	79.59	26	83.30
12	82.70	27	84.81
13	78.20	28	67.08
14	72.17	29	69.60
15	70.00	30	64.32

$$\text{LLR}\left(b^k\right) = \min_{G(,j)=1}\left(\text{LLR}_{\text{Polar}}\left(b^k\right)\right) \prod_{G(,j)=1} \text{sign}\left(\text{LLR}_{\text{Polar}}\left(b^k\right)\right). \tag{21}$$

The soft information output by the SCMA detector is consistent with the calculation in the previous section. In summary, the iterative decoding process in the logarithmic domain is consistent with the iterative decoding process, and the difference lies in some calculation formulas.

The MIMO system based on the joint detection and decoding algorithm can effectively improve the decoding performance of the system. Due to the similarity between SCMA and MIMO, this paper proposes a combination of the factor graph in the polarization code BP decoding algorithm and the SCMA factor graph to form a joint factor graph, as shown in Figure 3. Based on the factor graph, the optimal joint detection and decoding algorithm and the log-domain joint detection and decoding algorithm are proposed.

In iterative detection and decoding, the whole process can be divided into several steps. First, SCMA completes detection based on channel information. Then, the detector inputs the information to the polarization code decoder as the channel information of the decoder for decoding. Then, the polarization code decoder transmits the output external information to the detector as a priori information of the SCMA detector to perform detection again. Subsequently, the detector outputs new information and then passes it to the decoder. In this way, the algorithm iterates until the maximum number of iterations or meets a certain stopping criterion.

Different from iterative detection and decoding, in joint detection and decoding, the message is passed directly on the joint factor graph, and the whole detection and decoding process is decoded through joint detection and decoding. The process is as follows.

3.8.1. SCMA Resource Node Update. The update formula of the SCMA resource node in the joint factor graph is

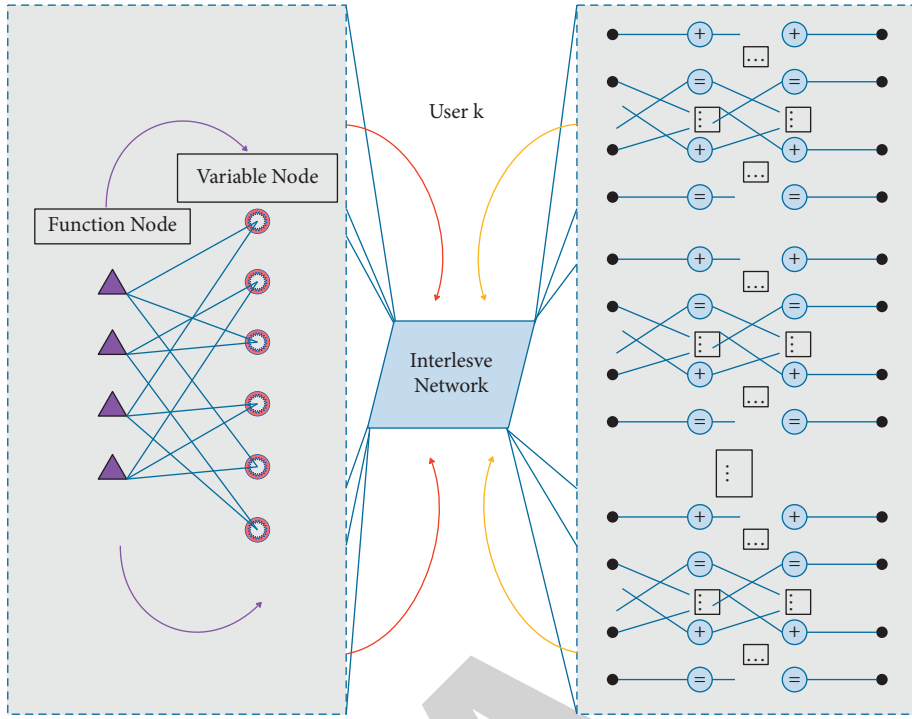


Figure 3: Joint factor graph.

$$I_{F_n}^{V_k}\left(\mathbf{x}_l^k\right) = P\left(y_n^l|\mathbf{x}_l^k\right) = \sum_{\mathbf{x}_i^i \in \mathcal{X}^i \mathbf{x}_i \in \mathbf{x}^j} P\left(y_n|\mathbf{x}_l^i, \mathbf{x}_l^j, \mathbf{x}_l^k\right) \cdot I_{V_i}^{F_n}\left(\mathbf{x}_l^i\right) \cdot I_{V_j}^{F_n}\left(\mathbf{x}_l^j\right), \quad 1 \le l \le \frac{L}{Q}. \tag{22}$$

3.8.2. Polarization Code Factor Graph Update. In this step, the probability domain BP decoding iteration of the polarization code is completed once, and the iteration formula is

$$\begin{cases} L_{i,j}^t = f\left(L_{i+1,2j-1}^{t-1}, g\left(L_{i+1,2j}^{t-1}, R_{i,j+N/2}^{t-1}\right)\right), \\ L_{i,j+N/2}^t = g\left(f\left(R_{i,j}^{t-1}, L_{i+1,2j-1}^{t-1}\right), L_{i+1,2j}^{t-1}\right), \\ R_{i+1,2j-1}^t = f\left(R_{i,j}^{t-1}, g\left(L_{i+1,2j}^{t-1}, R_{i,j+N/2}^{t-1}\right)\right), \\ R_{i+1,2j}^t = g\left(f\left(R_{i,j}^{t-1}, L_{i+1,2j-1}^{t-1}\right), R_{i,j+N/2}^{t-1}\right). \end{cases} \tag{23}$$

Among them, $f(\bullet)$ and $g(\bullet)$ are the calculation formulas of the probability domain BP. During the initial iteration, the probability of the joint variable node being transmitted to the polarization code is set to 0.5.

3.8.3. Joint Variable Node Update. In this step, the information of the leftmost node of the polarization code factor graph is converted from bit probability to symbol probability, as shown below:

$$P_e\left(b^k\right) = 0.5 \cdot \left(1 - \prod_{G(i,j)=1} \left(1 - 2P_{\text{Polar}}\left(b^k\right)\right)\right), \quad P_a\left(\mathbf{x}_l^k\right) = \prod_{i=1}^{i=Q} P_e\left(b_i^{k,l}\right), \quad \mathbf{b}^{k,l} = f^{-1}\left(\mathbf{x}_l^k\right), \mathbf{x}_l^k \in \chi^k. \tag{24}$$

The algorithm passes it to the SCMA variable node for update. The formula is

$$I_{V_k}^{F_n}\left(\mathbf{x}_l^k\right) = \frac{P_a\left(\mathbf{x}_l^k\right) I_{F_m}^{V_k}\left(\mathbf{x}_l^k\right)}{\sum_{\widehat{\mathbf{x}}_i \in \mathbf{x}^k} P_a\left(\widehat{\mathbf{x}}_l^k\right) \cdot I_{F_m}^{V_k}\left(\widehat{\mathbf{x}}_l^k\right)}. \tag{25}$$

The symbol probability that the algorithm passes to the rightmost node of the polarization code factor graph is

$$Q_j\left(\mathbf{x}_l^j\right) = I_{F_n}^{V_j}\left(\mathbf{x}_l^j\right) \cdot I_{F_m}^{V_j}\left(\mathbf{x}_l^j\right), \quad n, m \in \zeta_j \tag{26}$$

The algorithm converts the symbol probability to the bit probability required by the polarization code factor graph.

$$\widehat{P}_{\text{VNO}}\left(b_q^{j,l} = i\right) = \sum_{\mathbf{x}_i, b_q^j, i=i} Q_j\left(\mathbf{x}_l^j\right), \quad i \in \{0,1\}, n, m \in \zeta_j, \quad P_{\text{VNO}}\left(b_q^{j,l} = 0\right) = \frac{\widehat{P}_{\text{VNO}}\left(b_q^{j,l} = 0\right)}{\left(\widehat{P}_{\text{VNO}}\left(b_q^{j,l} = 0\right) + \widehat{P}_{\text{VNO}}\left(b_q^{j,l} = 1\right)\right)}. \tag{27}$$

The above steps are the entire process of one iteration of joint detection and decoding. The algorithm repeats the above steps until the maximum number of iterations is reached or a certain stopping criterion is met.

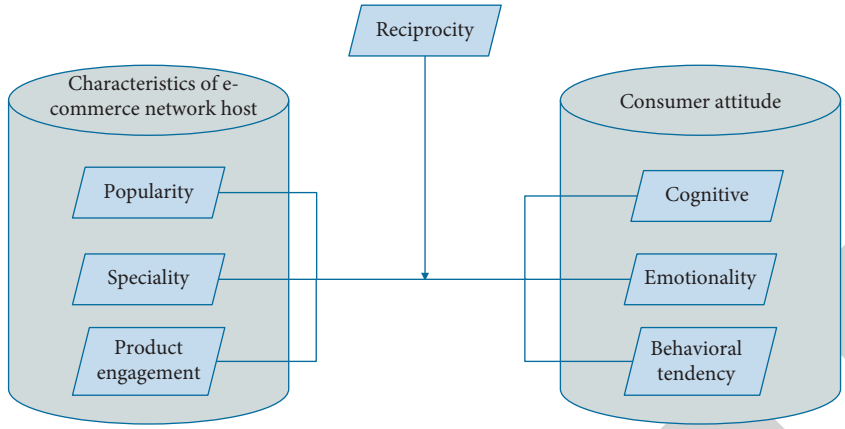


Figure 4: The influence of the characteristics of e-commerce network anchors on consumer attitudes.

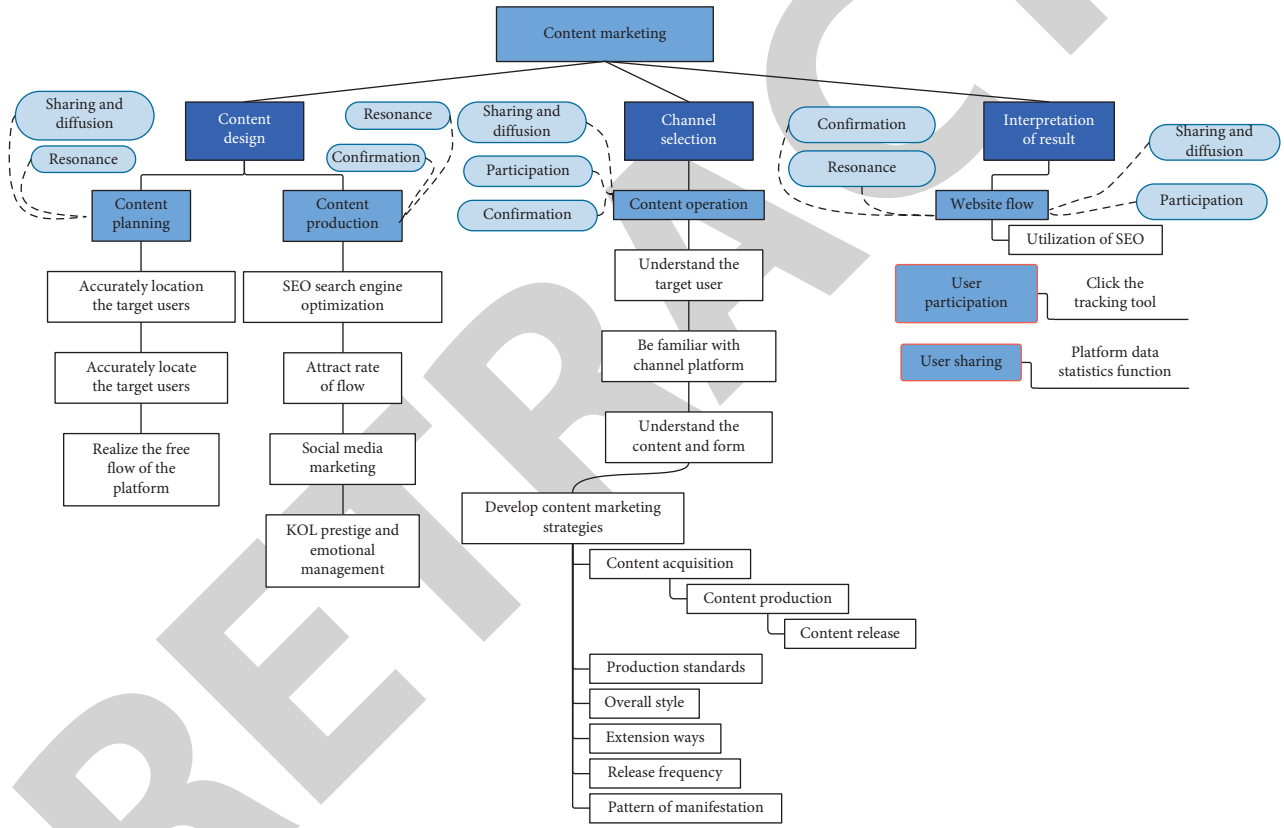


Figure 5: Social e-commerce consumer behavior prediction framework.

4. Social E-Commerce Consumer Behavior Prediction Model Based on Hierarchical Polarization Characteristics

The third part proposes the hierarchical planning feature method, and with the support of this method, the social e-commerce consumer behavior prediction model based on the hierarchical polarization feature is constructed.

This research mainly discusses the influence of the characteristics of e-commerce network anchors on consumer attitudes. According to the previous article, the following model is constructed, as shown in Figure 4.

This article combines the above analysis to construct a social e-commerce consumer behavior prediction framework, as shown in Figure 5.

Irrational consumer behavior is a phenomenon in which consumer behavior is alienated. This phenomenon causes consumption to become the focus of people's lives and triggers the bad social atmosphere of hedonism and money worship. In the daily life of the general public, irrational consumer behavior is common, but the degree is different. Among irrational consumption behaviors, comparison consumption and herd consumption are the most serious. Moreover, sub-healthy consumption patterns are now subtly

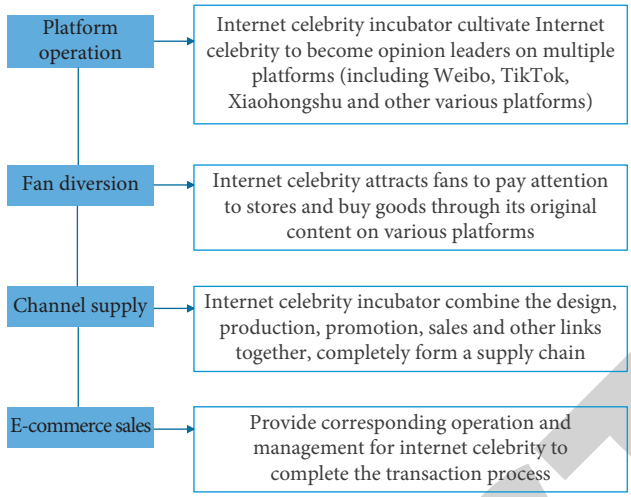


Figure 6: The consumption behavior process of Internet celebrity social e-commerce.

affecting people's daily lives, but many people do not have a clear understanding of irrational consumption behaviors.

Irrational consumer behavior is an unhealthy consumer behavior that is diametrically opposed to rational consumer behavior. According to the definition of rational consumption behavior, we can understand irrational consumption behavior as an individual's purchase behavior that lacks consideration of the maximization of commodity utility under unhealthy consumption concepts and is only for satisfying their own timely enjoyment psychology. People who make irrational consumption usually lack a serious review of their real needs, have no clear specific purchase goals, are easily stimulated and disturbed by the external environment, have no long-term plans for the future, and only focus on short-term psychological experiences. Irrational consumption behavior can be divided into common ones: impulsive consumption, conspicuous consumption, and blind consumption. Such irrational consumer behavior has prompted the emergence of many "shopaholics" who would rather max out dozens of credit cards and buy some things that they basically do not use. This kind of consumption is really a mental illness. The development of e-commerce platforms now allows consumption without leaving the house, which is much more convenient than shopping in the past, which makes this phenomenon even more serious. In fact, this is a kind of psychological abnormality caused by psychological backlog. What this group of people pursue is to get a certain degree of pleasure after consumption.

The Internet celebrity economy is to attract fans through the packaging of Internet celebrities derived from the self-media era through their own unique personality charm and superior skills, and then maintain fan stickiness through regular communication and exchanges with fans. Finally, it uses the fan effect to monetize the traffic, thus forming a complete economic situation of the net celebrity profit chain. Internet celebrities are no longer synonymous with "non-mainstream," and such groups have begun to have their own commercial value in the era of the Internet celebrity economy. The consumption behavior process of Internet celebrity social e-commerce is shown in Figure 6.

Perceived attraction is the subjective feelings of individual consumers about brand community attraction, and it is also the source of self-awareness and classification. Under the "Internet celebrity + live broadcast + e-commerce" model, there are three dimensions including the attraction of Internet celebrities, the attraction of live broadcasts, and the attraction of products. Brand community recognition is the psychological manifestation of self-recognition and classification after perceptual attraction. The repeat purchase intention is the dependent behavior tendency oriented by the brand community identification. This article believes that the attracting source of online celebrity live broadcast e-commerce, that is, perceptual attraction (influencer attraction, live broadcast attraction, product attraction), will lead to consumers' self-recognition and classification (identification of the online celebrity live broadcast e-commerce community), and then generate a corresponding tendency of dependence (repurchase willingness). At the same time, this study also selected age and gender as control variables. The research model is shown in Figure 7.

In this study, SmartPLS2.0 is used for SEM analysis, and the bootstrapping method is used to repeatedly sample 5000 times to test the significance of the path coefficient. The model test results are as follows (see Figure 8).

According to the model test results in Figure 8, first, consumer-brand community identification has a significant impact on consumers' repurchase intentions and explains 67.636% of the variance of repeat purchase intentions. Secondly, the three types of consumer perception (Internet celebrity attraction, live broadcast attraction, and product attraction) under the "Internet celebrity + live broadcast + e-commerce" model have a significant impact on brand community recognition and explain the 72.616% variance of brand community recognition. At the same time, among the three types of perceptual attraction, both live broadcast attraction and product attraction can significantly affect consumers' repurchase intentions, while online celebrity attraction cannot

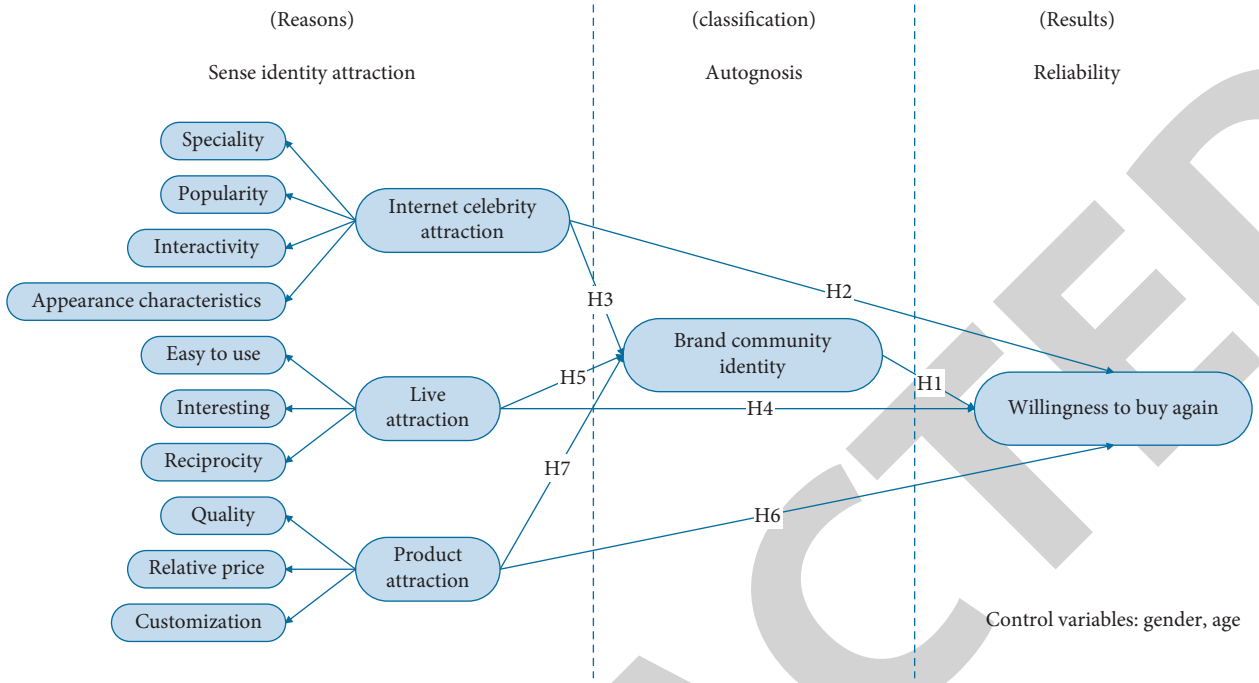
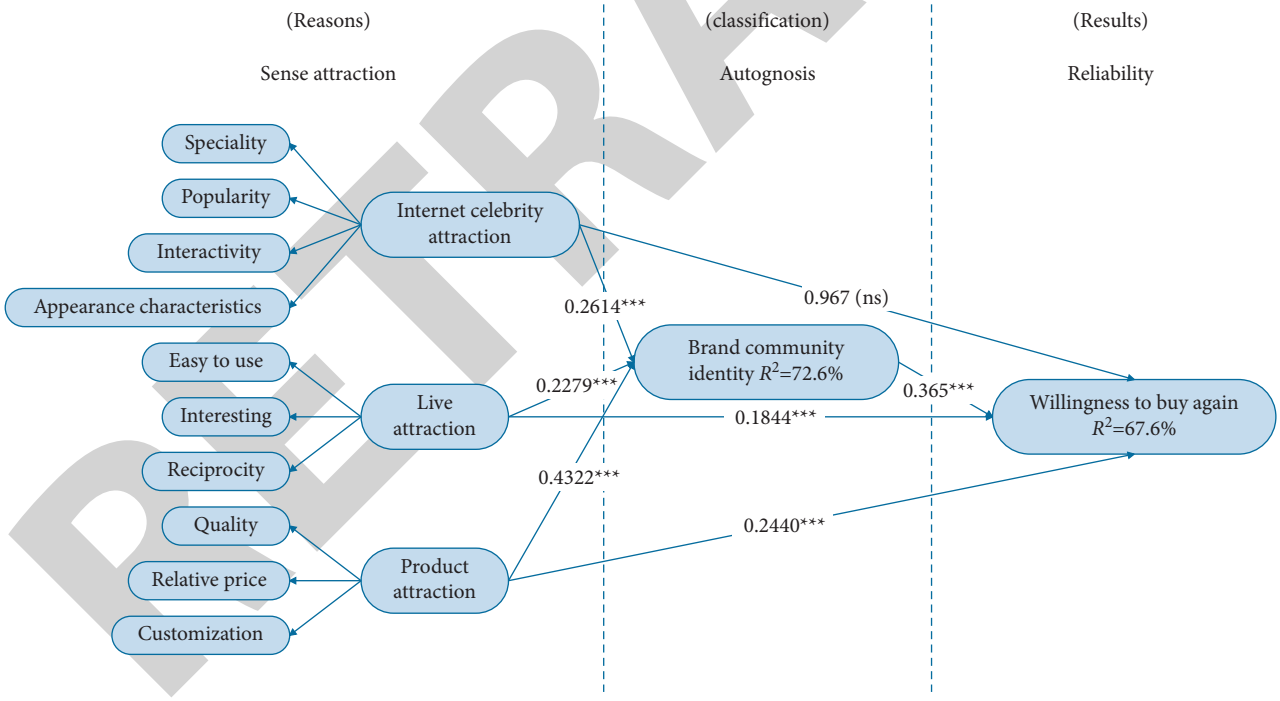


Figure 7: Research model.



(***, p<0.001;**, p<0.01;*, p<0.05;+, p<0.1;ns, Un-remarkable)

Figure 8: Model test results.

directly and significantly affect customers' repurchase intentions, which is inconsistent with the hypothesis.

After constructing the above model, the effect of the social e-commerce consumer behavior prediction model proposed in this paper is verified. First of all, this article verifies the hierarchical characteristics of the system constructed in this article, calculates the performance improvement effect of the system, and validates it through the simulation platform. The results are shown in Table 1 and Figure 9.

From the above research, we can see that the hierarchical characteristics can effectively improve the performance of the system model. On this basis, the social e-commerce

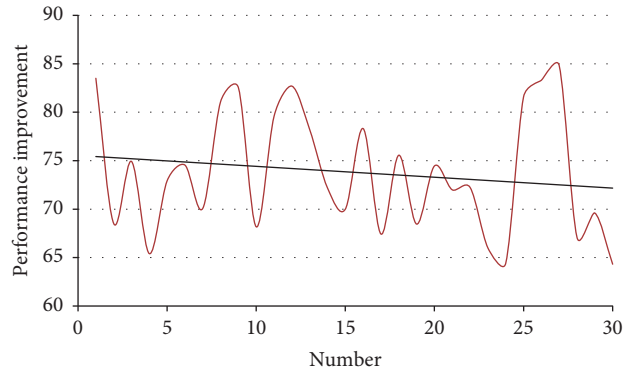


Figure 9: Statistical diagram of system performance improvement evaluation.

Table 2: Effectiveness verification of social e-commerce consumer behavior prediction model based on hierarchical polarization characteristics.

Number	Consumption forecast	Number	Consumption forecast
1	73.9	15	88.0
2	85.1	16	86.6
3	82.7	17	81.0
4	77.7	18	85.0
5	86.0	19	86.8
6	72.6	20	81.8
7	84.1	21	88.7
8	85.5	22	77.0
9	86.2	23	78.3
10	82.4	24	87.6
11	88.3	25	77.2
12	77.2	26	87.6
13	83.2	27	76.5
14	90.2	28	84.3
15	88.0	29	87.0
16	86.6	30	85.0

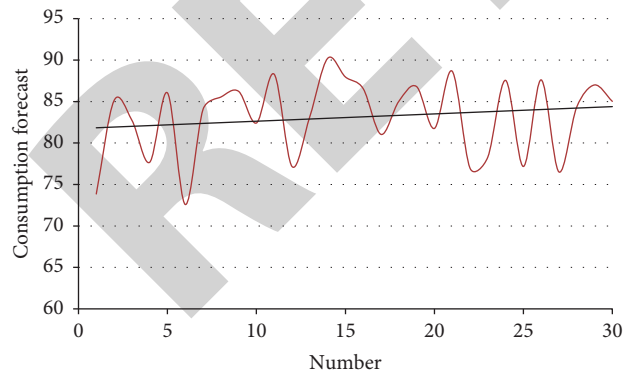


Figure 10: Statistical diagram of the effect of social e-commerce consumer behavior prediction model based on hierarchical polarization characteristics.

consumer behavior prediction model is verified, and data are collected from many current live delivery platforms for experimental analysis. The statistical test results are shown in Table 2 and Figure 10.

From the above research, it can be seen that the social e-commerce consumer behavior prediction model based on the hierarchical polarization characteristics proposed in this paper is effective and can play an important role in the prediction of social consumer behavior.

5. Conclusion

Social e-commerce can help many offline companies and traditional e-commerce companies to learn the current "net celebrity economy" model. Moreover, it promotes these companies to keep pace with the times in the era of new media. In addition, it encourages them to improve their competitiveness while maintaining their own state in this era of extremely high penetration rate of online shopping, and to obtain better returns, so that they will not be slowly banned. Secondly, this article focuses on the influence factors of e-commerce Internet celebrity live broadcast on the audience's irrational consumption and deeply analyzes the characteristics of e-commerce Internet celebrity live broadcast platform and the consumer psychology of the audience. This can help the Internet celebrity group to understand consumers' psychology in depth, help the Internet celebrity group to better establish a communication bridge with consumers to form a more mature and good interaction mechanism, and better use new media to promote sales activities. This article predicts and analyzes the consumption behavior of social e-commerce and combines the characteristics of hierarchical planning to intelligently process the system to improve the effectiveness of the system. The experimental analysis shows that the social e-commerce consumer behavior prediction model based on the layered polarization characteristics proposed in this article is effective and can play an important role in the prediction of social consumer behavior.

Data Availability

The labeled dataset used to support the findings of this study is available from the corresponding author upon request.

Conflicts of Interest

The authors declare no conflicts of interest.

Acknowledgments

This study was sponsored by 2020 Key Issues of Humanities and Social Sciences in Colleges and Universities in Anhui Province: Research on Structural Reform of the Joint Development of Rural E-Commerce and E-Commerce Logistics Enterprises in Chuzhou City, Anhui Province (No. SK2020A0763).

References

[1] J. Anitha and M. Kalaiarasu, "Optimized machine learning based collaborative filtering (OMLCF) recommendation system in e-commerce," *Journal of Ambient Intelligence and Humanized Computing*, vol. 12, no. 6, pp. 6387–6398, 2021.

Hindawi
Security and Communication Networks
Volume 2024, Article ID 9858901, 1 page
https://doi.org/10.1155/2024/9858901

Retraction

Retracted: Digital Reconstruction Method of Power Metering Production Data Based on Digital Twin Technology

Security and Communication Networks

Received 8 January 2024; Accepted 8 January 2024; Published 9 January 2024

This article has been retracted by Hindawi following an investigation undertaken by the publisher [1]. This investigation has uncovered evidence of one or more of the following indicators of systematic manipulation of the publication process:

(1) Discrepancies in scope

(2) Discrepancies in the description of the research reported

(3) Discrepancies between the availability of data and the research described

(4) Inappropriate citations

(5) Incoherent, meaningless and/or irrelevant content included in the article

(6) Manipulated or compromised peer review

The presence of these indicators undermines our confidence in the integrity of the article's content and we cannot, therefore, vouch for its reliability. Please note that this notice is intended solely to alert readers that the content of this article is unreliable. We have not investigated whether authors were aware of or involved in the systematic manipulation of the publication process.

Wiley and Hindawi regrets that the usual quality checks did not identify these issues before publication and have since put additional measures in place to safeguard research integrity.

We wish to credit our own Research Integrity and Research Publishing teams and anonymous and named external researchers and research integrity experts for contributing to this investigation.

The corresponding author, as the representative of all authors, has been given the opportunity to register their agreement or disagreement to this retraction. We have kept a record of any response received.

References

[1] H. Wang, H. Shen, C. Li et al., "Digital Reconstruction Method of Power Metering Production Data Based on Digital Twin Technology," *Security and Communication Networks*, vol. 2022, Article ID 6835371, 10 pages, 2022.

Hindawi
Security and Communication Networks
Volume 2022, Article ID 6835371, 10 pages
https://doi.org/10.1155/2022/6835371

Research Article

Digital Reconstruction Method of Power Metering Production Data Based on Digital Twin Technology

Hao Wang,[1] **Hongtao Shen**,[1] **Chong Li**,[1] **Bing Li**,[1] **Yi Wang**,[1] **Ruiming Wang**,[1] **and Zhaosheng Yang**[2]

[1]*State Grid Hebei Marketing Service Center, Shijiazhuang 050035, China*
[2]*Department of Information Engineering, Shijiazhuang University of Applied Technology, Shijiazhuang 050081, China*

Correspondence should be addressed to Hao Wang; 18731929706@163.com

Received 3 March 2022; Revised 24 March 2022; Accepted 12 April 2022; Published 26 May 2022

Academic Editor: Fang Liu

With the continuous improvement of the integration and intelligence of ubiquitous power Internet of things system equipment, its cost in life cycle management such as data service, operation monitoring, and safety protection is becoming higher and higher. At the same time, the probability of power grid failure, reduced operation efficiency, and function failure will gradually increase with the development of its scale. Accurately evaluating the metering performance of distribution network digital metering system in the operation of power system and improving its accuracy, stability, and reliability are the key issues for its future use in power trade settlement. In this paper, a digital reconstruction method of power metering production data based on digital twin is proposed. The operation data of power system is collected in real time through the data acquisition module, the operation data is analysed, identified, and predicted, and then the analysis, identification, and prediction results are used to realize the visualization and digitization of operation data. Further, the operation data of the digital metering system are monitored and analysed to verify the effectiveness of the method. The advantages and disadvantages of the design scheme of the digital metering system are obtained by analysing the active power error, which provides the basis of practice and selection for the application of the digital metering system.

1. Introduction

Digital twin refers to a kind of digital reproduction of physical entities, processes, and systems. The digital model obtains and analyses the real-time information of the physical model through multiple means and can present a variety of elements in the physical model and the real-time dynamic operation in the whole life cycle, so as to realize the functions of system monitoring, operation and maintenance, process and system optimization, event prediction, and simulation [1]. An intelligent operation data automatic acquisition and monitoring system is proposed in the smart grid monitoring system used in the substation. It uses several acquisition terminals to obtain the operation data of the power system and then realizes the monitoring function through the host computer and central server. However, due to many types of operation data, including data collected by sensors, video monitoring data, and equipment operation status, the presentation of operation data and fault feedback are not intuitive enough to directly reflect the actual operation status of the built facilities [2]. Because the operation information is displayed and saved separately, there is a lack of shut connection between the records and the proper model; such a statistics administration mode will lead to low protection effectivity [3]. In addition, in terms of data analysis, there is a problem of insufficient integration of information, and it is difficult for the internal relationship between data to be deeply excavated, which seriously affects the efficiency of operation and maintenance.

Theoretical analysis and simulation calculation are carried out for typical influencing factors, such as truncation error, rounding error, signal frequency offset, signal harmonic component, DC offset, random interference, and so on. The check technique of size error verification is

proposed, and some checks of digital watt hour meter are carried out with taking a look at tools to confirm the evaluation results. The influence on the measurement results and the treatment methods to reduce the measurement error are given [4]. By analysing the error factors of digital electric energy measurement, this paper puts forward some suggestions on reducing the error method, perfecting the function of electric energy meter, and putting forward constructive suggestions on the error verification method of digital electric energy measurement system [5].

The main organisational structure of this paper is as follows: Section 1 introduces the relevant background of power production measurement system and the current situation and problems of power measurement production data and explains the main problems discussed in this paper. Related work is discussed in Section 2. Section 3 analyses the power production system based on digital twin in detail. Section 4 analyses the method of digital reconstruction of raw tea according to data. Section 5 validates the operation data analysis method. Section 6 summarizes the full text.

2. Related Work

Digital twin refers to a kind of digital reproduction of physical entities, processes, and systems. The digital model obtains and analyses the real-time information of the physical model through multiple means and can present a variety of elements in the physical model and the real-time dynamic operation in the whole life cycle, to realize the functions of system monitoring, operation and maintenance, process and system optimization, event prediction, and simulation. In recent years, with the increasing acceleration of the intelligent process, to realize the interaction and integration of the physical world and the information world, the concept of digital twin came into being and continuously evolved and developed rapidly, which has played a great role in promoting many industries. However, drawing on its application in aerospace, automobile manufacturing, oil and gas pipeline, and other industries, the current application of digital twin in power industry has also made obvious progress. The main research on the application of digital twin is as follows.

In the process of the continuous improvement and development of the concept of digital twins, researchers have mainly carried out research on the modelling, physical information fusion, and service application of digital twins, focusing on the analysis of the relationship between digital twins and related industries, the establishment of virtual models, the analysis with the help of twin data fusion, service application criteria, and so on. The connotation of digital twin is to build a digital twin [6]. Its final manifestation is a complete and accurate digital description of physical entities, which can be used to simulate, monitor, diagnose, predict, and control physical entities [7]. With the in-depth improvement of synthetic brain software technology, in phrases of deepening the utility of twins, mixed with the parallel management theory, a digital quadruplet parallel evolution framework of parallel modelling, parallel prediction, and parallel execution of related structures has been formed, and energy power generation has been extended to the parallel system of social energy [8]. While researchers carried out in-depth research around digital twins, the concept of digital twins has gradually been accepted by American General Electric, German Siemens, and other enterprises and applied to technology development and production, forming digital twin development software tools such as Predix and scenter 3D, which has attracted extensive attention from academia, industry, and news media [9]. At the same time, many industries have carried out the application practice of digital twins. In BMW ding fen intelligent factory, manual monitoring is replaced by intelligent data analysis system based on digital twin. The US Air Force proposes to use the concept of digital twin to predict the structural life of aircraft; CNPC uses digital twins to promote the construction of smart pipe network; some literature also put forward the intelligent health management of power plant generator units based on the concept of digital twins [10].

Some scholars have studied the application of digital twin technology framework to power system online analysis. The implementation framework of digital twins in power system is designed, the key problems and core technologies faced in its construction are discussed, and the application status and prospect of digital twins in various fields of power system are clarified [11]. Others use digital twin technological know-how to construct the electricity tools enterprise net platform, centre of attention on the graph cloud, manufacturing cloud, check cloud, information cloud, and carrier cloud primarily based on the platform and talk about the software in the situations of strength gear design, manufacturing and operation, and protection administration [12]. Some scholars put forward the realization of perspective monitoring, fault prediction, and state optimization of generator unit operation and maintenance based on digital twin technology, which provides a new solution for the operation, maintenance, and management of power station units [13]. By organising a digital twin for simulation and early warning, firms can no longer solely minimize the nonfault shutdown time but additionally always decrease the work depth of employees. Intelligent power plants can also use digital twins to improve the intelligent level of power plants, to achieve the purpose of reducing personnel, increasing efficiency, energy conservation, and emission reduction. As a technology intensive and highly automated modern production enterprise, power plant has a good foundation in the application of digital twin [14]. From the connotation of digital twin and the architecture of DCS, the realization of local production process through DCs can also be regarded as a low-level digital twin.

3. Power Production System Based on Digital Twin

3.1. Overall Architecture of Digital Twin System. The modular production system based on digital twin is shown in Figure 1.

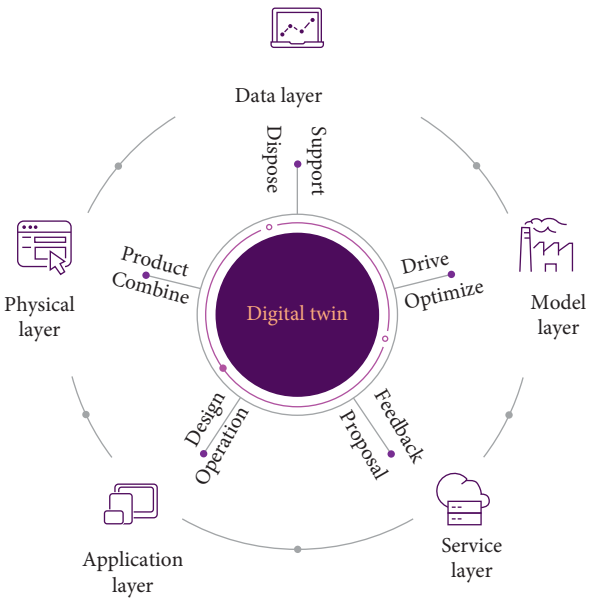


Figure 1: Model structure of digital twins.

(1) The physical layer includes modular production nodes and production units composed of modular production nodes. It is the carrier for the modular production system to perform production tasks. Modular production nodes can not only complete production tasks independently, but also form production units through combination to jointly execute production tasks [15]. The modular production node adopts standardized hardware design (circuit, network, and connection mechanism), which can quickly and cheaply combine into new production units according to production tasks, and the hardware equipment such as sensors, controllers, and effectors deployed in the modular node can enable it to have the ability of environment perception, computing decision-making, and manufacturing execution.

(2) The model layer is mainly responsible for modelling the modular production system in the information space and defining and describing the geometric attributes, physical rules, production operation logic, and operation knowledge of the digital twin workshop through the geometric model, physical model, behaviour model, and knowledge model, respectively; the intelligent negotiation mechanism is used to describe the system reconfiguration behaviour, such as negotiation and cooperation between modular production nodes, change of node type and number, and node reconfiguration [16]. The mannequin layer is the core of digital twin operation, the information layer, and the bodily layer, to map and describe the modular manufacturing device in the bodily house in the facts house, help the production managers understand the operation status of the production system, and support the functions of negotiation based dynamic reconstruction, simulation verification of reconstruction scheme, and model driven rapid reconstruction on the basis of real-time control function.

(3) The data layer is mainly used to store the basic configuration data and process data supporting the digital twin operation of modular production system. The data types include basic data, simulation data, and real-time data.

(4) The application layer mainly serves the design, operation, and simulation of modular production system. The reconfigurable application based on digital twin model includes model driven system design reconfiguration, operation scheme reconfiguration based on multiagent negotiation, and simulation verification of reconfiguration scheme. Model pushed machine diagram reconfiguration capacity that machine designers use the predefined mannequin factors in the mannequin layer to shortly diagram and reconstruct modular manufacturing nodes in the data area via visualization strategies; operation scheme reconfiguration based on multiagent negotiation refers to the generation of reconfiguration scheme through agent negotiation in the process of system operation to deal with external fluctuations of the system [17]. Simulation verification of reconfiguration scheme refers to verifying the effectiveness and rationality of reconfiguration scheme through the simulation results of model layer. The application layer aims to help system designers complete the tasks of design, verification, operation control, and reconstruction in the whole life cycle of modular production system through digital twin model, to improve the reconstruction efficiency [18].

3.2. Implementation Path and Foundation. Network flow digital twin is a systematic project integrating the technical achievements. Although its concept is still in the development stage, it has a certain technical foundation in related fields. Its core goal is to use the diversified modelling method based on mechanism and data to realize the panoramic image of the complex power metering and production system in the digital space and simulate the dynamic behaviour of the system in different scenarios through multiscale analysis and calculation, as well as support the flexible interaction with external elements. The technical framework is shown in Figure 2.

The modelling and simulation theory and method of physical energy system lay a foundation for the construction of digital twin core function of power metering and production system [19]. The existing research has carried out some research on the unified modelling and simulation method of electric, gas, and thermal multienergy flow under different time scales. For example, by transforming the partial differential equations of gas and thermal fluid into ordinary differential equations, the joint simulation of the dynamic characteristics of gas and thermal network can be

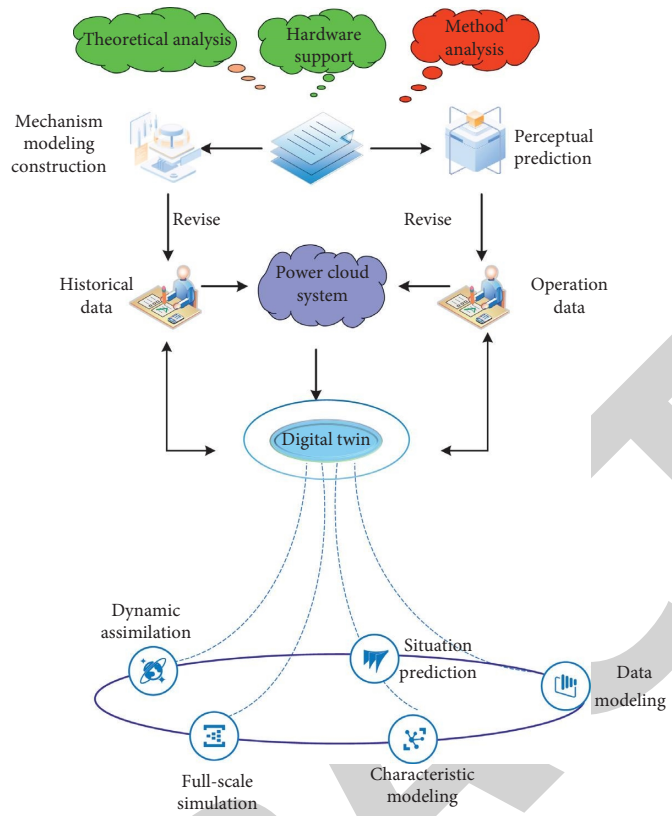


Figure 2: Composition of digital twin technology in power system.

realized. By mapping the gasoline and warmness community mannequin in time area to frequency domain, the unified modelling of fuel network, warmness community, and electricity grid can be realized [20]. From the perspective of circuit, the components in gas network and heat network can be compared as circuit components, so an analysis method of power metering production system which is unified with circuit analysis method is proposed. By transforming the complex characteristics of multienergy network in time domain into algebraic problems in complex frequency domain, a unified distributed parameter circuit and network model of electric, gas, and thermal systems can be established.

The fusion and utilization of multisource data are the key to construct the digital twin of power metering and production system. Firstly, considering the complexity of power metering and production system, it is difficult for a large number of links with unclear mechanism and opaque state to construct analytical mathematical models, which will rely more on data-driven methods to reveal their operation characteristics. Secondly, as a direct reflection of the state and characteristics of physical system, multisource operation data can be used to drive the continuous improvement of digital twin model and parameters and the synchronous evolution of virtual real system. For the related problems, on the one hand, the existing research starts with the steady-state characteristics and uses the data-driven method to realize the power flow calculation of electric and thermal networks [21]. On the other hand, focusing on the dynamic characteristics, the multitime scale characteristics of key energy conversion equipment such as micro gas turbine are modelled based on data-driven method. The existing research has carried out some work in the above aspects and realized typical applications such as intelligent urban building energy efficiency management and energy Internet monitoring based on information physics system.

4. Digital Twin Digital Reconstruction Method of Power Metering Production Data

4.1. Planning and Design of Power Energy System Based on Digital Twin. Electricity metering can be used for planning, operation, control, optimization, etc. of production systems. Figure 3 shows the operation optimization based on digital twin.

The modular idea of digital twin is not only reflected in the flexible configuration ability of power metering production system, but also reflected in the modular combination ability of its optimal planning mathematical problems. Especially with the establishment of more unified digital twin standards and specifications in the future and their wide application in the manufacturing industry, the digital twin of various energy production, conversion, consumption links, and devices may have been established in the factory stage and provided to users as an additional product function or service. This will greatly improve the planning and design efficiency of power metering production system as a modular combination of complex products.

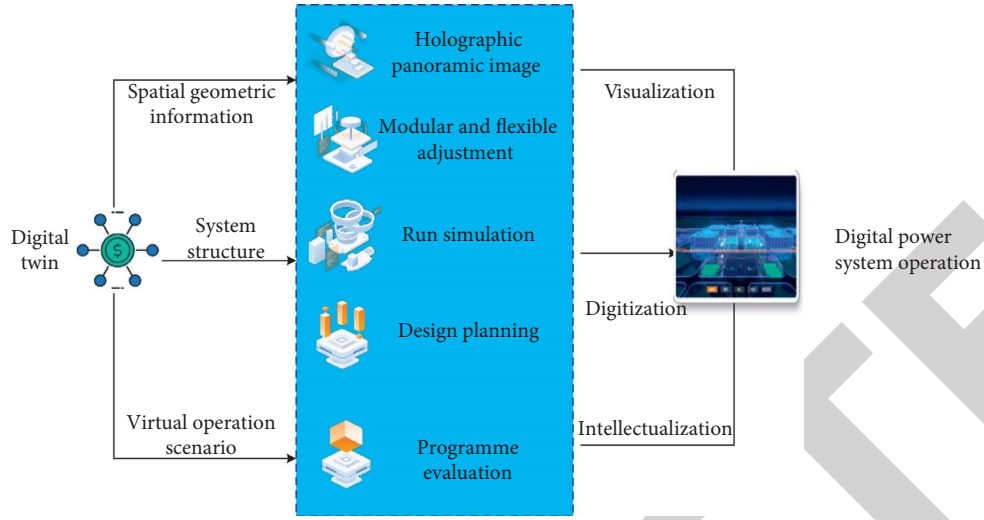


Figure 3: Power system design and operation optimization based on digital twin.

In addition, the holographic mirror image including the spatial structure characteristics of the energy system through digital twinning can support the integration of the planning and design scheme and the construction implementation scheme; that is, in the planning and design stage, the matching relationship between the planning scheme and the energy pipe corridor, architectural space, and urban layout is considered, so as to make the planning scheme realizable in the real environment and the coordination with the overall urban construction scheme can be an important constraint for planning and design. Further, combining digital twin technology with 3D printing architecture and other technologies to realize the rapid construction of infrastructure such as power metering production station and distribution room will greatly shorten the cycle from planning and design to construction and operation. Finally, digital twin provides a more realistic testing environment for the evaluation of planning schemes. The uncertainty of source and load in the operation of power metering and production system will significantly affect the actual performance of the planning scheme.

4.2. Digital Twin Fault Early Warning and Predictive Maintenance. The ability to diagnose the operation risk of power metering and production system is still insufficient; in particular the condition monitoring of urban underground power, gas, and heat pipelines is more difficult. Regular inspection is still the main way of energy system operation and maintenance, which means that it is difficult to find the best balance between system operation and maintenance cost and safety and reliability level, which may even lead to serious fault loss [22]. At the system level, the risk characteristic information of each key equipment can be integrated in the system level digital twin, and the system risk status can be described by using the fault characteristic data of the same type of equipment, historical operation and maintenance data, energy system measurement data, etc., so as to provide support for more complete status monitoring.

4.3. Coordinated Control and Optimization of Power Metering and Production Based on Digital Twin. At present, the operation optimization of power metering production system is mostly based on specific steady-state model. However, the production, transmission, conversion, and consumption characteristics of multiple types of energy in the actual system are difficult to describe by a simple model but are closely related to the system operation environment, working conditions, and other factors. The realization of fine operation scheduling considering the real state of different devices is of great significance to the operation practice of power metering production system. In this regard, the digital twin's panoramic mirror image and behaviour characterization ability of the real-time state of the real system are used.

The state data fed back to the digital space can be used to comprehensively judge the control effect and modify the control strategy, so as to realize the fine closed-loop control coordinated by various energy supply devices and improve the overall regulation level of the system. The relationship between electric energy and active power is as follows:

$$W = \frac{\sum_{j=1}^{N} u(j * \Delta t) i(j * \Delta t) \Delta t}{\int_{0}^{T} u(t) i(t) dt}. \quad (1)$$

When the instantaneous value of voltage and current sampled by the electronic transformer is transmitted to the digital electric energy meter through the merging unit, the electric energy meter receives it and hands it to the microprocessor for multiplication according to the definition, so as to obtain the average power.

$$P = \frac{\sum_{n=1}^{N} u(n) i(n)}{\sum_{n=1}^{N} P_n}. \quad (2)$$

The product of voltage instantaneous value and current instantaneous value is the average value in one cycle, and the integral expression of reactive power is the average value in

one cycle obtained by Hilbert transformation of voltage instantaneous value.

$$u(t) = \sum_{k=1}^{n} \sqrt{U_k \sin\left(k\omega t + \varphi_k\right)}, \tag{3}$$

where K and N are positive integers, and UK and IK are the effective values of the k-th harmonic of voltage and current, respectively.

$$v(t) = \frac{1}{\pi} \int_{-\infty}^{\infty} \frac{\left[\sqrt{U_k \sin\left(k\omega t + \varphi_k\right)}\right]}{t - x} \mathrm{d}x. \tag{4}$$

The truncation error in the calculation of active power is analysed by a similar method, and the effective value of voltage obtained by trapezoidal method is

$$U = \sqrt{\frac{1}{N} \sum_{k=0}^{N-1} u_k^2 + \frac{u_0^2 + u_N^2}{N}}. \tag{5}$$

4.4. Multidomain Collaboration of Digital Twins. In the future, the smart city will have a higher level of informatization and digitization, to form the concept of digital twin city. At this time, the digital twin of power metering and production system can play an important role in supporting urban development and efficient operation. Using the digital twin data fusion and utilization capability of the power metering and production system can form the energy big data foundation for urban development and support various advanced data analysis applications. For example, the energy consumption data of electric power, hydraulic power, heat, and gas gathered by digital twins, combined with urban population, meteorology, geography, and other information, can be used to study and judge the trend of urban economic development and provide richer and accurate decision-making basis for urban planning and construction. The user side model and data provided by digital twin can describe users' living and consumption habits and help form new urban management and commercial operation modes. Energy security is an important part of urban security; the digital twin panoramic perception ability of power metering and production system can be used to find the system operation risk, judge the fault location, and improve the security and reliability of energy supply.

5. Validation of Operation Data Analysis Method

5.1. Multidomain Collaboration of Digital Twins. The metering performance of electronic transformer and digital metering system put into operation in digital metering pilot is analysed. See Figure 4 for the original collected data randomly selected.

The abnormal value range obtained after calculation of the original collected data is shown in Figure 5. The ratio difference and angle difference of 12 randomly selected operation data meet the requirements of error limit and can be used for subsequent data analysis.

5.2. Operation Data Measurement Performance Analysis. Randomly select 12 groups of operation data of a digital output electronic current transformer located in phase B in the pilot from August 2019 to July 2020, apply the operation data analysis method proposed in Section 2 to carry out the measurement performance analysis of distribution network electronic current transformer, and use the quadratic curve to analyse the influence of single factor on error. Through the quadratic curve, the influence of temperature and load changes on the error is analysed, as shown in Figure 6.

The error of digital output electronic current transformer is less affected by temperature change, the variation range of specific difference is 0.05%, and the variation range of angular difference is 3 degrees. It is greatly affected by the load change, with the variation range of specific difference of 0.12% and the variation range of angular difference of 5 degrees. However, when the load current exceeds 10a and about 2% of the rated current, the impact is significantly smaller. The influence of compound factors on error is analysed by three-dimensional surface. Through the three-dimensional surface, the influence of the change of temperature/humidity and temperature/load on the error is analysed, as shown in Figure 7.

Measurement error surface of digital output electronic current transformer is not smooth at low load, and the error fluctuation is large. With the increase of load, the error surface is gradually smooth, the error fluctuation is gradually reduced, and the operation of the transformer is more stable. The extreme point of the error of electronic current transformer often appears in the extreme point of the environment, that is, high temperature and high humidity, low temperature and low humidity, high temperature and low humidity, and low temperature and high humidity. From the analysis results of two-dimensional curve and three-dimensional surface, the calculated information gain of each influencing factor can accurately reflect its influence on the error.

5.3. Performance Analysis of Digital Electric Energy Metering System. This section analyses the metering characteristics of the digital metering system composed of analogy output electronic transformer and the digital metering system composed of digital output electronic transformer through the error data of the total active power of the two typical design schemes of distribution network digital metering system in the pilot within one year. The stability, advantages, and disadvantages in long-term operation are shown in Figure 8.

The maximum monthly active energy error of the digital output metering system is −0.48%, and the variation of monthly energy error within one year is 0.24%. For one year's operation, the overall metering performance is stable and can be preferentially applied to power trade settlement. Due to the ECT failure of phase α in the analogy output metering system, the maximum monthly active energy error is −6.0%. For phases α and γ in normal operation, the maximum monthly active energy error is −0.99% and −1.17%, respectively, but the variation of electric energy error within one year is only 0.28% and 0.41%. The analogy output metering system has high

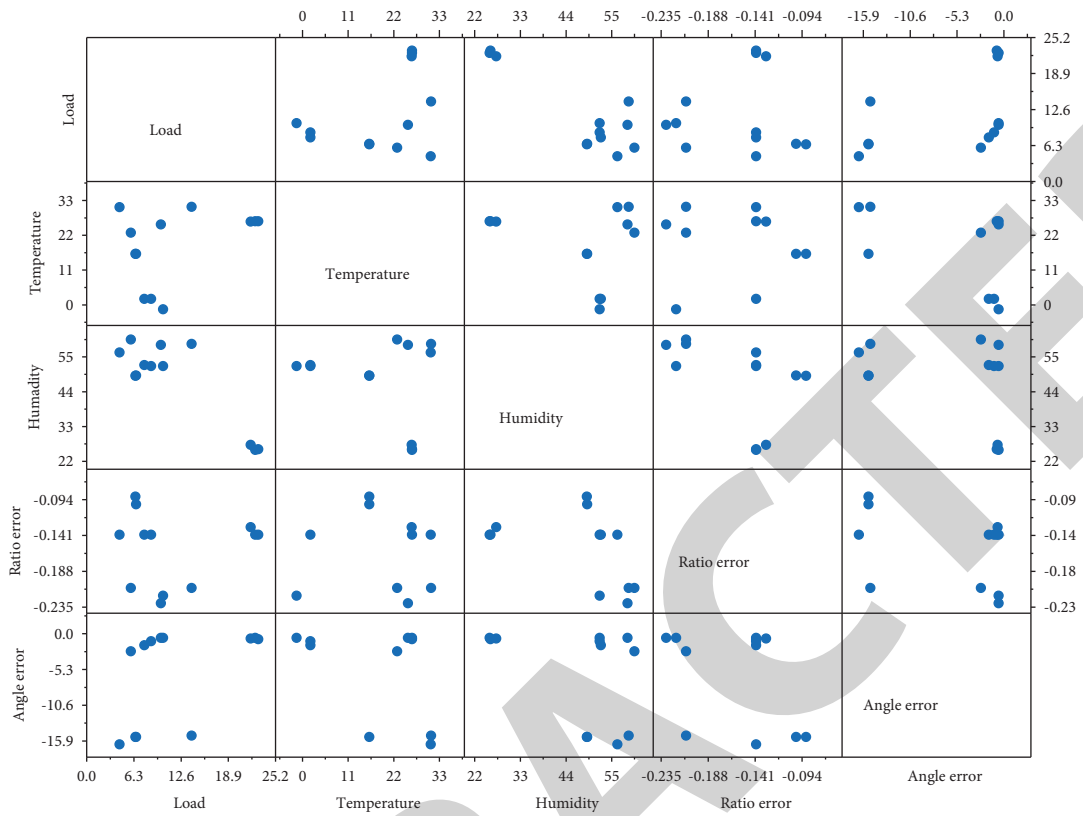


Figure 4: Raw data distribution of random sampling.

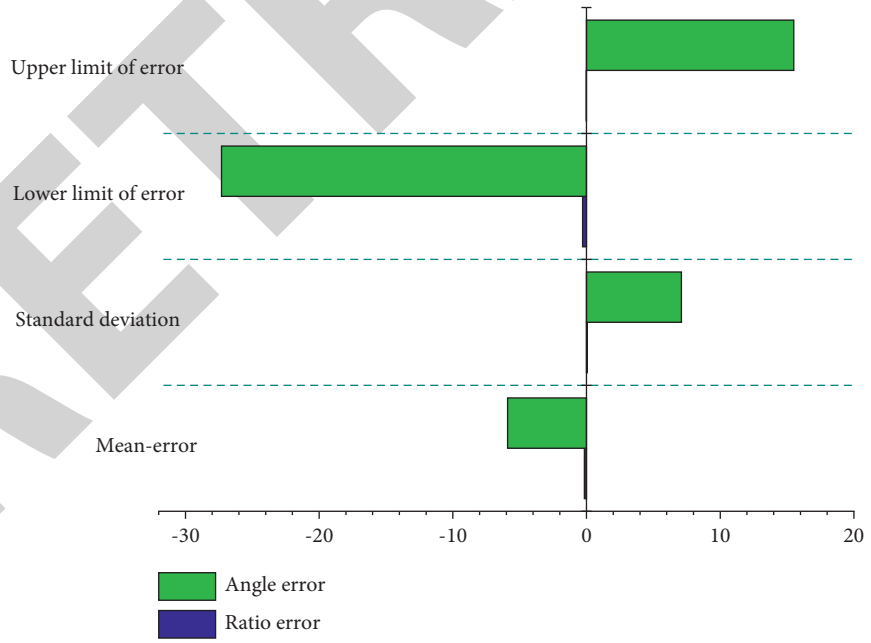


Figure 5: Calculation of outliers.

failure risk, and the metering equipment in normal operation also has large system error; before putting into operation, the system error can be eliminated through parameter configuration and then used for electric energy metering.

5.4. Power Parameter Monitoring Based on Digital Twin. The standard system is adopted, and the default admittance parameters are simulated with Manpower. In IEEE-9 system, node 1 is a balanced node, nodes 2 and 3 are PV nodes, and nodes 4, 5, and 6 are PQ nodes with load. It is

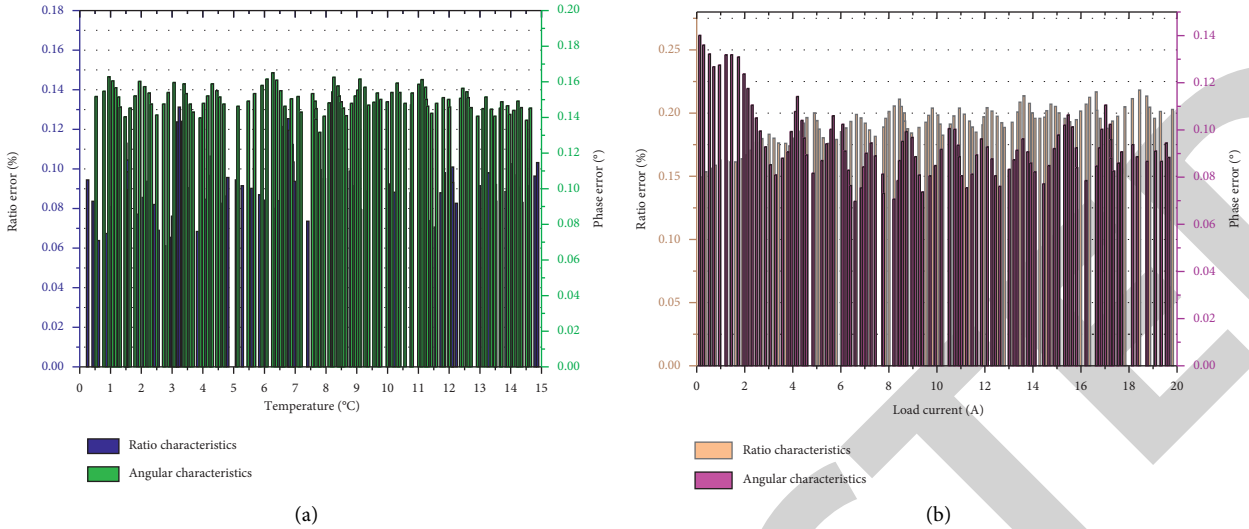


Figure 6: Error characteristics of digital output. (a) Temperature characteristic. (b) Load characteristic.

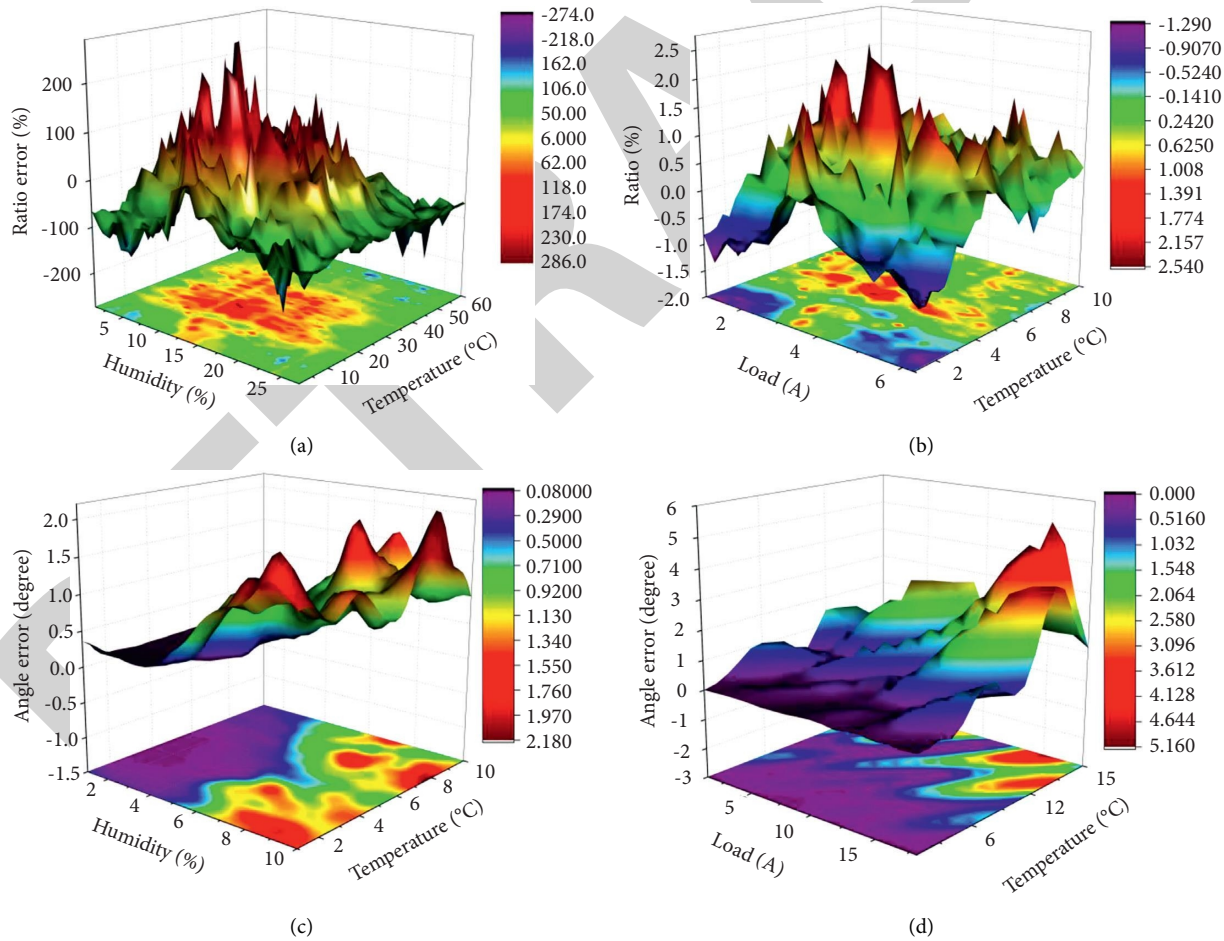


Figure 7: Analysis of digital output error characteristics. (a) Ratio of temperature/humidity. (b) Ratio of temperature/load. (c) Angle error of temperature/humidity. (d) Angle error of temperature/load.

assumed that the normalized load fluctuation of 3, 4, and 5 in a certain day is shown in Figure 9(a), and its measurement frequency is 9600 points per day. At the same time, small fluctuations are introduced into the measured data of each node to simulate load fluctuations and measurement errors. It is substituted into the traditional

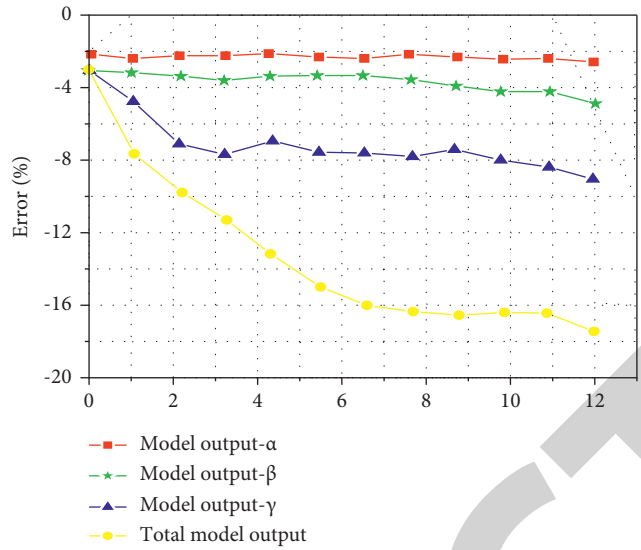


Figure 8: Error analysis of power data in digital metering system.

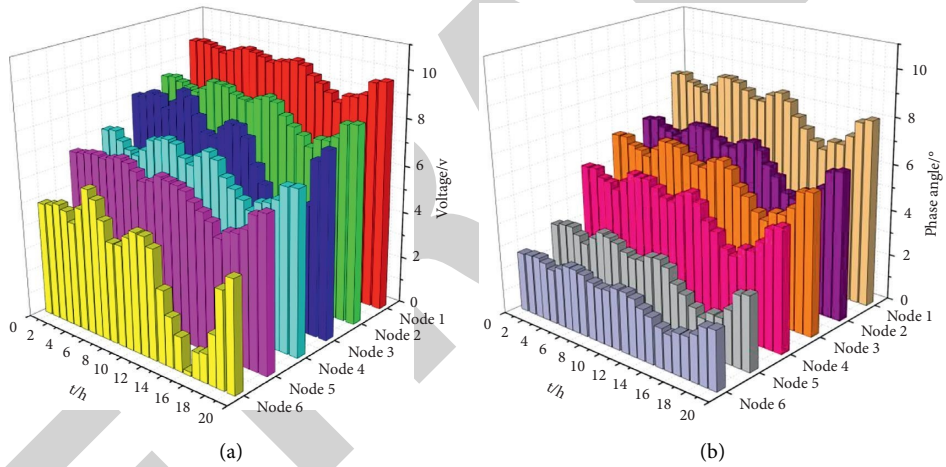


Figure 9: Power flow calculation results of power production metering data. (a) Voltage amplitude. (b) Voltage phase angle.

power flow program to obtain the system state quantity, as shown in Figure 9(b). Train ANN network to simulate load active power value P and voltage amplitude u and voltage phase angle, add small artificial fluctuations to the parameters, and normalize them.

Similarly, the normalized voltage amplitude and phase angle can be obtained, and a 5-layer ANN network can be established to select the activation function. Time 1–8400 is used as the training set and time 8401–9600 is used as the test set. The predicted values of the three active load nodes in the system are very close to the actual values, which indicates that DT successfully represents the actual physical system. Different from the traditional way, the establishment of DT system does not depend on the information of topology but is realized through two links: training and testing based on artificial neural network, that is, training the historical data set to establish the neural network and using the network to test the sampled data set to obtain the results.

6. Conclusion

Digital twin can be used as an important means of integration and utilization of sea volume data and extensive connection in digital city, which will make it possible for the interconnection and cooperative operation of energy system and various fields of the city in digital space. Digital twin mannequin is developed and displayed primarily based on the analysis, identification, and prediction effects of energy machine operation facts via the digital twin mannequin building module, which realizes the visualization function of power system operation data. Operators can intuitively obtain the actual operation status and fault feedback of the current power system through the displayed three-dimensional digital model, improve the operation and preservation efficiency of the power system of the substation; use the digital twin for scientific construction, which can intuitively show the operation efficiency of the system.

Hindawi
Security and Communication Networks
Volume 2024, Article ID 9893281, 1 page
https://doi.org/10.1155/2024/9893281

Retraction

Retracted: Analysis of Dynamic Influence Mechanism of Network Public Opinion Based on Simulation Feature Extraction

Security and Communication Networks

Received 8 January 2024; Accepted 8 January 2024; Published 9 January 2024

This article has been retracted by Hindawi following an investigation undertaken by the publisher [1]. This investigation has uncovered evidence of one or more of the following indicators of systematic manipulation of the publication process:

(1) Discrepancies in scope

(2) Discrepancies in the description of the research reported

(3) Discrepancies between the availability of data and the research described

(4) Inappropriate citations

(5) Incoherent, meaningless and/or irrelevant content included in the article

(6) Manipulated or compromised peer review

The presence of these indicators undermines our confidence in the integrity of the article's content and we cannot, therefore, vouch for its reliability. Please note that this notice is intended solely to alert readers that the content of this article is unreliable. We have not investigated whether authors were aware of or involved in the systematic manipulation of the publication process.

In addition, our investigation has also shown that one or more of the following human-subject reporting requirements has not been met in this article: ethical approval by an Institutional Review Board (IRB) committee or equivalent, patient/participant consent to participate, and/or agreement to publish patient/participant details (where relevant).

Wiley and Hindawi regrets that the usual quality checks did not identify these issues before publication and have since put additional measures in place to safeguard research integrity.

We wish to credit our own Research Integrity and Research Publishing teams and anonymous and named external researchers and research integrity experts for contributing to this investigation.

The corresponding author, as the representative of all authors, has been given the opportunity to register their agreement or disagreement to this retraction. We have kept a record of any response received.

References

[1] Y. Zhang, "Analysis of Dynamic Influence Mechanism of Network Public Opinion Based on Simulation Feature Extraction," *Security and Communication Networks*, vol. 2022, Article ID 8423643, 12 pages, 2022.

Hindawi
Security and Communication Networks
Volume 2022, Article ID 8423643, 12 pages
https://doi.org/10.1155/2022/8423643

Research Article

Analysis of Dynamic Influence Mechanism of Network Public Opinion Based on Simulation Feature Extraction

Yang Zhang

University of Shanghai for Science and Technology, Business School, Shanghai 200093, China

Correspondence should be addressed to Yang Zhang; 171910094@st.usst.edu.cn

Received 17 March 2022; Revised 29 April 2022; Accepted 9 May 2022; Published 24 May 2022

Academic Editor: Zhiping Cai

In order to improve the effect of network public opinion management, this paper constructs an intelligent computer network simulation model to analyze the dynamic influence mechanism of network public opinion. This paper converts semistructured text information into a form that is easy for computer analysis and recognition, which facilitates opinion extraction and sentiment analysis. Moreover, by analyzing the text content to be mined, this paper uses a specific algorithm to select different words that best represent the text to be tested as the characteristic words of network public opinion. These network public opinion feature words can classify texts, thereby reducing the complexity of text classification. The experimental study shows that the dynamic influence mechanism analysis model of network public opinion based on intelligent computer network simulation constructed in this paper has a good effect.

1. Introduction

Different from single text and pictures, short videos integrate various forms of expression, such as text, pictures, and videos, and are mainly divided into the following categories. One is pure picture stitching, which combines multiple pictures into a form similar to an electronic album. The second is to add subtitles to pictures, which are based on the combination of multiple pictures and add text descriptions. The third is video one-shot or mixed-cut, which simply processes the captured video and uploads it directly, or stitches multiple video clips together. The fourth is the form of video plus text, which is supplemented by text description on the basis of video. The fifth is pure text, which transforms the text in various forms to form a video. Metaphorization mainly refers to the dissemination of public opinion in an indirect and concealed way. Moreover, various forms of communication have prompted netizens to express and disseminate public opinion in various ways such as text, video, pictures, and actions. The process of metaphorization of social public opinion is consistent with the process of development and evolution of social public opinion. It is also under the stimulation of emergencies, the public responds to it, chooses metaphorical methods to express public opinion, and finally, public opinion superimposes and spreads. In the process of metaphorical dissemination of social public opinion, there is a phenomenon of mutual transformation between explicit and implicit public opinion, which brings a test to the guidance of social public opinion. Due to the limited duration of short videos, they are fragmented. First, because the content narrative is incomplete, a complete video may be divided into multiple short video segments for dissemination. The second is the fragmentation of the push sequence. The algorithmic recommendation mechanism of short videos makes the content presented to the audience more of their favorite content rather than the latest content in chronological order. Fragmentation of content narrative may lead to public opinion in the first half of the video, and when the public opinion enters a quiet period, it will stir up again due to the release of the second half of the video. At the same time, the fragmentation of the push sequence may lead to the fact that when the public opinion returns to a quiet period, the video that caused the public opinion is pushed to the public who do not know the truth, causing a public opinion crisis again, which constitutes the characteristic of the repeated crisis of social public opinion communication.

The traditional text public opinion cycle shows a development process from latent to outbreak, and finally to a quiet period. If there is a subsequent release of text content that will trigger public opinion, it will enter the latent period again, forming a closed-loop process. The intervention of short videos has made public opinion show a step-by-step rise and the characteristics of a reciprocating crisis. There must be contradictions behind the crisis of public opinion. There are many subjects involved in the society, the social ecology is complex, and the social system concentrates various contradictions. These contradictions can become the signs of the outbreak of public opinion.

Based on the above analysis, this paper constructs an intelligent computer network simulation model to analyze the dynamic impact mechanism of network public opinion and provides a reference for the subsequent management and control of network public opinion.

2. Related Work

The literature [1] found that news reports can set agendas for audiences, and this agenda setting is achieved through the number of reports, titles, layouts, etc., from which the influence of mass media on public opinion is obtained. The literature [2] uses the methods of social network and statistical analysis to analyze the influence of public political attention on election results and public opinion surveys. The literature [3] mainly starts from the perspective of public sentiment, by correlating the emotional information released by netizens on the network platform and related news content, and using the method of public opinion link tracking to monitor netizens' sentiments towards political actors.

The literature [4] uses the Delphi method to design the weight of the early warning indicator system, conducts in-depth research on the development, changes, and process of network public opinion, analyzes its propagation law, and accurately predicts the development trend of network public opinion. The literature [5] expounds the research on the three subsystems of the network public opinion early warning mechanism, including the database research and judgment analysis system, the public opinion information processing and mining system, and the early warning joint control and disposal system, early warning mechanism. The literature [6] improves and optimizes the traditional topic tracking model on the basis of Rocchio algorithm. The literature [7] proposes a topic detection algorithm, which is based on K-means clustering, a detection method.

On the basis of the four-dimensional indicators studied in the literature [8], dimensional indicators including audio, video, and images are introduced, thereby establishing a network public opinion security evaluation system with five dimensions. Through this evaluation system, network public opinion can be studied. More comprehensively monitor the development trend of network public opinion; based on the research method of intuitionistic fuzzy reasoning, the literature [9] determines the weight of the evaluation index elements, so as to implement monitoring, early warning and evaluation of network public opinion. The literature [10] systematically detects leaders in the dissemination of network public opinion, mainly using frequent pattern mining algorithm for monitoring. The literature [11] builds a network public opinion monitoring and early warning model and further improves network public opinion by proposing a single-granularity opinion mining algorithm early warning model.

Based on the analysis of the characteristics of network public opinion, such as fast dissemination speed, wide dissemination range, and large dissemination base, the literature [12] proposes a strategy to deal with network public opinion and a path selection method to guide it. The literature [13] puts forward relevant methods to deal with the outbreak of network public opinion and measures to guide the development of public opinion in a benign direction through in-depth analysis of various aspects of network public opinion.

The literature [14] established a system dynamics model for the dissemination process of network public opinion based on the SIR model. Through experimental simulation to find its propagation law, to find out the factors that affect the trend of public opinion propagation and to maintain a balance that is conducive to the stability of the system. The literature [15] mainly conducts in-depth and comprehensive research on the popularity of network public opinion and establishes a model that can predict the development trend of network public opinion. It mainly conducts in-depth research on the comprehensive application of events, media, netizens, and government and proposes solutions and coping strategies when the network public opinion crisis occurs through the simulation results of the model. The literature [16] considered the characteristics of network public opinion dissemination, combined AHP with system dynamics, and established a model with network public opinion early warning mechanism that can be analyzed from both the government and the media. The model is simulated, and through the simulation results, a reasonable early warning mechanism for network public opinion is proposed.

The term "social network" was first proposed by Brown and gradually formed the current social network analysis method that can be applied to many fields such as psychology, sociology, and statistics. The literature [17] proposed a classic rumor propagation SIR model when studying the law of rumor spreading. In the model, two parameters that affect rumor spreading, diffusion rate and removal rate, are set as constants. After simulating the model, it is concluded that the whole process of rumors from spreading to disappearing will not be known to everyone. The literature [18] uses the social network analysis method to analyze the density, diameter, clustering coefficient, etc. The relevant parameters are divided into trees.

The literature [19] proposed a traversal algorithm that can move the cell, also considered the firmness of the cell, and designed the calculation formula of the majority rule. Four parameters are defined in this formula, namely, tendency strength, tendency aggregation degree, cell peak value, and cell tendency value, and the influence of the

changes of their set values on the process of public opinion dissemination is discussed separately. The literature [19] introduced the algorithm of fuzzy reasoning in the cellular automata model to fuzzify some information in the process of network public opinion. At the same time, in the established network public opinion propagation model based on fuzzy cellular automata, two parameters are set: environmental fitness and preference, and their impact on public opinion dissemination is analyzed through simulation results.

3. Intelligent Network Public Opinion Dynamic Text Analysis

The network public opinion feature words are generally divided into two categories, one is the general network public opinion feature term, and the other is the exclusive network public opinion feature term. The so-called general network public opinion feature terms refer to words that appear frequently in a specific document. The extraction of these terms is based on a weight function, and the network public opinion feature weight calculated by the function is used to measure the frequency of the term. The larger the value, the higher the occurrence frequency, and the stronger the representativeness of the network public opinion feature word in the text. Proprietary network public opinion feature terms are different from general network public opinion feature terms. Proprietary network public opinion feature terms are words with specific and special meanings, such as proper nouns, time nouns, person names, place names, and numbers. Proprietary network public opinion feature items must be extracted according to the specific network public opinion feature words themselves.

Information gain refers to calculating the frequency of a specific network public opinion feature word appearing or not appearing in the text, so as to measure the probability that a document is classified into a certain category. The main idea of the algorithm is that specific network public opinion feature words can provide a certain basis for the classification of texts. For example, for a specific network public opinion feature word, its existence can provide a certain amount of information for document classification. The dispersion value formed in the process of changing the amount of information represents the gain information provided by the network public opinion feature word for a certain type of text.

The information gain is expressed by the following equation.

In the process of information gain, the value of x is $x_1, x_2, \ldots, x_n, p_1, p_2, \ldots, p_n$ represents the classification probability, and the entropy of x is defined:

$$H(x) = -\sum_{i=1}^{n} p_i * \log_2 p_i. \tag{1}$$

For the appeal equation, the more feasible values of x, the more informative it is to prove it.

C is the text category set, c is the text category variable. Then, the information gain formula is

$$\begin{aligned} IG(t_k) &= H(C) - H(C \mid t_k) \\ &= -\sum_{c \in C} p(c)\log(p(c)) + p(t_k)\sum_{c \in C} p(c \mid t_k)\log(p(c \mid t_k)) \\ &\quad + p(\overline{t_k})\sum_{c \in C} p(c \mid \overline{t_k})\log(p(c \mid \overline{t_k})) \\ &= \sum_{c \in C}\left(P(c, t_k)\log\left(\frac{P(c, t_k)}{P(c)P(t_k)}\right)\right. \\ &\quad \left. + P(c, \overline{t_k})\log\left(\frac{P(c, \overline{t}_k)}{P(c)P(\overline{t_k})}\right)\right), \end{aligned} \tag{2}$$

where $H(C)$ represents the entropy value change function in the whole process of information gain, and $H(C \mid t_k)$ represents the conditional entropy of the system under the condition that the network public opinion feature t_k occurs. The larger the entropy value is, the better the network public opinion feature words can represent the text.

Mutual information of two random events x and y is specified:

$$MI(x, y) = H(x) + H(y) - H(x, y), \tag{3}$$

where $H(x, y)$ is the joint entropy value, and the H function is defined as follows:

$$H(x, y) = -\sum p(x, y)\log p(x, y). \tag{4}$$

It is generally believed that if the frequency of a certain network public opinion feature word in a certain category of documents is much higher than that in other categories of texts, it is considered that the network public opinion feature word has a greater amount of mutual information for this type of document. Therefore, mutual information is a measure of the relationship between characteristic words of network public opinion and classified documents. The more the network public opinion feature word can express a text, the greater the calculation value of its mutual information.

The mutual information of network public opinion feature word t_k and document category c is defined as follows:

$$\begin{aligned} M(c, t_k) &= \log\left(\frac{p(c, t_k)}{p(c)p(t_k)}\right) \\ &= \log\frac{p(t_k \mid c)}{p(t_k)} \approx \log\frac{A \times N}{(A + C)(A + B)}, \end{aligned} \tag{5}$$

where N refers to the number of documents to be classified, A is the number of network public opinion features t_k included in class c documents, B is the number of documents that contain t_k but do not belong to class c, and C is the number of documents belonging to c but not including t_k.

The chi-square test is a widely used statistical test algorithm. In text classification, the chi-square test is used to measure the association between documents. The chi-square statistical test is a measure of the dispersion between the

theoretical value and the sample to be tested. It is used to analyze the degree of association between two network public opinion feature words. Moreover, the characteristic of the chi-square test is that it counts the presence or absence of the characteristic words of network public opinion. Therefore, in some respects, the chi-square test is more accurate than the mutual information calculation.

The formula for calculating χ^2 of the network public opinion feature word t_k, t_k is as follows:

$$\chi^2(c, t_k) = \frac{p(c, t_k)p(\overline{c}, \overline{t_k}) - p(c, t_k)p(\overline{c}, t_k)}{p(c)p(t_k)p(\overline{c})p(t_k)}. \quad (6)$$

Fitting the feature word t_k of network public opinion, the following function is obtained:

$$\chi^2_{\text{avg}}(t_k) = \sum_{c \in C} p(c)\chi^2(c, t_k). \quad (7)$$

The larger the chi-square statistic value, the higher the correlation degree between the network public opinion feature t_k and the document category c.

In text representation, the selection of text network public opinion features is also crucial. As a text network public opinion feature that refers to a text, its granularity can be word, phrase, sentence, or paragraph. The selection of text network public opinion features with different granularities will also achieve different text representation effects. Generally speaking, the language granularity of words is selected as the basic unit of the characteristics of text network public opinion.

There are many methods of text representation, and the most commonly used method with ideal effect is the Vector Space Model. The model vectorizes the document and replaces the text with a vector d, which is represented by the formula

$$d_i = (w_{i1}, w_{i2}, \ldots, w_{\text{in}}), \quad (8)$$

where t_k represents the feature of the text network public opinion and w_{ik} represents the weight of the k-th network public opinion feature item entry t_k of the text d_i, that is, the proportion of the network public opinion feature word in the text d_i. The larger the value of w_{ik}, the greater the importance of the network public opinion feature in the text d_i, and the high proportion value also indicates that the network public opinion feature item is more representative of the text d_i.

This paper is also dynamically analyzing the online review information, among which, an essential step is text representation, which converts semistructured text information into a form that can be recognized and processed by computers. In order to analyze the comment text dynamically, this paper uses the content network public opinion feature information of the text and the external network public opinion feature information to represent the text.

Naive Bayes is a calculation method based on the theory of statistical probability. The Naive Bayes algorithm assumes that the distribution of network public opinion feature words in document D_i is irrelevant. The basic idea is to calculate the probability that an unknown document belongs to a certain category through the prior probability of the category and the conditional probability of the network public opinion feature distribution relative to the category.

$TF(W_k)$ is the frequency of network public opinion feature word W_k appearing in a certain document. $P(C_j)$ is the probability of belonging to a class:

$$\frac{P(C_i)P(D_j \mid C_i)}{P(D_j)} = \frac{P(C_i)\prod_{k=1}^{D_j} P(W_k \mid C_i)TF(W_k)}{P(D_j)}. \quad (9)$$

Among them, C_i represents a specific category i, D_i represents the text of the category to be tested, and W_k is the characteristic word of network public opinion that appears in D_j. $P(C_i)$ and $P(W_k \mid C_i)$ can be obtained in advance by training.

The algorithm process of Naive Bayes classification $W = (W_1, W_2, W_3, \ldots, W_k)$ represents the probability of occurrence of network public opinion feature words:

$$W_k = P(W_k \mid C_j) = \frac{1 + \sum_{i=1}^{|D|} N(W_k, d_i)}{|V| + \sum_{s=1} \sum_{i=1}^{|D|} N(W_s, d_i)}, \quad (10)$$

where N is the frequency of network public opinion feature words appearing in a document and n is the number of network public opinion feature words.

$P(C_r \mid \theta)$ represents the similarity value between documents. If the documents continue to increase, according to the segmentation results of the characteristic words of network public opinion, the probability that the document d_i to be tested belongs to class C_j can be expressed as

$$P(C_j \mid d_i; \quad \theta) = \frac{P(C_j \mid \theta)\prod_{k=1}^{n} P(W_k \mid C_j; \theta)^{N(W_k, d_j)}}{\sum_{r=1}^{|C|} P(C \mid \theta)\prod_{k=1}^{n} P(W_k \mid C_r; \theta)^{N(W_k, d_j)}}. \quad (11)$$

In the above formula, $|C|$ represents the number of categories, and $P(C_j \mid \theta)$ is the ratio of the number of training document C_j to the total number of documents. The probability value of the newly added document belonging to each category is calculated, and then, the text to be tested is classified into the category with the highest calculated probability.

The support vector machine first constructs the decision function and then substitutes the quantized test samples into the decision function to calculate the category. N is the number of sample sets, the training sample set is $\{(x_i, y_i), i = 1, 2, \ldots, N\}$, and x_i and y_i, respectively, represent two types of sample labels.

In the linear condition, $W^*X + b = 0$ is used to represent the decision function, that is, the optimal classification surface or hyperplane. W, b is the two parameters of the hyperplane, which determine the way of classification, and W^*X represents the inner product of the sample vector and X. If $X \in RN$ belongs to the first category, the variable flag is defined as positive $(y_i = 1)$; otherwise, the variable flag is defined as negative $(y_i = -1)$.

The discriminant equation is adopted: $g(x) = w^T x + b$. On this basis, it is normalized so that the hyperplane function can correctly classify the test data and satisfy:

$$y_i\left(w^T x_i + b\right) - 1 \geq 0, \quad i = 1, 2, \ldots, n. \tag{12}$$

It can be used under the above conditions to solve the minimum problem of the following equations instead of solving the optimal classification surface problem:

$$\phi(w) = \frac{1}{2}\|w\|^2 = \frac{1}{2}\left(w^T w\right). \tag{13}$$

The Lagrange function is defined as follows:

$$L(w, b, \lambda) = \frac{1}{2} w^T w - \sum_{i=1}^{n} \lambda_i \left[y_i\left(w^T x_i + b\right) - 1 \right]. \tag{14}$$

Among them, $\square_i \square 0$ is the Lagrange coefficient. Differentiating the equations with respect to $w, b, \square_i$ and making them equal to 0, we get

$$\begin{aligned} &\frac{\partial L}{\partial w} = 0 \Rightarrow w = \sum_{i=1}^{n} \lambda_i y_i x_i, \\ &\frac{\partial L}{\partial b} = 0 \Rightarrow \sum_{i=1}^{n} \lambda_i y_i = 0, \\ &\frac{\partial L}{\partial \lambda_i} = 0 \Rightarrow \lambda_i \left[y_i\left(w^T x_i + b\right) - 1 \right] = 0. \end{aligned} \tag{15}$$

Under the above three formulas and constraints, the problem is transformed into the following dual problem, and at the same time, a quadratic function mechanism problem under inequality constraints is formed:

$$L_D = \sum_{i=1}^{n} \lambda_i - \frac{1}{2} \sum_{i=1}^{n} \sum_{j=1}^{n} \lambda_i \lambda_j y_i y_j \left(x_i^T x_j\right). \tag{16}$$

If λ_i^* is the optimal solution of the equation, then

$$w^* = \sum_{i=1}^{n} \lambda_i^* y_i x_i. \tag{17}$$

Among them, the sample of $C_i \neq 0$ is the support vector. By linearly fitting the coefficient vector and support vector of the optimal classification hyperplane, b^* can be solved by the constraints $\lambda_i [y_i (w^T x_i + b) - 1] = 0$, and the optimal classification function can be expressed as

$$f(x) = \operatorname{sgn}\left(\left(w^*\right)^T x + b^* \right) = \operatorname{sgn}\left(\sum_{i=1}^{n} \lambda_i^* y_i x_i^* x + b^* \right). \tag{18}$$

In the solution of nonlinear problems, only one hyperplane cannot completely distinguish the categories, so the loose variables can be used to assist.

The specific steps of the agglomerative hierarchical clustering algorithm are as follows:

(1) $D = \{d_1, \ldots, d_i, \ldots, d_n\}$ is a set of documents, d_i is an independent cluster, denoted as $c_i = \{d_i\}$, and a large cluster C is used to contain all documents in D, namely, $C = \{c_1, \cdots, c_i, \cdots, c_n\}$.

(2) The algorithm calculates the similarity $\operatorname{sim}(c_i, c_j)$ between any two clusters in C.

(3) According to $\operatorname{sim}(c_i, c_j)$, the algorithm selects a pair of clusters c_i, c_j with the largest similarity, and combines c_i and c_j into a new cluster $c_k = c_i \bigcup c_j$, and the new combination formed by the tuples in Dd is $C = \{c_1, \ldots, c_{n-1}\}$.

(4) The algorithm repeats steps 2 and 3 until all the clusters in C are merged into one cluster or a preset condition is satisfied. The algorithm of split hierarchical clustering is just the opposite of this algorithm, that is, all documents are classified into the same class at the beginning, and then new classes are continuously split on the basis of this class until the termination condition of the clustering is satisfied.

4. Analysis of Dynamic Influence Mechanism of Network Public Opinion Based on Intelligent Computer Network Simulation

The Internet is a virtual world, the identities of speakers are not disclosed, and there is a lack of corresponding rules and effective supervision. The Internet has gradually become an external space for some netizens to vent their emotions. Due to the influence of various environmental factors, some online speech is irrational, easily sentimental, and emotional, and some people use the Internet as a place to vent their negative emotions and spread and infect each other through the Internet. These emotional remarks are likely to gradually develop into public opinion that is harmful to society under the response of the public. Moreover, with the development of cyberspace, more and more technical methods and ideas have been applied to network public opinion. The components of network public opinion can be divided into the subject, object, ontology, media, and network public opinion environment. The elements of network public opinion are shown in Figure 1.

The dissemination of online public opinion is a process of continuous fermentation and dissemination on the Internet through communication channels after the formation of public opinion. Moreover, the network public opinion dissemination channel is an important part of the occurrence and development of public opinion. Online public opinion dissemination channels are mostly online social platforms such as "two microchannels, one end, and one forum," while knowledge platforms, live webcasts, and microvideos have also become one of the channels for online public opinion dissemination. The dissemination channels of online public opinion are shown in Figure 2.

According to the actual application requirements of the new media industry network public opinion monitoring and analysis subsystem, this paper combines the crawler technology and sentiment analysis technology to design the overall architecture of the new media industry network public opinion monitoring and analysis subsystem. The framework of this system is mainly divided into six layers: public opinion collection, public opinion

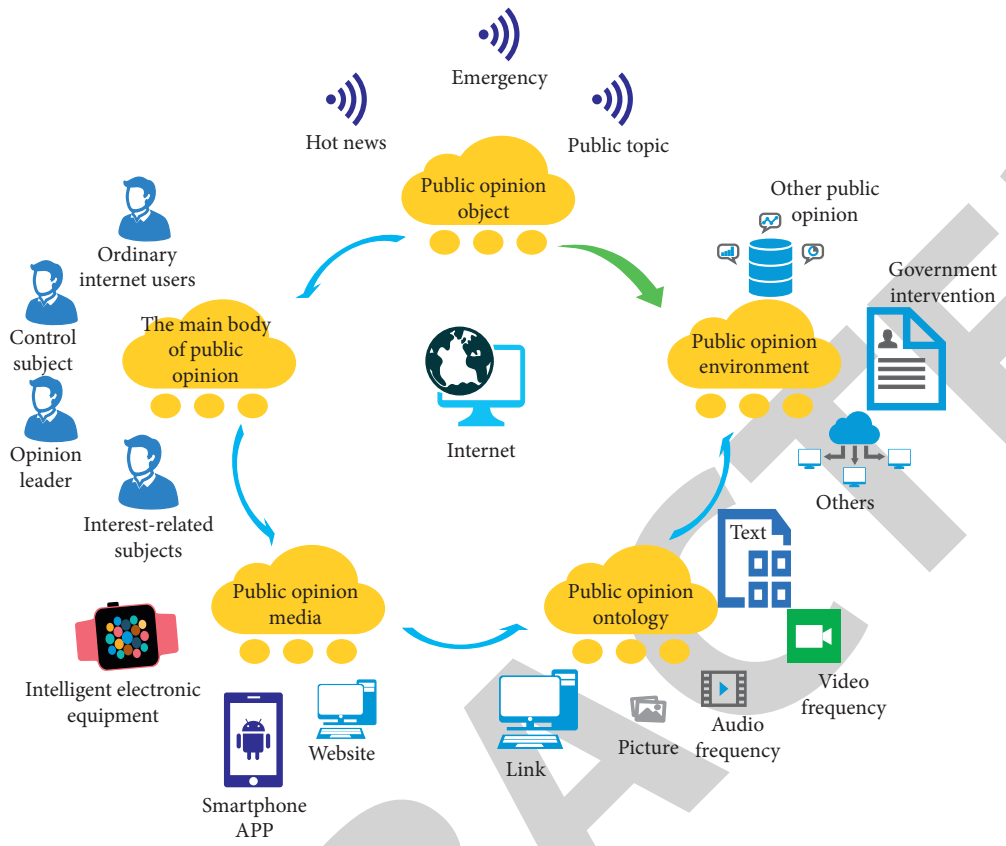


Figure 1: Diagram of the elements of network public opinion.

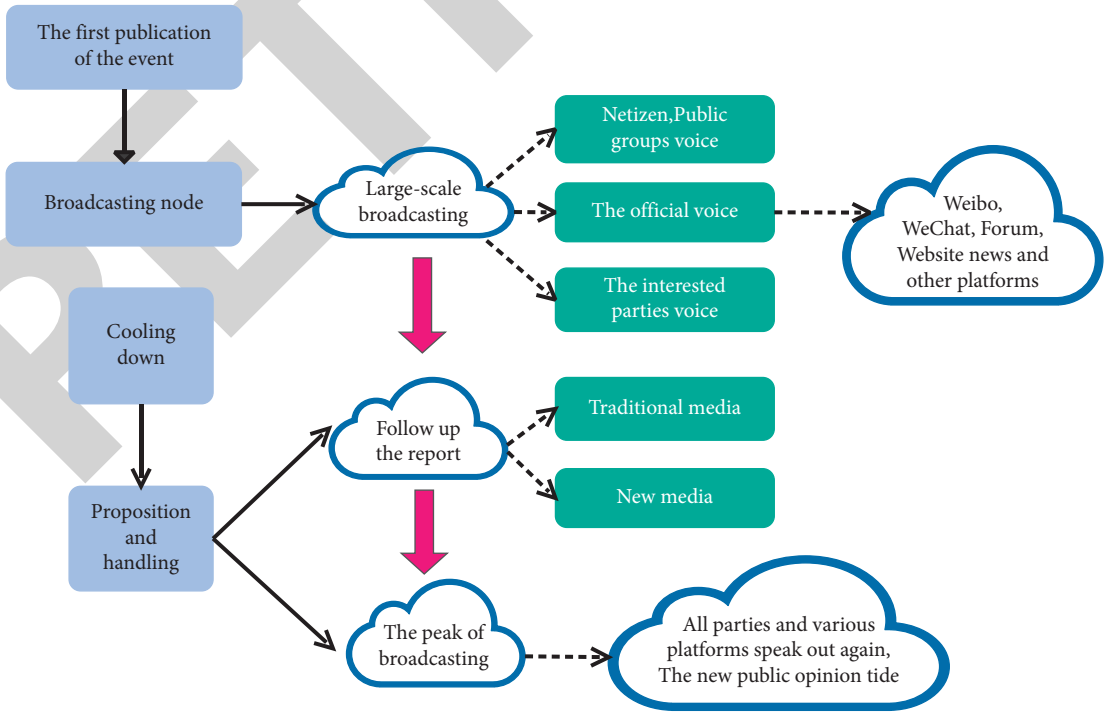


Figure 2: Network public opinion dissemination channel diagram.

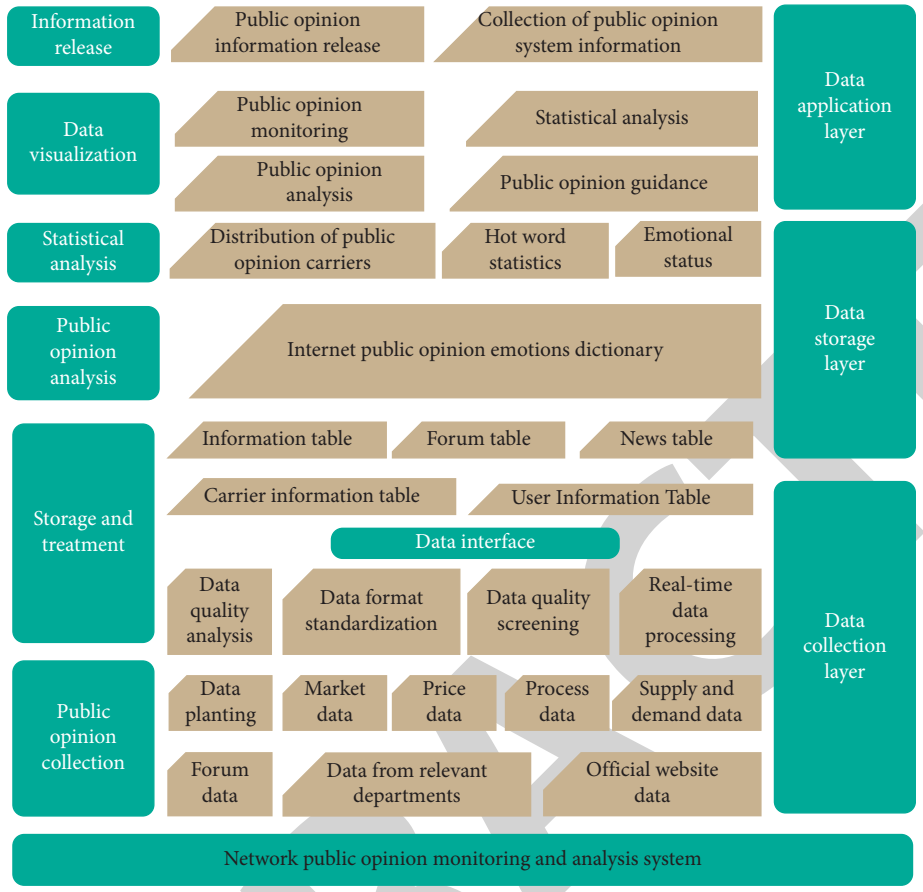


Figure 3: Architecture diagram of network public opinion monitoring and analysis system.

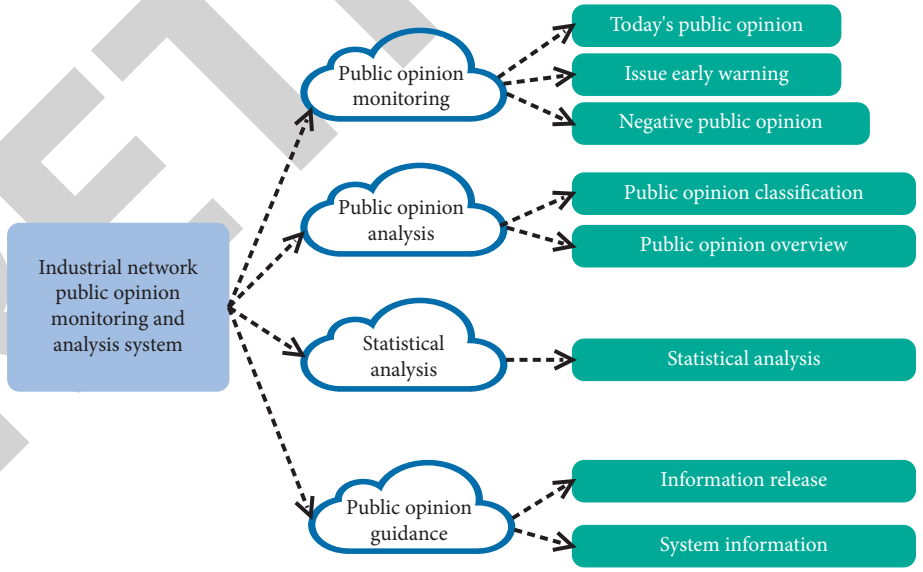


Figure 4: Functional structure diagram of the public opinion monitoring and analysis system.

storage and processing, public opinion analysis, statistical analysis, data visualization, and information release. The system can not only perform statistical analysis on the latest and historical network public opinion of the new media industry but also improve the system's ability of public opinion information storage, public opinion analysis, statistical analysis, and practical application. The architecture of the network public opinion monitoring and analysis subsystem of the new media industry is shown in Figure 3.

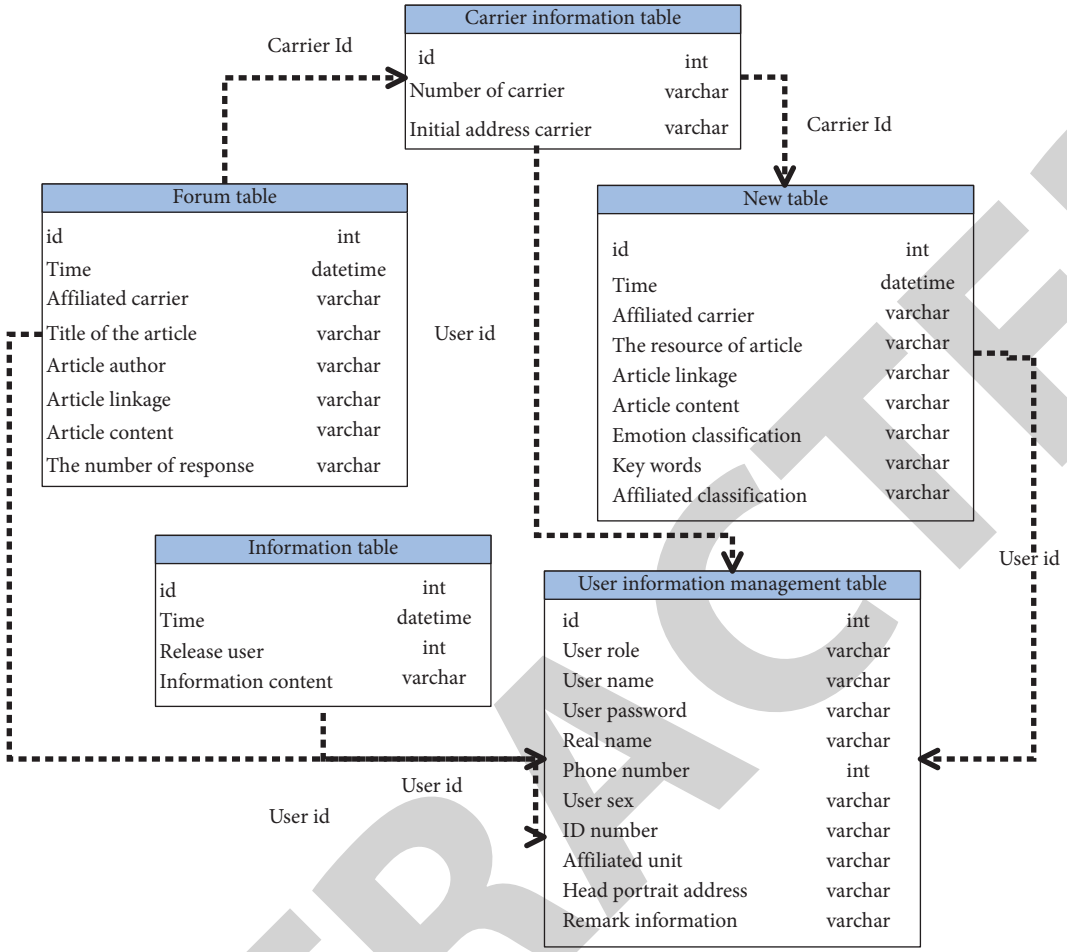
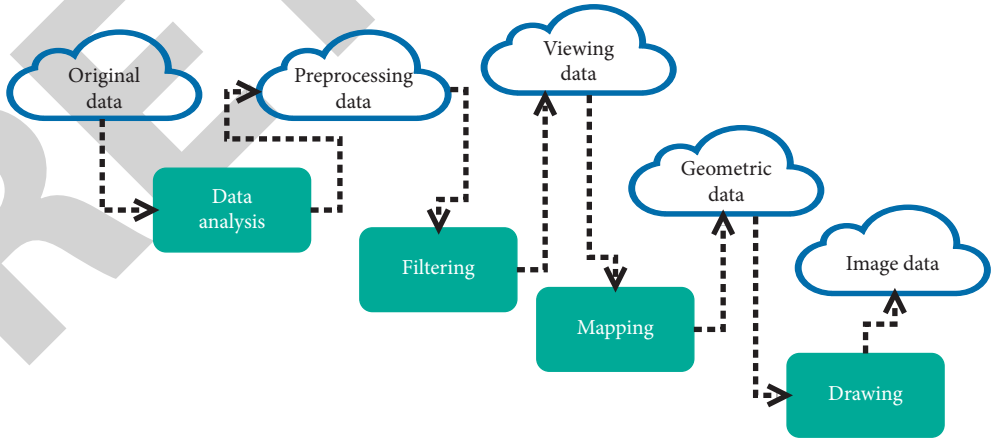


Figure 5: Database structure diagram.



(a)

Figure 6: Continued.

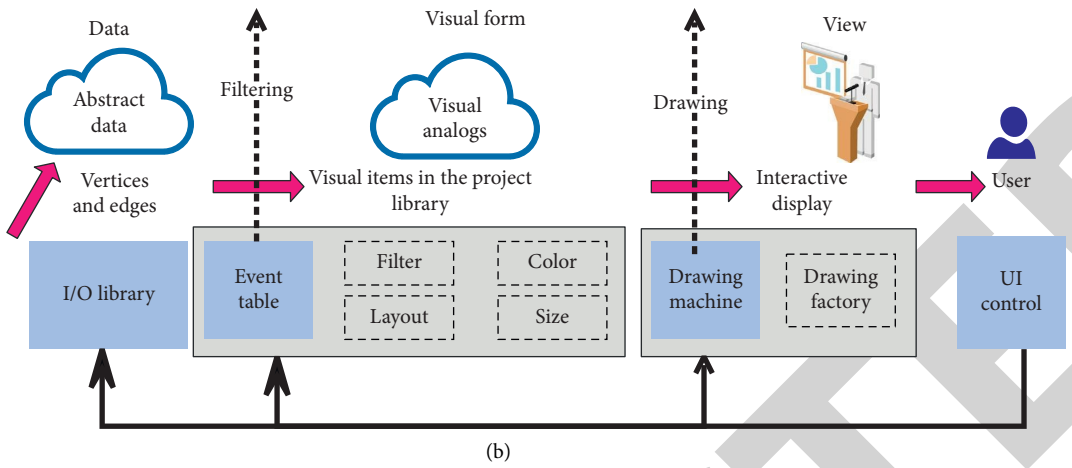


Figure 6: Network public opinion visualization process. (a) Scientific visualization pipeline. (b) Information visualization process.

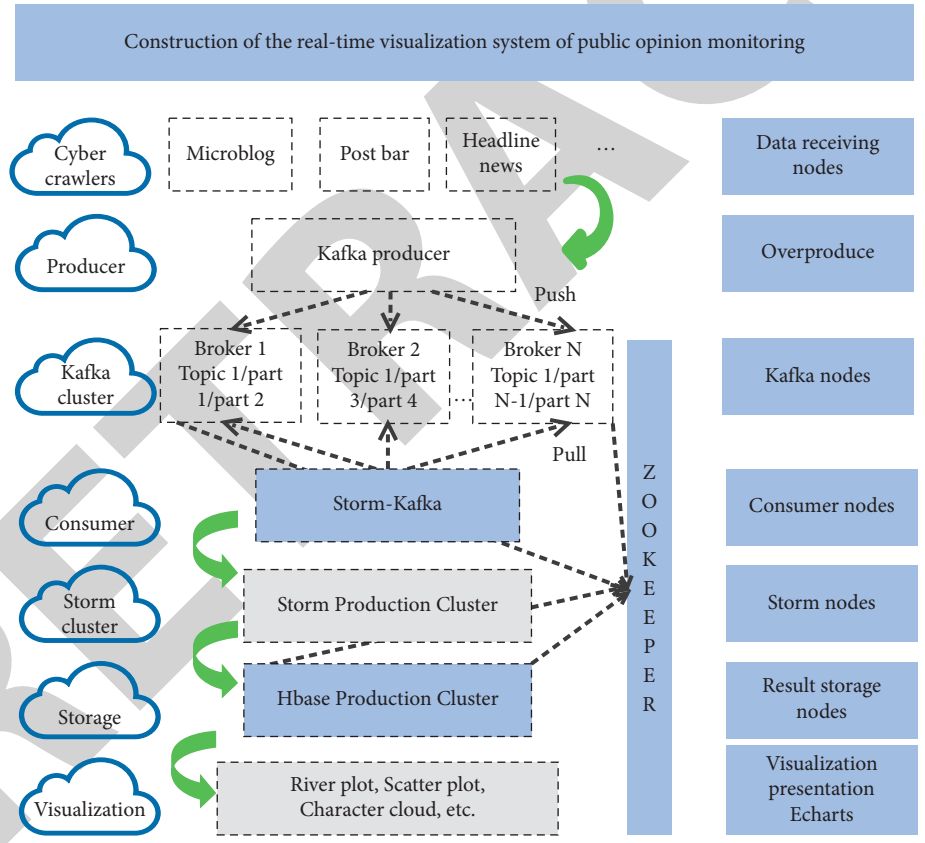


Figure 7: The architecture of the real-time visual monitoring system for network public opinion.

Based on the analysis of the actual needs of the new media industry, this paper designs the network public opinion monitoring and analysis subsystem of the new media industry, which is mainly composed of four modules: public opinion monitoring, public opinion analysis, statistical analysis, and public opinion guidance. Among them, public opinion monitoring includes three submodules: today's public opinion, issuing early warning, and negative public opinion. The public opinion analysis includes two submodules: public opinion classification and public opinion overview. The public opinion guide includes two submodules: news release and system news. The functional structure of the new media industry public opinion monitoring and analysis subsystem is shown in Figure 4.

According to the characteristics that most of the network public opinion data in the new media industry are in the

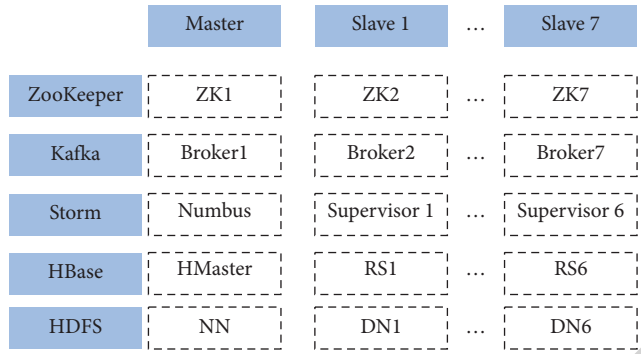


Figure 8: Schematic diagram of cluster deployment of network public opinion monitoring system.

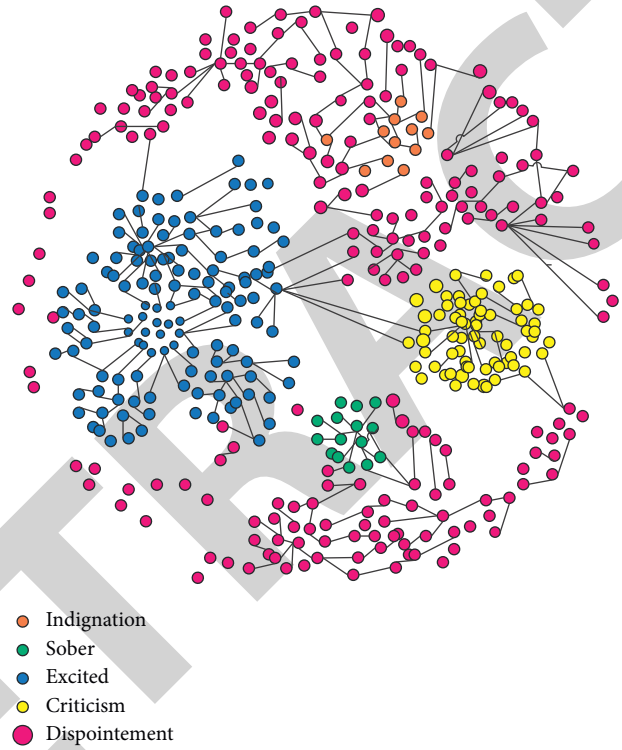


Figure 9: Diagram of audience sentiment clustering results.

form of text, the system uses a MySQL database that has good storage and processing capabilities for structured data. In order to better manage these network public opinion data, the structure of each table needs to be designed. The main table structure of this system is shown in Figure 5.

Visualization technology specifically describes the conversion process from data to visualization and obtains image data step by step in a serial manner to realize data visualization, as shown in Figure 6.

According to the main functions and design goals, the entire network public opinion real-time visual monitoring system is divided into seven layers: data receiving layer, producer layer, message queue layer, consumer layer, business logic layer, storage layer, and visual presentation layer. Among them, the data receiving layer is to obtain network public opinion data through web crawler. The message queue layer is composed of Kafka, a high-throughput distributed publish-subscribe messaging system, which can process all action flow data in consumer-scale websites and support buffering. The business logic layer adopts the real-time stream computing framework Storm. The storage layer uses the distributed, column-oriented open source database Hbase. The final visualization display uses Baidu open source visualization processing controller Echarts as the visualization data display. The detailed architecture is shown in Figure 7.

The network public opinion monitoring system uses multiple distributed architectures, and the deployment and configuration of clusters in the early stage are complex. Figure 8 shows the cluster environment built and deployed by the network public opinion monitoring system.

Table 1: Statistical table of the analysis effect of the analysis model of the dynamic influence mechanism of network public opinion based on intelligent computer network simulation.

Num	The effect of network public opinion analysis	Num	The effect of network public opinion analysis	Num	The effect of network public opinion analysis
1	89.23	25	82.65	49	87.69
2	84.74	26	82.15	50	85.83
3	91.25	27	86.26	51	80.75
4	85.94	28	86.55	52	93.84
5	80.86	29	80.83	53	92.93
6	79.19	30	80.48	54	92.69
7	87.29	31	91.26	55	80.16
8	80.35	32	81.92	56	92.27
9	89.33	33	82.15	57	84.46
10	87.30	34	93.21	58	89.93
11	89.68	35	89.47	59	93.94
12	84.96	36	85.67	60	90.32
13	85.46	37	88.75	61	79.96
14	85.37	38	79.71	62	79.34
15	91.82	39	83.13	63	85.45
16	82.66	40	81.49	64	84.63
17	84.62	41	86.55	65	86.64
18	89.17	42	85.79	66	90.03
19	82.86	43	92.15	67	89.97
20	79.93	44	83.02	68	87.67
21	84.57	45	83.94	69	92.02
22	82.00	46	79.75	70	81.99
23	90.95	47	88.64	71	90.22
24	93.00	48	92.04	72	91.33

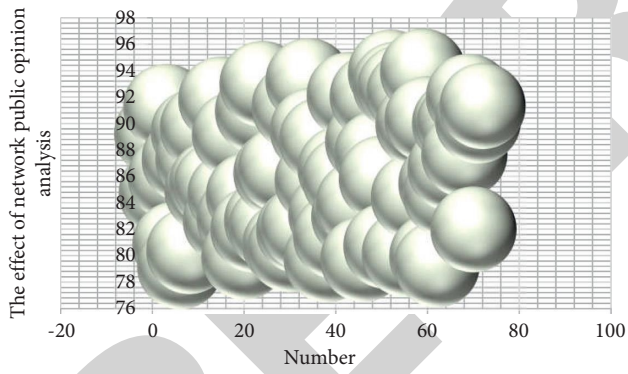


Figure 10: Statistical diagram of the analysis effect of the analysis model of the dynamic influence mechanism of network public opinion based on intelligent computer network simulation.

Cluster analysis and visualization visualize related information to help users quickly perceive the association between different data, so as to highlight the time-series evolution of cluster features. Figure 9 shows the clustering results of audience sentiment for D&G insulting China incidents analyzed by the model in this paper.

This paper takes the past network public opinion data as the output, processes it through the model of this paper, and verifies the effect of the intelligent network public opinion impact analysis model of this paper through network public opinion analysis, and obtains the results shown in Table 1 and Figure 10.

From the above analysis, it can be seen that the analysis model of network public opinion dynamic influence mechanism based on intelligent computer network simulation constructed in this paper has a good effect.

5. Conclusion

The interaction of circles, media reports, and the attention of opinion leaders have led to the outbreak of public opinion. The outpouring of public opinion in this period, short video rumors, follow-up videos, etc. may add another fire to public opinion, and the phenomenon of public opinion reversal occurs from time to time, which urges relevant departments to intervene. After the relevant parties involved took effective measures to deal with the public opinion, the public opinion also entered a recovery period and a calm period. However, the release of follow-up videos may push public opinion to an outbreak period again, and especially, some users of short video apps may not pay attention to other media such as Weibo and online media. In this paper, an intelligent computer network simulation model is constructed to analyze the dynamic influence mechanism of network public opinion. By analyzing the text content to be mined, this paper uses a specific algorithm to select different words that best represent the text to be tested as the characteristic words of network public opinion. These network public opinion feature words can classify texts, thereby reducing the complexity of text classification. The experimental study shows that the dynamic influence mechanism analysis model of network public opinion based

Hindawi
Security and Communication Networks
Volume 2022, Article ID 8757594, 12 pages
https://doi.org/10.1155/2022/8757594

Research Article

Reversible Data Hiding in Encrypted Images Based on Adaptive Gradient Prediction

Jiaohua Qin, Zhibin He, Xuyu Xiang, and Yun Tan

School of Computer and Information Engineering, Central South University of Forestry and Technology, Changsha 410004, China

Correspondence should be addressed to Jiaohua Qin; qinjiaohua@163.com

Received 11 January 2022; Revised 24 February 2022; Accepted 2 May 2022; Published 24 May 2022

Academic Editor: Andrea Michienzi

The existing reversible data hiding (RDH) technology solves the problem that the ciphertext data and carrier are easily damaged in the traditional scheme, which has become a research hotspot in information hiding. However, because of the small coverage area of the predictor and poor prediction ability of the existing reversible data hiding in encrypted images (RDH-EI) technology based on pixel predictor, the embedding performance of the algorithm is limited. Therefore, this paper proposes an adaptive gradient prediction (AGP) scheme. The AGP employs a comprehensive and efficient local complexity measurement strategy to make predictions based on pixel changes around the predicted pixel, including horizontal, vertical, and diagonal directions. The experimental results show that the AGP-RDHEI scheme has apparent advantages in embedding rate.

1. Introduction

The development of cloud computing technology has promoted the continuous sharing of massive media data [1], providing users with convenient and low-cost computing and storage services. However, in recent years, personal privacy leaks have occurred many times, resulting in the leakage of a large amount of personal information and resources, and have become the focus of continuous public attention [2]. Therefore, technologies such as digital watermarking and steganography [3, 4] have been proposed successively. Steganography focuses on the imperceptibility of hidden data and embedded data, but the carrier will be tampered. Digital watermarking technology possesses strong robustness, which ignores the integrity of the carrier. However, it is necessary to ensure the carrier's integrity while extracting data losslessly for some specific fields.

Reversible data hiding, different from the above two algorithms, can accurately restore the cover image after extracting the embedded data, and is widely used in military and medical image data hiding [5]. Existing RDH methods can be roughly classified into three parts: lossless compression-based RDH [6, 7], histogram translation-based RDH [8, 9], and differential expansion-based RDH [10, 11]. However, with the continuous improvement of users' requirements for data security, the traditional reversible data hiding technology has been unable to meet the needs of practical applications. Therefore, the researchers put forward to combine the encryption algorithm with the reversible data hiding algorithm, further ensuring the data security during the transmission process, and realizing the reversible data hiding of encrypted images.

The existing RDH-EI technologies are mainly divided into two parts. One is the vacating room after encryption (VRAE) [12, 13], which uses an encryption algorithm to encrypt the original image and then frees up room for secret data embedding. The other is reserving room before encryption (RRBE) [14, 15], which utilizes the spatial correlation of the original image to reserve room, then encrypts the image, and performs secret data embedding. However, traditional RDH-EI needs to synchronize the image restoration and data extraction process at the receiver [15], which requires the recipient to establish a high degree of trust with the content owner. To ensure that the receiver can manipulate the secret data without revealing the content, Zhang [16] first proposed separable RDH-EI, which can perform different operations by sending different keys, so that the receiver's operations are subject to the type of key obtained.

To meet different security requirements, many improved RDH-EI schemes have been proposed [13, 17–19]. Yi and Zhou [13] designed a RDH algorithm based on parametric binary tree labeling (PBTL), making full use of the spatial redundancy of the image, and solved the problem of low embedding rate (ER). Wu et al. [17] proposed an improved parametric binary tree labeling (IPBTL) RDH-EI method and achieved a higher ER than [13], but has low utilization of spatial redundancy. Meanwhile, Yin et al. proposed an RDH encryption image algorithm based on pixel prediction and multi-MSB plane rearrangement [18], which solved the problem of large space for auxiliary information through arithmetic coding and data compression, and introduced the medium edge detector (MED) that improves ER. Subsequently, Yang et al. [19] introduced block scrambling in the encryption algorithm and adaptive coding in the embedding process to improve the compression rate and embedding ability. However, both methods use MED. But MED makes predictions based on three pixels around the predicted pixel: the top pixel, the left pixel, and the top-left pixel. Since the number of pixels involved in the prediction is small, the coverage of the predictor is small, it cannot perceive images with complex textures well, resulting in low prediction accuracy. Consequently, Wu et al. [20] proposed the gradient-adjusted prediction (GAP), which only considers the horizontal and vertical gradients of the pixels in the neighborhood, and the prediction accuracy is still poor for complex images.

To fully consider the characteristics of pixel changes in different images, this paper proposes a pixel prediction scheme based on adaptive gradient based on [17, 20, 21]. When measuring complexity, we add the change in pixels in the diagonal direction to the calculation. At the same time, we combine the AGP with the PBTL scheme to free up more space in the image for secret information embedding. Compared with [17], this method takes the edge information of each image into consideration, achieving more accurate pixel prediction and higher embedding capacity.

The rest of the paper is structured as follows. Section 2 reviews some related research. Section 3 describes the RDH-EI method based on AGP. Section 4 presents the experimental results and analysis. Finally, Section 5 summarizes the paper and proposes future work.

2. Related Work

2.1. Gradient-Adjusted Prediction (GAP). The GAP, proposed by Wu and Memon [20], mainly utilizes the gradient change between adjacent pixels to estimate pixel values. Specifically, it makes predictions through the seven neighborhoods around the current pixel of the cover image, as shown in Figure 1.

2.2. Parameter Binary Tree Labeling (PBTL). The parametric binary tree labeling scheme mainly employs the binary sequence of 1 to 7 bits on the parametric binary tree to label the pixels of different categories. The construction rule of a 7-level binary tree is left 0 right 1. Giving parameters α and β,

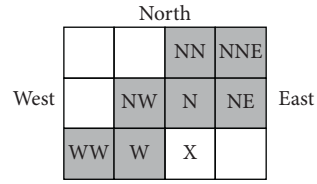


Figure 1: Predictive template used by GAP.

pixels can be divided into embeddable pixel class G_1 and non-embeddable pixel class G_2, where $1 \le \alpha, \beta \le 7$. G_1 consists of embeddable pixels P_e and G_2 includes non-embeddable pixels P_n. The overall algorithm steps can be described as follows:

Step 1: build a 7-layer full-parameter binary tree

Step 2: after determining the parameters α and β, the label sequence of the pixels can be determined according to the parameters and the binary tree.

Step 3: for G_2, all P_n are labeled by β bits of "0, . . ., 0," which is the first node at the β_{th} layer of the binary tree.

Step 4: for G_1, all pixels can be divided into n_α different sub-categories due to the different prediction errors of the pixels. The calculation of n_α is as follows:

$$n_\alpha = \begin{cases} 2^\alpha - 1, & \text{if } \alpha \le \beta, \\ \left(2^\beta - 1\right) * 2^{\alpha - \beta}, & \text{otherwise.} \end{cases} \quad (1)$$

Step 5: after determining the value of n_α, use n_α different nodes from the α_{th} layer of the binary tree to label pixels in G_1 from right to left.

3. Proposed Scheme

The RDH-EI method's general framework using AGP is shown in Figure 2, which can be split into three stages. In the first stage, the content owner measures the local complexity of the predicted pixel and adaptively adjusts the prediction model to calculate the prediction error of the image. Then, the image is encrypted according to the method of stream cipher and the pixels are classified and labeled according to the PBTL scheme to obtain the labeled encrypted image in the second stage. Finally, in the third stage, the image receiver can perform data extraction or image recovery after receiving the stego image. We will introduce each component in the following subsections.

3.1. Pixel Prediction Based on AGP. Since the predicted pixels are mainly predicted according to their adjacent pixels in the process of pixel prediction, the change degree of nearby pixels and the prediction model of the predictor become the key factors affecting the prediction accuracy. However, the existing schemes ignore the pixel changes in the diagonal direction when measuring the local complexity of pixels, causing low prediction accuracy for complex images. Therefore, an adaptive gradient predictor is proposed in this section, and the complexity measurement scheme and prediction model are detailed below.

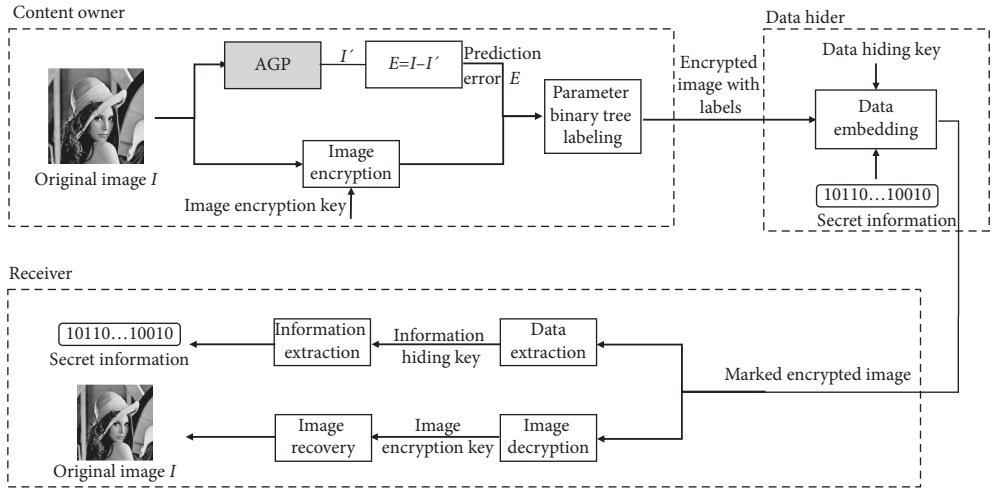


Figure 2: Framework of the proposed scheme.

3.1.1. Local Complexity Measurement. To fully estimate the nearby changes of pixels, this scheme optimizes the GAP. Specifically, we consider the pixel changes in the diagonal direction when calculating the local complexity, and introduce diagonal and anti-diagonal gradients when measuring local complexity, as shown in Figure 3.

The red and blue arrows represent the diagonal and the anti-diagonal direction. The gradient of intensity at the current pixel $I_{(i,j)}$ can be formulated as:

$$\begin{aligned} g_x &= \left|I_{(i,j-1)} - I_{(i,j-2)}\right| + \left|I_{(i-1,j)} - I_{(i-1,j-1)}\right| \\ &\quad + \left|I_{(i-1,j)} - I_{(i-1,j+1)}\right| + \left|I_{(i-1,j-1)} - I_{(i-1,j-2)}\right|, \\ g_y &= \left|I_{(i,j-1)} - I_{(i-1,j-1)}\right| + \left|I_{(i-1,j)} - I_{(i-2,j)}\right| \\ &\quad + \left|I_{(i-1,j+1)} - I_{(i-2,j+1)}\right| + \left|I_{(i,j-2)} - I_{(i-1,j-2)}\right|, \\ g'_x &= \left|I_{(i-1,j-2)} - I_{(i,j-1)}\right| + \left|I_{(i-2,j)} - I_{(i-1,j+1)}\right|, \\ g'_y &= \left|I_{(i-2,j+1)} - I_{(i-1,j)}\right| + \left|I_{(i-1,j-1)} - I_{(i,j-2)}\right|, \end{aligned} \tag{2}$$

where g_x, g_y, g'_x and g'_y represent the estimated gradient of the predicted pixel in the horizontal, vertical, diagonal, and anti-diagonal directions, respectively. The value of g_x, g_y, g'_x and g'_y are used to detect the magnitude and orientation of edges in the cover image, and make necessary adjustments in the prediction to obtain better prediction results under the local edges of the image.

The local complexity D_1, D_2 of the predicted pixel is formulated as:

$$\begin{aligned} D_1 &= g_x - g_{y'}, \\ D_2 &= g'_x - g'_y, \end{aligned} \tag{3}$$

where D_1 denotes the gradient complexity in the horizontal and vertical directions, D_2 is the gradient complexity in the diagonal and anti-diagonal directions. The value of D_1 and D_2 are used to detect the complexity around the pixel.

According to the local complexity measurement method above, we divide the situation around the predicted pixel

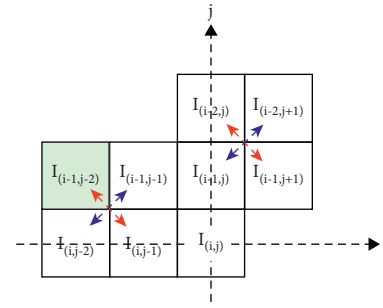


Figure 3: Diagonal gradient and anti-angle gradient.

into sharp and non-sharp edges. When the surrounding pixel value of the predicted pixel varies greatly, the value of the predicted pixel can be calculated by:

$$I'_{(i,j)} = \begin{cases} I_{(i,j-1)} + \lfloor \frac{h_1}{2} + \frac{h_2}{8} + \frac{d_1}{8} + \frac{d_2}{8}, & D_1 > T_1 \text{ and } D_2 > T_4, \\ I_{(i,j-1)} + \lfloor \frac{h_1}{2} + \frac{h_2}{8} + \frac{d_1}{64} + \frac{d_2}{64}, & D_1 > T_1 \text{ and } D_2 \le T_4, \\ I_{(i-1,j)} + \lfloor \frac{v_2}{2} + \frac{v_3}{8} + \frac{a_1}{8} + \frac{a_2}{16}, & D_1 < -T_1 \text{ and } D_2 < -T_4, \\ I_{(i-1,j)} + \lfloor \frac{v_2}{2} + \frac{v_3}{8} + \frac{d_1}{64} + \frac{d_2}{64}, & D_1 < -T_1 \text{ and } D_2 \ge -T_4. \end{cases} \tag{4}$$

Otherwise, if the position of the predicted pixel is a non-sharp edge, the predicted value is mainly affected by the prediction operator θ, which is defined as follows:

$$\begin{aligned} \theta = \lfloor & \frac{\left(I_{(i-1,j)} + I_{(i,j-1)}\right)}{2} + \frac{\left(I_{(i-1,j+1)} - I_{(i-1,j-1)}\right)}{4} \\ & + \frac{d_1}{32} + \frac{a_1}{8} + \frac{a_2}{8} + \frac{h_3}{8} + \frac{v_1}{8}. \end{aligned} \tag{5}$$

The value of θ is used to fine-tune the predicted value. The predicted value is calculated as follows:

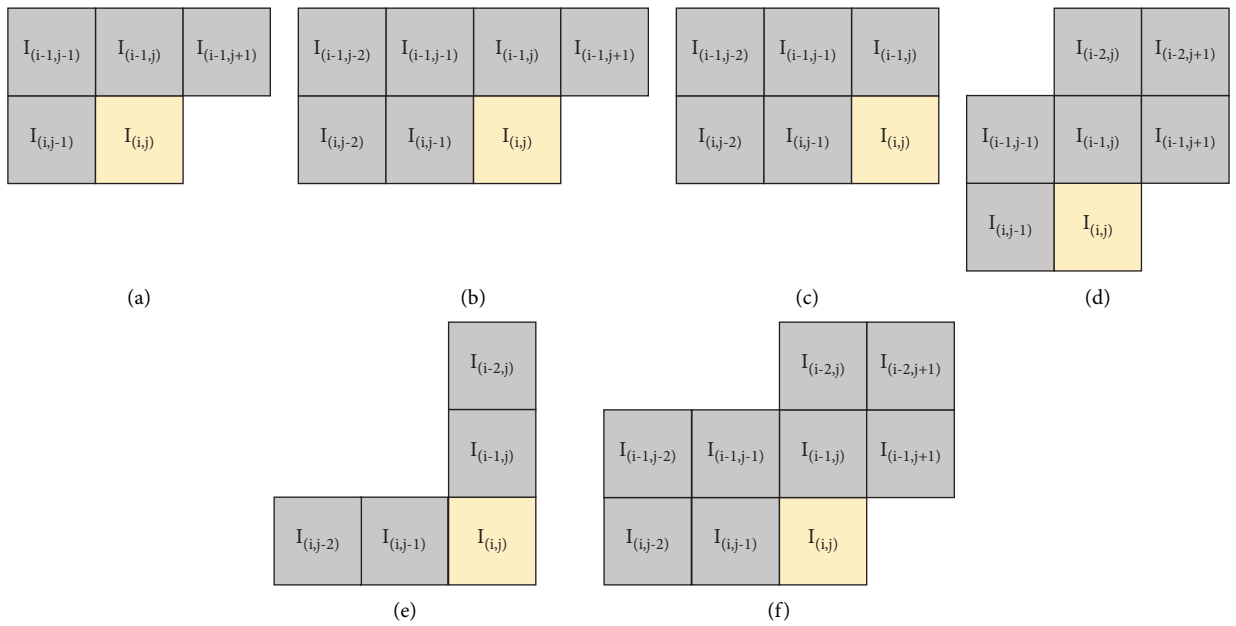


FIGURE 4: Prediction model of AGP in different locations. (a) $i = 2, j = 2$. (b) $i = 2, 2 < j <$ col. (c) $i = 2, j =$ col. (d) $2 < i <$ row, $j = 2$. (e) $i =$ row, $j =$ col. (f) Others.

$$I'_{(i,j)} = \begin{cases} \left\lfloor \dfrac{\left(\theta + I_{(i,j-1)}\right)}{2} + \dfrac{h_2}{8} + \dfrac{a_1}{32} + \dfrac{d_1}{16}, & D_1 > T_2, \\ \left\lfloor \dfrac{\left(3 * \theta + I_{(i,j-1)}\right)}{4} + \dfrac{h_2}{16} + \dfrac{a_1}{32} + \dfrac{d_1}{64}, & D_1 > T_3, \\ \left\lfloor \dfrac{\left(\theta + I_{(i-1,j)}\right)}{2} + \dfrac{h_2}{8} + \dfrac{a_2}{8} + \dfrac{d_2}{8}, & D_1 < -T_2, \\ \dfrac{\left(3 * \theta + I_{(i-1,j)}\right)}{4} + \dfrac{h_2}{8} + \dfrac{a_2}{8} + \dfrac{d_2}{8}, & D_1 < -T_3, \end{cases} \tag{6}$$

where T_1, T_2, T_3 denotes the thresholds used to determine the edge of the pixel. The value of T_1, T_2 and T_3 are used to judge horizontal and vertical edges. T_4 is adopted to judge diagonal edges. The strategy for threshold selection is described experimentally in Section 4.3.

For convenience, this part uses h_k, $v_k (k = 1, 2, 3, 4)$ to represent the horizontal and vertical gradients, and d_r, $a_r (r = 1, 2)$ to represent the diagonal and anti-diagonal gradient, which can be formulated respectively as:

$$\begin{aligned} h_1 &= I_{(i,j-1)} - I_{(i,j-2)} v_1 = I_{(i,j-1)} - I_{(i-1,j-1)}, \\ h_2 &= I_{(i-1,j)} - I_{(i-1,j-1)} v_2 = I_{(i-1,j)} - I_{(i-2,j)}, \\ h_3 &= I_{(i-1,j)} - I_{(i-1,j+1)} v_3 = I_{(i-1,j+1)} - I_{(i-2,j+1)}, \\ h_4 &= I_{(i-1,j-1)} - I_{(i-1,j-2)} v_4 = I_{(i,j-2)} - I_{(i-1,j-2)}, \\ d_1 &= I_{(i-1,j-2)} - I_{(i,j-1)} a_1 = I_{(i-2,j+1)} - I_{(i-1,j)}, \\ d_2 &= I_{(i-2,j)} - I_{(i-1,j+1)} a_2 = I_{(i-1,j-1)} - I_{(i,j-2)}. \end{aligned} \tag{7}$$

3.1.2. Adaptive Gradient Prediction Model. Most of the existing pixel prediction schemes can improve the performance of simple images, but its performance cannot be well developed for complex images with complex content and rich texture. The AGP can be shown in Figure 4. In the pixel prediction stage, the pixels in the first row and the first column of the image, as reference pixels, remain unchanged, and are used to predict the remaining pixels of the image in the image restoration stage. Since the position of the predicted pixel is constantly changing, AGP will adaptively adjust the prediction model according to the position of the pixel.

After the predicted image is calculated from the cover image by the AGP algorithm, the prediction error matrix elements are calculated by subtracting the predicted image from the cover image. The prediction error $E_{(i,j)}$ is defined as:

$$E_{(i,j)} = I_{(i,j)} - I'_{(i,j)}, \tag{8}$$

where $I_{(i,j)}$ and (i, j) is the original pixel value of the cover image and the predicted pixel value of the predicted image, respectively.

3.2. Image Encryption Based on Stream Cipher. In the stage of image encryption, we use stream cipher to encrypt the image and secret data, which can be formulated as follows:

$$I_E(i, j)_k = \left\lfloor \frac{I(i, j)}{2^{k-1}} \right\rfloor \oplus r(i, j)_k, \quad k \in \{1, 2, \ldots, 8\}, \tag{9}$$

where $\lfloor * \rfloor$ denotes round down, $I_E(i, j)_k$ denotes the result of image pixel $I(i, j)$ encryption, $\oplus$ is the exclusive OR operation, and $r(i, j)_k$ is the bitstream generated by the pseudo-random matrix $R_{m \times n}$. The content owner uses the

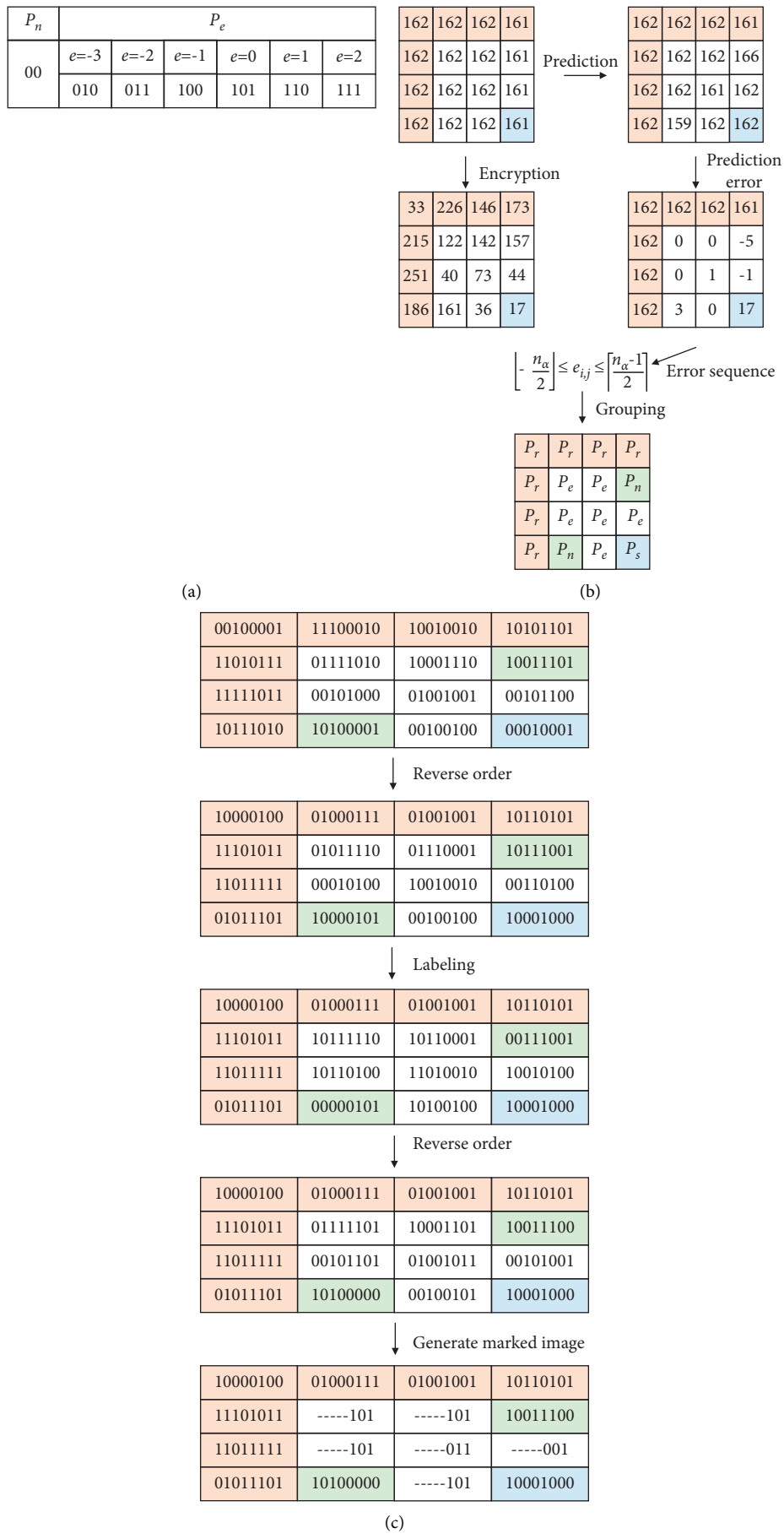
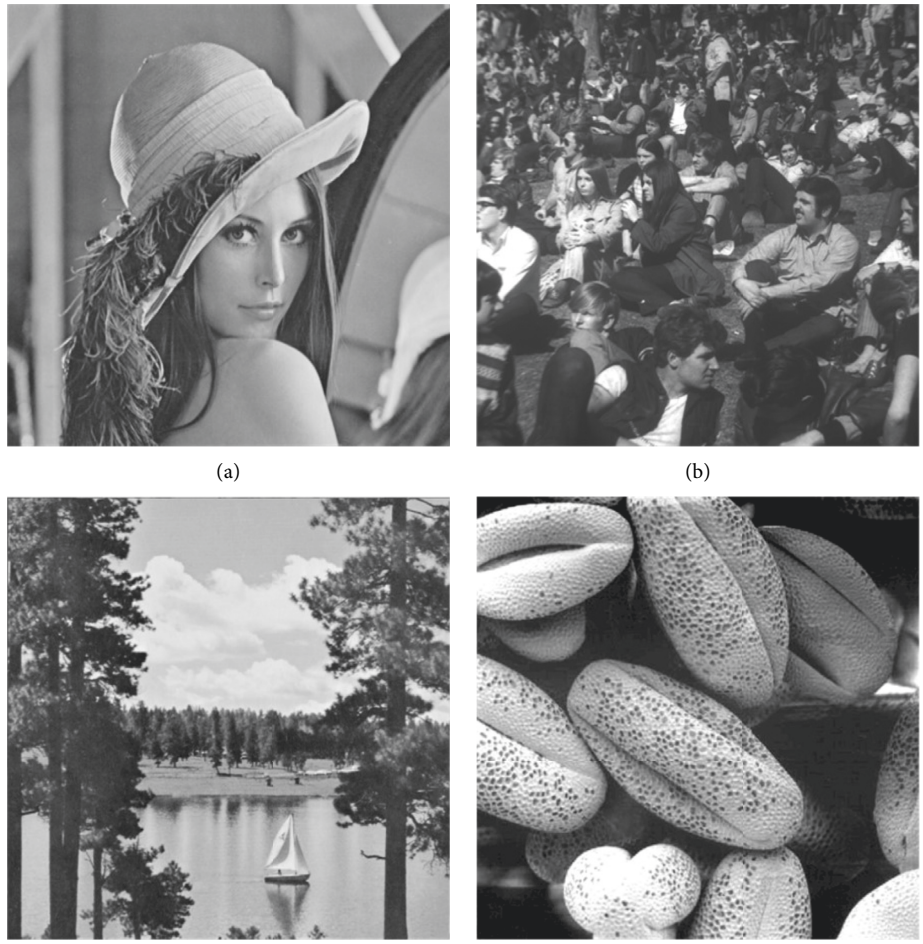


Figure 5: PBTL-based labeling process. (a) Marker bit selection. (b) Pixel grouping. (c) Pixel labeling.



(a) (b) (c) (d)

Figure 6: Test images. (a) Lena. (b) Crowd. (c) Lake. (d) Beans.

encryption key to generate a pseudo-random matrix $R_{m\times n}$, and then performs an exclusive OR operation with each bit of the image pixel to obtain the encrypted image bitstream.

3.3. PBTL-Based Pixel Grouping and Labeling. Inspired by IPBTL [17], we combine the AGP scheme and PBTL scheme in this paper. The content owner first performs pixel prediction on the original image via AGP, and then separates all pixels into four sets based on the prediction error, namely: reference pixel P_r, embeddable pixel P_e, non-embeddable pixel P_n and special pixel P_s. P_r remains unchanged during the prediction and recovery stages, which is used to predict the remaining pixels. At the same time, P_s remains unchanged during the data embedding process, which is employed to store parameters α and β. The remaining two sets are classified by equation (10).

If $E_{(i,j)}$ satisfies the following condition, the pixel $I_{(i,j)}$ belongs to P_e. Otherwise, it belongs to P_n.

$$I_{(i,j)} \in \begin{cases} P_e, & \left\lfloor -\frac{n_\alpha}{2} \right\rfloor \le E_{(i,j)} \le \left\lceil \frac{n_\alpha - 1}{2} \right\rceil, \\ P_n, & \text{others}, \end{cases} \tag{10}$$

where $E_{(i,j)}$ represents the prediction error of $I_{(i,j)}$, $\lceil * \rceil$ and $\lfloor * \rfloor$ represent the ceil and floor operations, respectively. n_α can be calculated by equation (1). N_r, N_e, and N_n denote the number of P_r, P_e, and P_n, respectively. P_s is the pixel for storing parameters. Thus, the whole image $m \times n = N_r + N_e + N_n + 1$.

Since pixels P_r and P_s are pre-defined, they can be easily distinguished, and only pixels in P_e and P_n need to be labeled. First, two parameters, α and β are obtained. Then, we use the binary code generated by PBTL to label pixels in P_e and P_n. Precisely speaking, for each pixels in P_n, it is only necessary to replace β bits binary sequence "0, ..., 0" with the most significant bits (MSB) of P_n by bit replacement, and the remaining other $(8 - \beta)$ bits unchanged. Simultaneously, for each pixel in P_e, we classify it into n_α different subcategories according to different values of $E_{(i,j)}$, and label it by n_α different α bits binary codes. Due to the correlation between pixels, adjacent pixels may have the same prediction error which can be labeled with the same binary code. Since marking the MSB of a pixel by bit substitution may lead to the leakage of the content information of the image, this paper inverts the binary code of all pixels in the labeling process to ensure the security of the image content. Figure 5(a) shows the labeling sequence corresponding to

Table 1: Threshold selection strategy.

T_1	ER(bpp)	T_2	ER(bpp)	T_3	ER(bpp)	T_4	ER(bpp)
50	2.7504	2	2.7420	2	2.7546	50	2.7520
60	2.7527	4	2.7448	4	2.7550	60	2.7525
70	2.7537	8	2.7479	**8**	**2.7551**	70	2.7528
80	**2.7551**	16	2.7526	16	2.7530	**80**	**2.7551**
90	2.7550	**32**	**2.7551**	32	2.7461	90	2.7530
100	2.7548	64	2.7510	64	2.7461	100	2.7530
110	2.7544	128	2.7460	128	2.7461	110	2.7530

different prediction errors; Figure 5(b) represents the classification of pixels according to the prediction error, and the pixel labeling process based on PBTL can be seen in Figure 5(c).

3.4. Data Extraction and Image Recovery. After receiving the marked image, we extract the parameters α and β from P_s firstly, by which the binary tree can be restored. The positions of P_e and P_n can be determined by checking the labeled bits of the non-reference pixels. The extracted data includes two parts: secret data and auxiliary information. Auxiliary information is applied to recover the cover image, which consists of the replaced original β bits of pixel in P_n and the original 8 bits of pixel in P_s.

Subsequently, we employ the embedding data for the original data recovery. The embedding pixel P_e includes α bits labeling bits and $(8-\alpha)$ bits for embedding data. Therefore, the entire embedded data includes $(8-\alpha)*N_e$ bits, where the number of auxiliary information and secret data is $(8+\beta*N_n)$ bits and $(8-\alpha)*N_e-(8+\beta*N_n)$ bits, respectively. To ensure the security of the approach, the embedded data and cover image are encrypted through k_d and k_e, respectively. Finally, the encrypted stego image can be generated.

In order to effectively evaluate the embedding performance of our method, we adopt the embedding rate $r_{\alpha,\beta}$ as the measurement index, which is defined as:

$$r_{\alpha,\beta}=\frac{(8-\alpha)*N_e-(8+\beta*N_n)}{m*n}, \tag{11}$$

where the maximum embedding rate $r_{\max}$(bpp) can be formulated as:

$$r_{\max}=\max\left(r_{\alpha,\beta}\right)_{\alpha,\beta=1}^{7}. \tag{12}$$

To show more details of the scheme, we take the pixel labeling process when the parameter is $\alpha=3,\beta=2$ as an example and display it in Figure 5. The labeling bits selection is shown in Figure 5(a), where P_n is labeled with "00," and P_e is labeled with "010," "011," "100," "101," "110" and "111." For example, pixels with a prediction error of "−3" are labeled with the sequence of "010." The detailed process of secret data extraction can be summarized as follows:

Step 1: after receiving the marked encrypted image I_E and data hiding key k_d, the receiver firstly extracts parameters α and β from the pre-defined special pixel P_s.

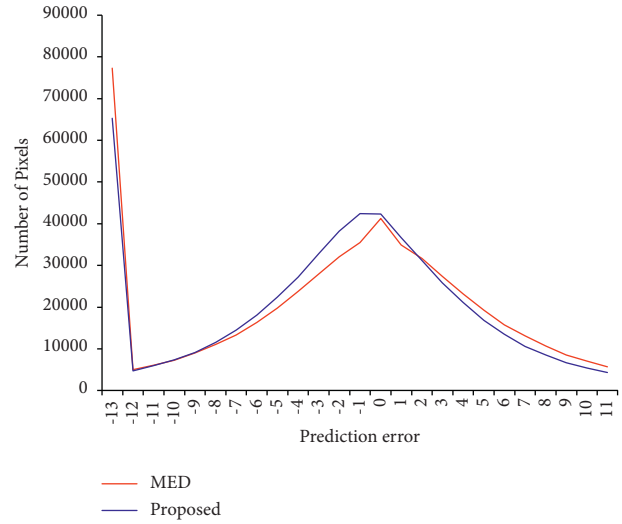


Figure 7: Prediction performance comparison.

Step 2: check α or β bits label of remaining pixels in the 8 bits binary sequence in the reverse order.

Step 3: classify them into embeddable pixel set P_e and non-embeddable pixel set P_n.

Step 4: extract $(8-\alpha)$ bits of the payload from the pixel in turn, and obtain the encrypted data.

Step 5: decrypt the original secret information D by using k_d.

After obtaining the marked image, the recipient can restore the original image only by obtaining the image encryption key k_e. First, the auxiliary information is extracted in the embedded data. Next, we recover the replaced bits in P_n and the original 8 bits binary sequence in P_s by the first part of the auxiliary information and the second part of the auxiliary information, respectively. Then, the original values of P_n and P_s are restored according to the auxiliary information. Finally, the key k_e is used to fully obtain the original image.

4. Experimental Results and Analysis

To verify the performance of the proposed method, this section designs many experiments. This section consists of five parts. The experimental environment and the dataset used are introduced in Sections 4.1 and 4.2. Threshold selection experiments and comparative experiments for

Table 2: The embedding rate of the test images when $\beta = 3, \alpha = 1, \ldots, 7$.

Image	(α, β)	(2, 3)	(3, 3)	(4, 3)	(5, 3)	(6, 3)	(7, 3)
Lena	MED	—	1.7087	2.7872	2.6770	1.9407	0.9929
	GAP	—	2.0343	2.9882	2.7369	1.9537	0.9945
	Proposed	—	**2.0664**	**3.0642**	**2.7874**	**1.9689**	**0.9957**
Crowd	MED	0.9243	2.2093	2.6540	2.5488	1.9133	0.9932
	GAP	0.9153	2.2540	2.7320	2.5863	1.9245	0.9937
	Proposed	**0.9985**	**2.3671**	**2.8291**	**2.6379**	**1.9370**	**0.9939**
Lake	MED	—	—	1.2060	2.0836	1.8390	0.9906
	GAP	—	0.1794	1.5029	2.2203	1.8547	0.9901
	Proposed	—	**0.2786**	**1.5751**	**2.2413**	**1.8665**	**0.9909**
Beans	MED	—	**0.8664**	1.7448	2.2484	1.8867	0.9912
	GAP	—	0.7109	1.6675	2.1988	1.8780	0.9909
	Proposed	—	0.7937	**1.7787**	**2.2785**	**1.8996**	**0.9927**

Table 3: The embedding rate of the test images when $\beta = 2, \alpha = 1, \ldots, 7$.

Image	(α, β)	(2, 2)	(3, 2)	(4, 2)	(5, 2)	(6, 2)	(7, 2)
Lena	MED	0.3933	1.6609	2.6867	2.6447	1.9285	0.9919
	GAP	**0.6109**	2.0127	2.8977	2.7055	1.9440	0.9935
	Proposed	0.6022	**2.0573**	**2.9596**	**2.7551**	**1.9595**	**0.9951**
Crowd	MED	1.4856	2.3263	2.6530	2.5180	1.8966	0.9906
	GAP	1.4777	2.3745	2.7126	2.5536	1.9071	0.9912
	Proposed	**1.5516**	**2.4751**	**2.8050**	**2.6053**	**1.9228**	**0.9922**
Lake	MED	—	0.2035	1.2433	1.9997	1.8080	0.9856
	GAP	—	0.4672	1.5093	2.1449	1.8284	0.9852
	Proposed	—	**0.5587**	**1.5769**	**2.1707**	**1.8399**	**0.9866**
Beans	MED	**0.5456**	**1.1069**	1.8032	2.1669	1.8569	0.9880
	GAP	0.2821	0.9647	1.7169	2.1335	1.8461	0.9877
	Proposed	0.2842	1.0453	**1.8053**	**2.2070**	**1.8691**	**0.9906**

predictors are presented in Section 4.3. Four gray images, Lena, Crowd, Lake, and Beans shown in Figure 6 are used to display the specific performance in our experiments in Section 4.4. To reduce the effect of image randomness on the authenticity of the results, the average embedding rate on three large image datasets: UCID [22], BOSSbase [23], and BOWS-2 [24]is compared. Some evaluation indexes estimate the performance of the proposed scheme, i.e., embedding rate, peak signal-to-noise ratio (PSNR), and structural similarity index (SSIM) experiments.

4.1. Experimental Environment. This experiment uses Intel(R) Core (TM) i7-10750H CPU @ 2.60 GHz, 16.00 GB RAM, and Nvidia GeForce RTX 2060 gpu. All experiments are done under MATLAB R2019a.

4.2. Datasets. The specific description of the three datasets is as follows:

(1) UCID: The UCID dataset was created by Gerald Schaefer et al. It contains 1338 uncompressed TIFF images, involving various subjects such as indoor and outdoor natural scenes and artificial objects, all taken by a digital color camera. This dataset is mainly used to evaluate image compression and color quantization.

(2) BOSSbase: Patrick Bas and others created BOSSbase. The BOSSbase dataset consists of uncompressed images taken by seven different cameras. All images are created from full-resolution color images and are finally converted into grayscale images through operations such as resizing and cropping. BOSSbase has gone through three versions: 7518 for the 0.9 version in June 2010, 9074 for the 0.92 version, and finally 10000 for the 1.0 version in May 2011.

(3) BOWS-2: BOWS-2 was created by P. Bas et al. It contains 10000 512×512 PGM images. This dataset is taken by 7 different cameras. The creation of this dataset is mainly provided for participants who participate in the BOSS steganalysis contest.

4.3. Predictor Analysis. To verify the effectiveness of threshold selection, this section conducts performance experiments under different threshold settings. The optimal or near-optimal result of the target image is selected as the threshold, and the effectiveness of the threshold is verified on a large image dataset. For ordinary edges and weak edges, the

Table 4: The embedding rate of the test images when $\beta = 4, \alpha = 1, \ldots, 7$.

Image	(α, β)	(2, 4)	(3, 4)	(4, 4)	(5, 4)	(6, 4)	(7, 4)
Lena	MED	—	1.2997	2.7703	2.6693	1.9423	0.9933
	GAP	—	1.6660	2.9584	2.7341	1.9559	0.9950
	Proposed	—	**1.7021**	**3.0398**	**2.7869**	**1.9707**	**0.9958**
Crowd	MED	0.3629	1.8629	2.5719	2.5336	1.9146	0.9938
	GAP	0.3529	1.9132	2.6538	2.5759	1.9266	0.9942
	Proposed	**0.4454**	**2.0404**	**2.7535**	**2.6312**	**1.9391**	**0.9943**
Lake	MED	—	—	1.0276	2.0587	1.8432	0.9919
	GAP	—	—	1.3471	2.2013	1.8567	0.9914
	Proposed	—	—	**1.4239**	**2.2261**	**1.8687**	**0.9918**
Beans	MED	—	**0.3522**	1.5942	2.2255	1.8912	0.9919
	GAP	—	0.1773	1.5036	2.1805	1.8829	0.9917
	Proposed	—	0.2704	**1.6302**	**2.2675**	**1.9060**	**0.9934**

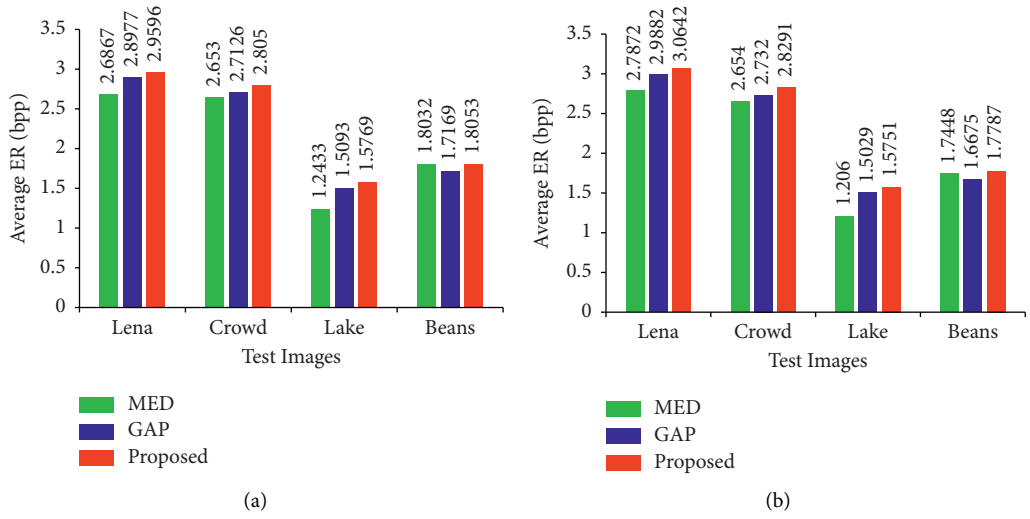


Figure 8: Comparison of the average ER (bpp) of test images between different methods. (a) $\alpha = 4$, $\beta = 2$. (b) $\alpha = 4$, $\beta = 3$.

power of 2 is taken as the threshold selection strategy. The threshold is dynamically adjusted according to the neighborhood complexity of the predicted pixel to achieve local optimization. The neighborhood gradient produces a weak influence when the predicted pixel is in the sharp edge. When it is in the ordinary edge or the soft edge, the effect produced by the neighborhood gradient increases slightly. Table 1 analyzes the embedding performance of Lena under different thresholds.

It can be seen from Table 1 that the predicted pixel on sharp edges has the best case when T_1 is 80. Similarly, the predicted pixel on normal edges has the best case when T_2 is 32. When the predicted pixel is on a weak edge, the threshold T_3 is 8. For diagonal gradient edges, when the threshold T_4 is 80, the solution's performance is optimal.

To verify the predictive performance of the scheme, three gray images of Lena, Man, and Baboon were selected to conduct prediction error experiments. As shown in Figure 7,

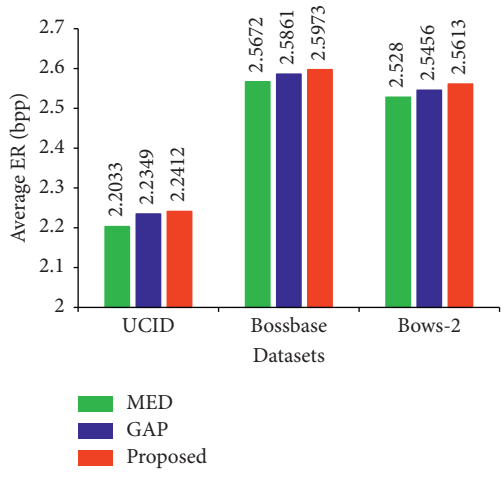


Figure 9: Comparison of the average ER (bpp) of datasets between different methods.

Table 5: Comparison of embedding performance on three datasets.

Datasets	(α, β)	Methods	Best case	Average
UCID	$\alpha = 5, \beta = 2$	MED	2.9759	**2.2683**
		GAP	2.9794	2.2412
		Proposed	**2.9860**	2.2473
	$\alpha = 4, \beta = 2$	MED	3.9349	2.2551
		GAP	3.9364	2.2604
		Proposed	**3.9367**	**2.2621**
	$\alpha = 5, \beta = 3$	MED	2.9793	2.2033
		GAP	2.9834	2.2349
		Proposed	**2.9883**	**2.2412**
BOSSbase	$\alpha = 5, \beta = 2$	MED	2.9882	2.5613
		GAP	2.9882	2.5756
		Proposed	2.9882	**2.5869**
	$\alpha = 4, \beta = 2$	MED	3.9843	2.9332
		GAP	3.9843	2.9218
		Proposed	3.9843	**2.9424**
	$\alpha = 5, \beta = 3$	MED	2.9882	2.5672
		GAP	2.9882	2.5861
		Proposed	2.9882	**2.5973**
BOWS-2	$\alpha = 5, \beta = 2$	MED	2.9882	2.5194
		GAP	2.9882	2.5320
		Proposed	2.9882	**2.5475**
	$\alpha = 4, \beta = 2$	MED	3.9838	2.8311
		GAP	3.9838	2.8144
		Proposed	**3.9841**	**2.8415**
	$\alpha = 5, \beta = 3$	MED	2.9882	2.5280
		GAP	2.9882	2.5456
		Proposed	2.9882	**2.5613**

the x-axis is the prediction error, and the y-axis is the number of pixels under that error.

It can be seen that in the prediction error interval [−12, 2], the number of pixels of this scheme is significantly higher than that of MED, which means that there are more embedded pixels. In contrast, this scheme has significantly fewer non-embeddable pixels than MED. Therefore, this scheme has better prediction performance.

4.4. Comparison and Analysis of Embedding Capacity. To verify the performance of the AGP-RDHEI scheme. This section compares the embedding rate of this scheme with the MED method [17] and the GAP method [20]. As shown Table 2 in Tables 2–4, four test images were selected for ER experiments. The parameter settings of experiments are $\beta = 2, 3, 4$ and $\alpha = 2, 3, \ldots, 7$.

It can be seen that when α is set to a small value, the encrypted image with labels cannot embed secret data. The "/" in Tables 2–4 indicates that the auxiliary information is larger than the reserved room, so the secret data cannot be embedded. Tables 2–4 shows that the maximum embedding rate can be achieved by adjusting the parameter settings. Furthermore, this scheme has better results for images with complex textures. The maximum ER on the four images can reach 3.0642bpp, 2.8291bpp, 1.5751bpp and 1.7787bpp, respectively.

To more intuitively reflect the performance advantages of this solution, Figure 8 visualizes the embedding rate experiment with the parameter set to $\alpha = 4, \beta = 2, 3$.

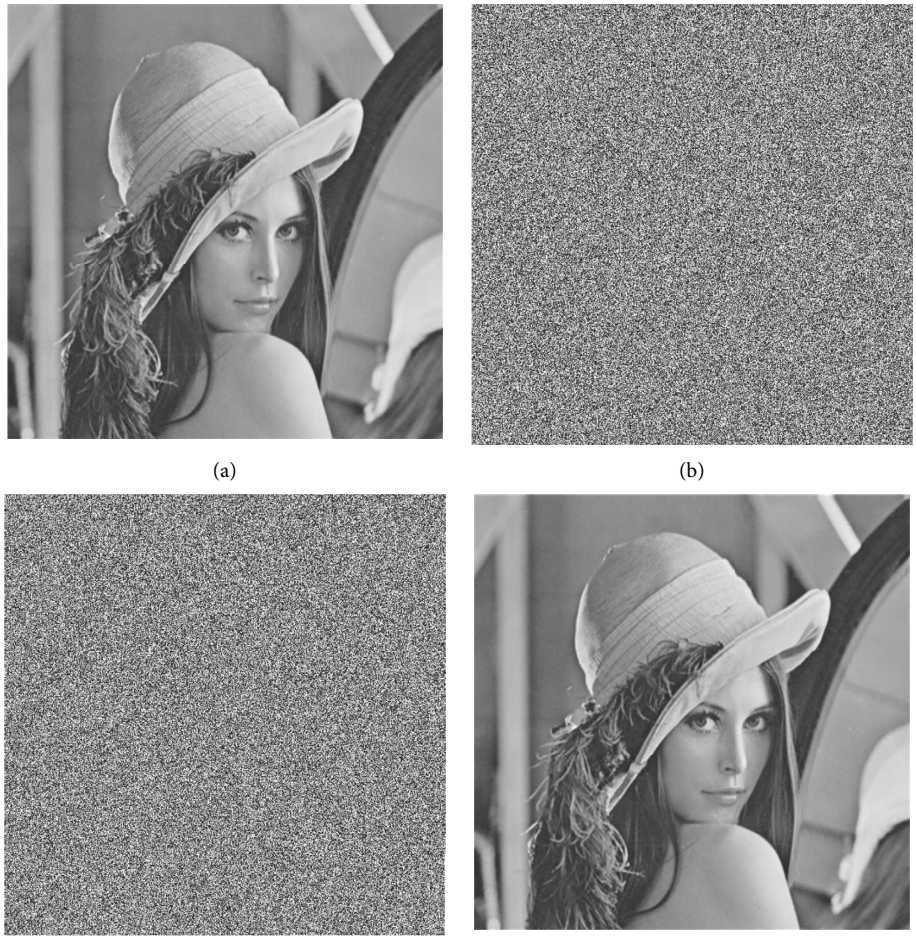
Figure 9 shows the comparative experiments of different schemes on three datasets with the parameter set to $\alpha = 5, \beta = 3$ to reduce the randomness of the selected test images.

The abscissa is the name of the image library, and the ordinate is the average embedding rate in Figure 9. It can be seen that the algorithm in this paper also has promising results on large image datasets. Its average embedding rate is better than literature [20] and significantly better [17].

To further verify the performance of the scheme. As shown in Table 5, we added two sets of experiments with different parameter settings. It can be seen that the results of this scheme under different parameter settings have advantages. It can achieve 2.9424bpp on BOSSbase and 2.8415bpp on BOWS-2.

4.5. Security Analysis. Figure 10 shows the simulation result of Lena, and the sub-figure are the process images of the scheme at different stages. In addition, since the original image and data are encrypted, which can effectively prevent the leakage of image content and data during transmission. It can be seen that it is not easy to detect the content of the original image, e.g., Figures 10(b) and 10(c).

To further verify the security of the scheme, PSNR and SSIM experiments had also been conducted. The smaller the value of SSIM, the greater the distortion of the image. As shown in Table 6 and Tables 6–8, the SSIM value of the encrypted image is almost zero, which effectively protects the security of the image.



(a) (b) (c) (d)

Figure 10: Simulation results of the solution on the Lena image. (a) Original image. (b) Encrypted image. (c) Secret image. (d) Recovered image.

Table 6: PSNR and SSIM of the original images and tagged encrypted images when $\alpha = 5, \beta = 2$.

Encrypted image with label	Lena	Crowd	Lake	Beans
PSNR	9.2231	8.2648	8.2204	7.6936
SSIM	0.0342	0.0318	0.0288	0.0235

Table 7: PSNR and SSIM of the original images and encrypted images when $\alpha = 5, \beta = 2$.

Encrypted image	Lena	Crowd	Lake	Beans
PSNR	9.2255	8.2341	8.2198	7.6256
SSIM	0.0341	0.0301	0.0291	0.0219

Table 8: PSNR and SSIM of the original images and the marked encrypted images when $\alpha = 5, \beta = 2$.

Marked encrypted image	Lena	Crowd	Lake	Beans
PSNR	9.2295	8.2721	8.2327	7.7018
SSIM	0.0365	0.0327	0.0281	0.0254

5. Conclusion

In this paper, we propose a new RDH-EI algorithm based on adaptive gradient prediction, which can be widely applied to various existing schemes. AGP can adaptively adjust the prediction model with the position of the predicted pixel, which improves the predictor's ability to perceive local pixel changes. In addition, the diagonal gradient is introduced when measuring local complexity, effectively enhancing the sensitivity of the predictor to pixel changes. Moreover, we combine the AGP with the PBTL scheme, which reserves more room for embedding data to achieve a high embedding capacity. In the future, we can try to optimize the predictor and labeling scheme to further improve the embedding performance of the scheme.

Data Availability

The datasets UCID, BOSSbase, and BOWS-2 used in this paper can be available from [22–24]. All the experiment results, codes, and data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Acknowledgments

This work was supported by the Soft Science Research Project of Guangdong Digital Government Reform and Construction Expert Committee (No. ZJWKT202204), the National Natural Science Foundation of China under Grant (62002392), and the Natural Science Foundation of Hunan Province under Grant (2020JJ4140 and 2020JJ4141).

References

[1] T. Zheng, Y. Luo, T. Zhou, and Z. Cai, "Towards differential access control and privacy-preserving for secure media data sharing in the cloud," *Journal of Computer Security*, vol. 113, 2022.

[2] X. Zhang, "Reversible data hiding with optimal value transfer," *IEEE Transactions on Multimedia*, vol. 15, no. 2, pp. 316–325, 2013.

[3] C. Wang, Y. Liu, Y. Tong, and J. Wang, "GAN-GLS: generative lyric steganography based on generative adversarial Networks," *Computers, Materials & Continua*, vol. 69, no. 1, pp. 1375–1390, 2021.

[4] Q. Liu, X. Xiang, J. Qin, Y. Tan, and Q. Zhang, "A robust coverless steganography scheme using camouflage image," *IEEE Transactions on Circuits and Systems for Video Technology*, 2022.

[5] Y. Luo, J. Qin, X. Xiang, and Y. Tan, "Coverless image steganography based on multi-object recognition," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 31, no. 7, pp. 2779–2791, 2021.

[6] J. Fridrich, M. Goljan, and R. Du, "Lossless data embedding: new paradigm in digital watermarking," *EURASIP Journal on Applied Signal Processing*, vol. 2002, no. 1, pp. 185–196, 2002.

[7] M. U. Celik, G. Sharma, A. M. Tekalp, and E. Saber, "Lossless generalized-LSB data embedding," *IEEE Transactions on Image Processing*, vol. 14, no. 2, pp. 253–266, 2005.

[8] L. Lixin Luo, Z. Zhenyong Chen, M. Ming Chen, X. Zhang Xiong, and Z. Xiong, "Reversible image watermarking using interpolation technique," *IEEE Transactions on Information Forensics and Security*, vol. 5, no. 1, pp. 187–193, 2010.

[9] X. Xiaolong Li, W. Weiming Zhang, X. Bin Yang, and B. Yang, "A novel reversible data hiding scheme based on two-dimensional difference-histogram modification," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 7, pp. 1091–1100, 2013.

[10] W. Puech, M. Chaumont, and O. Strauss, "A reversible data hiding method for encrypted images," Security, Forensics, Steganography, and Watermarking of Multimedia Contents X," *Proceedings of SPIE*, vol. 6819, 2008.

[11] X. Zhang, "Reversible data hiding in encrypted image," *IEEE Signal Processing Letters*, vol. 18, no. 4, pp. 255–258, 2011.

[12] J. Zhou, W. Sun, L. Dong, X. Liu, O. C. Au, and Y. Y. Tang, "Secure reversible image data hiding over encrypted domain via key modulation," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 26, no. 3, pp. 441–452, 2016.

[13] S. Yi and Y. Zhou, "Separable and reversible data hiding in encrypted images using parametric binary tree labeling," *IEEE Transactions on Multimedia*, vol. 21, no. 1, pp. 51–64, 2019.

[14] P. Puteaux and W. Puech, "An efficient MSB prediction-based method for high-capacity reversible data hiding in encrypted images," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 7, pp. 1670–1681, 2018.

[15] S. Yi and Y. Zhou, "Binary-block embedding for reversible data hiding in encrypted images," *Signal Processing*, vol. 133, pp. 40–51, 2017.

[16] X. Zhang, "Separable reversible data hiding in encrypted image," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 2, pp. 826–832, 2012.

[17] Y. Wu, Y. Xiang, Y. Guo, J. Tang, and Z. Yin, "An improved reversible data hiding in encrypted images using parametric binary tree labeling," *IEEE Transactions on Multimedia*, vol. 22, no. 8, pp. 1929–1938, 2020.

[18] Z. Yin, X. She, J. Tang, and B. Luo, "Reversible data hiding in encrypted images based on pixel prediction and multi-MSB planes rearrangement," *Signal Processing*, vol. 187, no. 2, Article ID 108146, 2021.

[19] Y. Yang, H. He, and F. Chen, "Reversible data hiding of image encryption based on prediction error adaptive coding," *Journal of Computer Research and Development*, vol. 58, no. 6, pp. 1340–1350, 2021.

[20] X. Wu and N. Memon, "Context-based, adaptive, lossless image coding," *IEEE Transactions on Communications*, vol. 45, no. 4, pp. 437–444, 1997.

[21] R. Uyyala and R. Pal, "Reversible data hiding using improved gradient based prediction and adaptive histogram bin shifting," in *Proceedings of the 2020 7th International Conference on Signal Processing and Integrated Networks (SPIN)*, pp. 720–726, Noida, India, February 2020.

[22] G. Schaefer and M. Stich, "Ucid: An uncompressed color image database," vol. 5307, pp. 472–480, 2003, https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.101.8709&rep=rep1&type=pdf.

[23] P. Bas, T. Filler, and T. Pevný, "Break our steganographic system: the ins and outs of organizing BOSS," in *Proceedings of the International Workshop on Information Hiding*, pp. 59–70, Prague, Czech, October 2011.

[24] P. Bas and T. Furon, "Image database of bows-2," *Access*, vol. 20, 2017.

Hindawi
Security and Communication Networks
Volume 2024, Article ID 9823136, 1 page
https://doi.org/10.1155/2024/9823136

Retraction

Retracted: Intelligent Planning of Tourist Routes Based on Cloud Computing and Marching Algorithm

Security and Communication Networks

Received 8 January 2024; Accepted 8 January 2024; Published 9 January 2024

This article has been retracted by Hindawi following an investigation undertaken by the publisher [1]. This investigation has uncovered evidence of one or more of the following indicators of systematic manipulation of the publication process:

(1) Discrepancies in scope

(2) Discrepancies in the description of the research reported

(3) Discrepancies between the availability of data and the research described

(4) Inappropriate citations

(5) Incoherent, meaningless and/or irrelevant content included in the article

(6) Manipulated or compromised peer review

The presence of these indicators undermines our confidence in the integrity of the article's content and we cannot, therefore, vouch for its reliability. Please note that this notice is intended solely to alert readers that the content of this article is unreliable. We have not investigated whether authors were aware of or involved in the systematic manipulation of the publication process.

Wiley and Hindawi regrets that the usual quality checks did not identify these issues before publication and have since put additional measures in place to safeguard research integrity.

We wish to credit our own Research Integrity and Research Publishing teams and anonymous and named external researchers and research integrity experts for contributing to this investigation.

The corresponding author, as the representative of all authors, has been given the opportunity to register their agreement or disagreement to this retraction. We have kept a record of any response received.

References

[1] J. Lu, "Intelligent Planning of Tourist Routes Based on Cloud Computing and Marching Algorithm," *Security and Communication Networks*, vol. 2022, Article ID 8793392, 14 pages, 2022.

Hindawi
Security and Communication Networks
Volume 2022, Article ID 8793392, 14 pages
https://doi.org/10.1155/2022/8793392

Research Article

Intelligent Planning of Tourist Routes Based on Cloud Computing and Marching Algorithm

Junli Lu

Tourism College, Yellow River Conservancy Technical Institute, KaiFeng 475004, China

Correspondence should be addressed to Junli Lu; lujunli@yrcti.edu.cn

Received 17 March 2022; Revised 19 April 2022; Accepted 28 April 2022; Published 23 May 2022

Academic Editor: Fang Liu

In order to improve the effect of modern tourism route planning, this article combines the cloud computing advancement algorithm to construct a tourism route intelligent planning system and combines the current people's tourism needs to carry out intelligent tourism route planning. Based on the fast forward algorithm of the program function equation, this article uses the fast forward algorithm to solve the discrete nonlinear program function equation and directly obtain the cloud computing data. In addition, the self-intersection phenomenon of the wave front must be considered when describing the characteristics of the cloud computing information field by using the process of the equivalent cloud computing information front expanding to the surrounding. Finally, this article constructs the intelligent system structure. The research results show that the intelligent travel route planning system based on cloud computing and marching algorithm proposed in this article can play an important role in modern smart tourism.

1. Introduction

With the development of society, the income of my country's tourism industry has grown rapidly, and a growing theme of popularization of consumption, quality demand, globalization of development, industrial modernization, and internationalization of competition has emerged. As a kind of travel activity including cultural thoughts, cultural travel is not only beneficial to protect and develop various characteristic civilizations, enrich and improve the intrinsic and value of tourism products, but also help to accelerate the transformation and development of regional economic structure. At present, short-term vacations for short-distance travel and long-term vacations for long-distance travel have become popular travel methods. Because of this, the popular tourist attractions will be full every holiday, which will bring people an uncomfortable travel experience and cause overload to the destination. Moreover, with the improvement of the economic level, every family has a family car. In order to better experience travel, self-driving travel and self-guided travel have become the first choice for family travel.

It is time-consuming and labor-intensive to plan a satisfactory travel itinerary only by tourists themselves to search and integrate massive information. However, now the major travel websites only provide a large number of travel products, strategies, and other information, and there is no entrance that can automatically plan travel routes according to the needs of tourists, and there is a lack of such services in the market.

This article combines the cloud computing promotion algorithm to build a travel route intelligent planning system and combines the current people's travel needs to carry out intelligent travel route planning to improve the efficiency of people's travel.

2. Related Work

The team-oriented problem with time dependencies and time windows means given a set of nodes and the travel time between each pair of nodes, where each node is associated with profit, visit time, and time window, the goal is to find the starting node from the starting node. A fixed number of disjoint paths to a destination node, each not exceeding a

given time limit, maximizing the total profit collected by visiting nodes in all paths without violating its time window. Literature [1] proposes two different methods to solve the above problems: (1) use precalculation to get the average travel time between all POI pairs, minus the time-dependent limit; and (2) add time-dependence to the travel time, but this method is based on the simplified assumption of periodic service time, which is not in line with the real urban transportation network. In addition, there are some TOP variants for simulating the tourist route planning problem. Considering more attributes of the problem or multiple constraints on different attributes, literature [2] introduced a heuristic algorithm for the TOP variant, and this algorithm applies two different priority rules when inserting nodes during driving and the algorithm is superior to other heuristic algorithms in terms of solution quality and execution time, and can obtain the optimal solution in the instance solved by the exact algorithm in a relatively short time; Literature [3] formulated a team orientation problem with capacity constraints and time windows, adding constraints on the availability of service nodes in a limited time, and using an integer linear programming solution method to obtain accurate solutions; however, this method is not suitable for real-time applications.

In the tourism field, users usually share their own experiences and comments after a trip, forming a large amount of user-generated content including user comments, photos, check-in data, travel notes, and GPS tracks. The program offers great opportunities [4]. While there may be noise or bias in an individual review or travelogue, taking contributions from a large number of users as a whole can effectively capture the essence of an attraction. Therefore, more and more research studies use technologies such as spatial analysis and data mining to analyze these contents [5], obtain the relevant literatures and historical trajectory information of users, discover the similarity between tourists, and realize the recommendation of travel routes.

As the number of GPS-equipped devices continues to grow, more and more trajectories are continuously generated and shared, changing the way people interact with the web. Based on this trajectory information, some application problems become feasible, such as travel route planning problem, GPS trajectory contains rich information, users can mine the time spent in one location, and the order of visits to different locations. This information can be used to mining popular attractions and general travel routes in a designated area to further improve route recommendation [6]. Literature [7] mines the user's travel habits using the user's historical GPS information and proposes two personalized travel route recommendation algorithms, which can consider the user's personal literature when recommending and improve the degree of personalization of the recommendation results. (1) First, use the collaborative filtering technology to estimate the user's travel behavior frequency, and then, generate a route that conforms to the user's travel habits based on the Naive Bayes model. (2) In the process of route generation, the user's cold start problem is considered, and the average value of the implicit factor vectors of all users is used as the implicit factor vector of users whose travel habits have not been mined; literature [8] integrates the user's travel habits. It can better limit the length of the generated route to meet the user's historical travel habits. The research in the literature [9] did not consider the sequence of the user's travel habits nor the dynamics of the user's travel, and there was a certain deviation in the rationality of the generated route results.

Literature [10] proposed a route reasoning framework based on collective knowledge. First, given a location sequence and time span, popular route information is obtained by aggregating user photo data in a mutually reinforcing manner, and then, the route algorithm constructs a top-k route based on the user-specified query. Literature [11] uses a large collection of geo-tagged photos collected from Panoramio to propose a travel route generation algorithm that takes into account the time spent at each location, the total travel time, and user literatures. Based on the above shortcomings, the literature [12] uses user photo data and adds more contextual information to improve the accuracy of route recommendation results. Literature [13] uses geo-tagged photos to extract the semantic information of tourist attractions while mining user literature information and considers the user's current context information, including spatiotemporal context information, social context information, and weather context information, when making recommendations. Based on the principle that there is a similarity in context when tourists visit scenic spots, Literature [14] proposes a heuristic-based context similarity calculation method, which can accurately describe the context similarity between users, so as to guide the users in the route. Contextual information is added to the recommendation process to provide users with more accurate recommendations.

Literature [15] uses a multisource social media fusion method to integrate fragmented tourism information from multiple aspects to recommend routes to users. Use the method of information entropy to calculate the proportion of a word in a comment, so as to further obtain the proportion of a comment in all comments, remove the invalid comment information of the scenic spots, and take the order of the scenic spots in the travel notes as the user's visit to the scenic spot sequence, and then use the sequence pattern mining algorithm to mine popular routes from user travel notes, and finally obtain the correlation between multisource information based on the similarity between user reviews and pictures of scenic spots and the popular routes mined from travel notes, and realize user route recommendation. In literature [16], a novel framework named ScenicPlanner is proposed for travel route recommendation using geo-tagged images and user check-in information in geo-location-based social networks. Literature [17] applied a heuristic algorithm to iteratively add road segments to maximize the total attractions score while satisfying user-specified constraints (including origin, destination, and total new travel distance); finally, through 3 real-world datasets, the efficiency and effectiveness of the framework are verified.

3. Cloud Computing Marching Algorithm

The program function equation is also known as the travel time field equation. Through this equation, it transitions to the category of geometric cloud computing, which greatly simplifies the elastic wave equation, and the problem of computing the cloud computing information field will be easier to deal with. However, the prerequisite for the transition from wave cloud computing to geometric cloud computing is that the wavelength of cloud computing information tends to zero; that is, it is applicable when the frequency tends to high frequency. Therefore, under the premise of high frequency, the elastic wave equation of longitudinal waves in isotropic medium can be expressed as the following formula [18]:

$$\nabla^2\phi - \frac{1}{v}\frac{\partial^2\phi}{\partial t^2} = 0. \tag{1}$$

Among them, ϕ is the scalar potential function of the longitudinal wave, v is the speed of the longitudinal wave, and t is the time. The general solution form of the above formula is

$$\phi = A\ \exp[-iw(T(x) + t)], \tag{2}$$

where $A = A(x)$ is the amplitude, w is the angular frequency, and T is the isophase surface.

Then, the function ϕ is the Laplace operator, which can be expressed as the following formula:

$$\begin{aligned}\nabla^2\phi = {} & \nabla^2 A\ \exp[-iw(T+t)] \\ & - iw\nabla T\cdot\nabla A\ \exp[-iw(T+t)] \\ & - iw\nabla A\cdot\nabla T\ \exp[-iw(T+t)] \\ & - iwA\nabla^2 T\ \exp[-iw(T+t)] \\ & - w^2 A\nabla T\cdot\nabla T\ \exp[iw(T+t)].\end{aligned} \tag{3}$$

The second derivative of function ϕ with respect to time t is calculated as

$$\frac{\partial^2\phi}{\partial t^2} = -w^2 A\ \exp[-iw(T+t)]. \tag{4}$$

Substituting formula (4) into formula (3), we can get

$$\nabla^2 A - w^2 A|\nabla T|^2 - i\left[2w\nabla A\cdot\nabla T + wA\nabla^2 T\right] = \frac{-Aw^2}{\alpha^2}. \tag{5}$$

The above formula consists of real part and imaginary part. If the real part is taken and both sides of the equal sign are divided by Aw^2 at the same time, it can be obtained [19]:

$$\frac{\nabla^2 A}{Aw^2} - |\nabla T|^2 = -\frac{1}{\alpha^2}. \tag{6}$$

Because the high-frequency assumption ($w \longrightarrow \infty$) has been made, the function equation can be obtained:

$$|\nabla T| = s, \tag{7}$$

where $s = 1/v$ is the slow speed, and $T(x)$ is the travel time of cloud computing information. When T is constant, T represents the wave front.

The fast-advance algorithm systematically constructs the travel time of cloud computing information by adopting a narrowband method. The principle is roughly as shown in Figure 1. In the figure, the black solid point area on the left side is the upwind area, also called the near area, the pink solid point area in the middle is the narrow band area, and the hollow point area on the right side is the downwind area, also called the far area. Points in the upwind area are receiver points, points in the narrowband area are narrowband points, and points in the downwind area are far points.

The implementation process of the fast forward algorithm can be vividly compared to "wind blowing wheat waves," and all the grid points in Figure 1 can be visually regarded as a wheat field, the wind travels from the upwind area to the downwind area, and the wheat waves dance with the wind.

The specific update process of the wavefront expansion of the fast-marching algorithm on the grid nodes is shown in Figure 2, where the black solid point is the receiving point, that is, the known travel time point. As shown in Figure 2(b), according to the basic idea of wavefront expansion of the fast-marching algorithm, the known travel time point is selected to calculate the travel time value of the unknown point in the upwind direction; that is, the travel time value of the four grid nodes near the epicenter is calculated using the upwind difference method. As shown in Figure 2(c), the four pink solid points at the upper, lower, left, and right sides of the hypocenter are regarded as the initial narrowband. It is necessary to select the minimum travel time point in the narrowband and change the attribute of this point from the narrowband point to the accepting point. As shown in Figure 2(d), the travel time of the surrounding points is calculated again with the newly changed travel time point as the accepted point attribute as the center. As shown in Figure 2(e), the minimum travel time point is selected again from all the expanded narrowband points, and its attribute is changed to the acceptance point. As shown in Figure 2(f), the above operations are repeated in sequence until all far points are calculated. In order to clearly and intuitively show the entire implementation process of the fast-marching algorithm, its flow can be summarized in Figure 3.

The program function equation of formula (7) can be expressed as follows in the two-dimensional rectangular coordinate system [20]:

$$\left(\frac{\partial t(x,z)}{\partial x}\right)^2 + \left(\frac{\partial t(x,z)}{\partial z}\right)^2 = s^2(x,z), \tag{8}$$

where t is the cloud computing information travel time and s is the slowness, that is, the reciprocal of the speed. Next, the upper wind difference method is used to replace the partial differential method in the functional equation; that is, the upper wind difference method is used to discretize formula (8), and its discrete expression can be expressed as follows:

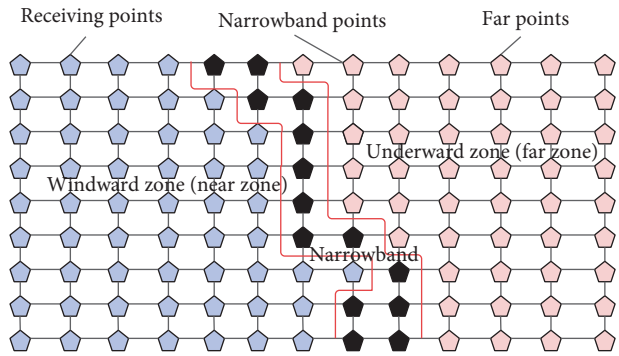


Figure 1: Schematic diagram of FMM implementation.

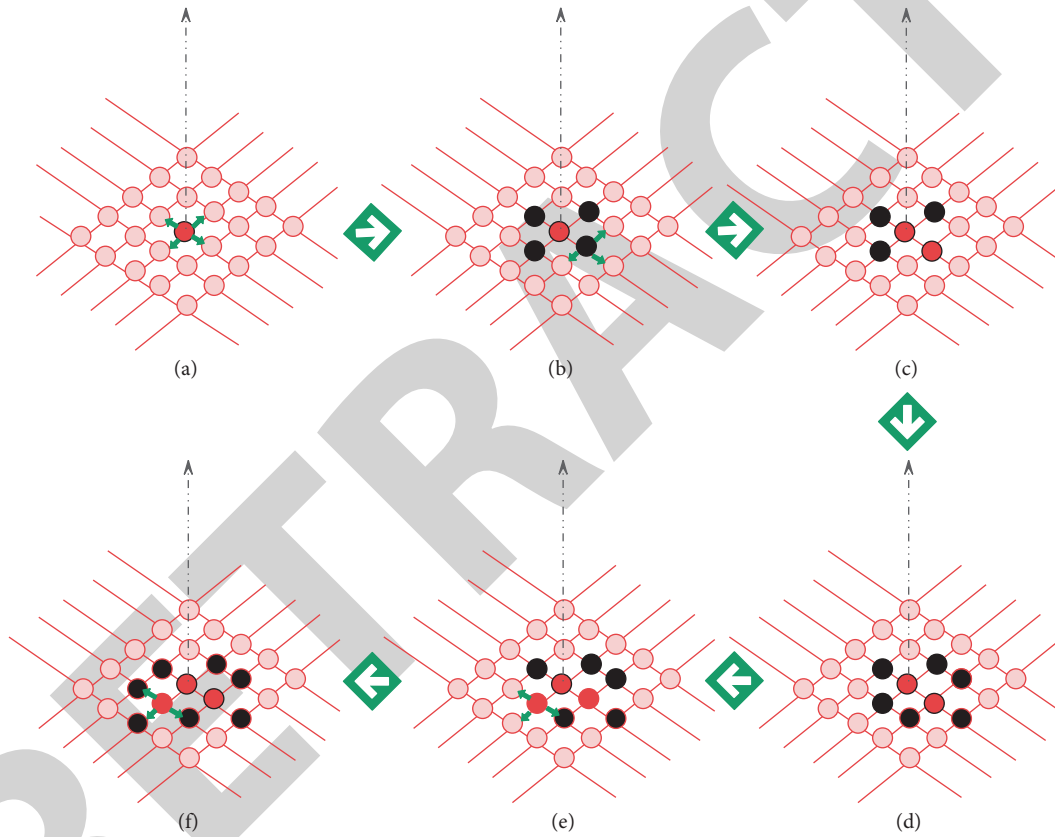


Figure 2: Grid node update process of fast-marching algorithm.

$$|\Delta t| = \begin{bmatrix} \max\left(D_{i,j}^{-x}t, 0\right)^2 + \min\left(D_{i,t}^{+x}, 0\right)^2 + \\ \max\left(D_{i,j}^{-z}t, 0\right)^2 + \min\left(D_{i,t}^{+z}, 0\right)^2 \end{bmatrix}^{1/2} = s_{i,j}. \quad (9)$$

The above formula is further simplified, and its simplified expression is

$$|\Delta t| = \left[\max\left(D_{i,j}^{-x}t, -D_{i,j}^{+x}t, 0\right)^2 + \max\left(D_{i,j}^{-z}t, -D_{i,j}^{+z}t, 0\right)^2\right]^{1/2} = s_{i,j}. \quad (10)$$

In the above formula, $D_{ij}^{+x}t, D_{ij}^{-x}t$ represents the forward and backward difference operators of travel time t in the x-direction at point (i, j), respectively. $D_{ij}^{+z}t, D_{ij}^{-z}t$ represents the forward and backward difference operators in the z-direction at point (i, j), respectively, for travel time t.

It should be pointed out that the first-order upwind difference operator is [21]

$$D_{i,j}^{-x}t = \frac{t_{i,j} - t_{i,j-1}}{\Delta x}, D_{i,j}^{+x}t = \frac{t_{i,j+1} - t_{i,j}}{\Delta x},$$
$$D_{i,j}^{-z}t = \frac{t_{i,j} - t_{i-1,j}}{\Delta z}, D_{ij}^{-z}t = \frac{t_{i+1,j} - t_{i,j}}{\Delta z}. \quad (11)$$

The second-order upwind difference operator is

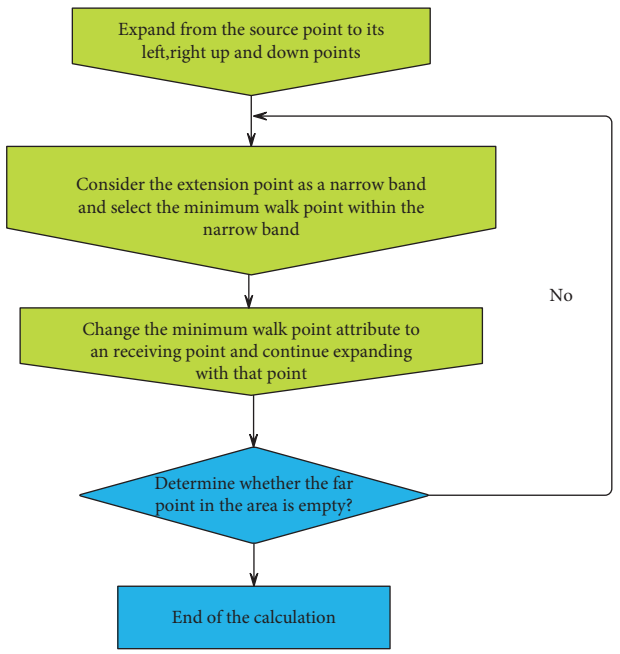


Figure 3: Implementation flowchart of fast-marching algorithm.

$$D_{i,j}^{-x}t = \frac{3t_{i,j} - 4t_{i,j-1} + t_{i,j-2}}{2\Delta x}, D_{ij}^{-x}t = \frac{3t_{i,j} - 4t_{i,j+1} + t_{i,j+2}}{2\Delta x},$$
$$D_{i,j}^{-z}t = \frac{3t_{i,j} - 4t_{i-1,j} + t_{i-2,j}}{2\Delta z}, D_{i,j}^{+z}t = \frac{3t_{i,j} - 4t_{i+1,j} + t_{i+2,j}}{2\Delta z}. \quad (12)$$

The fast-marching algorithm is based on Huygens and Fermat's principles and uses the process of expanding the front of the equivalent cloud computing information. The self-intersection phenomenon of the wave front must be considered when characterizing the cloud computing information field. As shown in Figure 4(a), if the cloud computing information encounters its gradient discontinuity in the medium propagation, there will be a dovetail phenomenon in front of the propagating wave. However, the upwind difference method can still guarantee the stability of solving (10) in this case. It can be seen from Figure 4(b) that the first-arrival wavefront obtained by the solution under the viscous limitation is not continuous. In Figure 4(c), the grey dots are known points (i.e., the travel time of this point is known), and the black dots are the points to be found (i.e., the travel time of this point needs to be obtained). The following will explain in detail how the upwind difference method is a viscous solution at the stable computing node $T_{i,j}$ based on this figure:

In Figure 4(c), we use the known travel time node information around the target point to calculate the travel time value at node $T_{i,j}$ and use the first-order operator to solve (10). In the Q1 and Q2 regions, although the solved travel time value cannot yet fully meet the requirements for the first-order accuracy, its approximate value can be calculated by the two formulas $T_{i,j} = T_{i-1,j} + \delta x \cdot s_{i,j}$ and $T_{i,j} = T_{i+1,j} + \delta x \cdot s_{i,j}$. At the same time, in the Q3 and Q4 regions, the information of the two travel time nodes is known, and the directly solved value fully meets the first-order accuracy requirements. In the Q3 region, the quadratic equation can be expressed as

$$\left(\frac{T_{i+1,j} - T_{i,j}}{\delta x}\right)^2 + \left(\frac{T_{i,j} - T_{i,j-1}}{\delta z}\right)^2 = \left(s_{i,j}\right)^2. \quad (13)$$

By solving the above formula, two solutions can be finally obtained. The larger value of the two is selected as the approximate value of the local wave front travel time. Similarly, the quadratic equation in the Q4 region can be expressed as

$$\left(\frac{T_{i,j} - T_{i-1,j}}{\delta x}\right)^2 + \left(\frac{T_{i,j} - T_{i,j-1}}{\delta z}\right)^2 = \left(s_{i,j}\right)^2. \quad (14)$$

Similarly, in the obtained two solutions, the larger value is used as the approximate value of the travel time in front of the local wave. Finally, the minimum value among these solutions is selected as the final result value of the travel time at point $T_{i,j}$. The fast-marching algorithm uses the upwind difference scheme to discretize the program function equation, which replaces the differential method to discretize the program function equation, and then simplifies the program function expression, and its expression is as follows:

$$|\Delta t| = \left[\max\left(D_{i,j}^{-x}t, -D_{i,j}^{+x}t, 0\right)^2 + \max\left(D_{i,j}^{-z}t, -D_{i,j}^{+z}t, 0\right)^2\right]^{1/2} = s_{i,j}, \quad (15)$$

where $D_{ij}^{-x}t, D_{ij}^{+x}t, D_{ij}^{+z}t, D_{ij}^{-z}t$ represents the forward and backward difference operators of the travel time function t at the grid node (i, j) in the x- and z-directions, respectively. Since the use of difference operators of different orders will affect the accuracy of the fast-marching algorithm and also change the difference calculation formula, it is necessary to deduce the first-order and second-order difference operators and their calculation formulas that are commonly used in this algorithm in detail in this section.

In the two-dimensional case, the travel time function $t(x, z)$ is a function of the spatial position coordinates (x, z), and the first-order partial differential operator of this function in its x- and z-directions can be expressed as $\partial t/\partial x, \partial t/\partial z$, respectively. In the process of discrete operation, the partial differential calculation method can be replaced by the difference method, so that it can be approximated. First, we use a rectangular grid to perform gridding operations in the computing area. The coordinate positions of grid nodes are shown in Figure 5.

Next, we will use the Taylor series expansion method to derive the first- and second-order upwind difference operators. First, a difference operator in the z-direction is established at the target point (i, j), and then, the function t is expanded at the value of the point $(i + 1, j)$ by Taylor series as

$$t_{i+1,j} = t_{i,j} + \left.\frac{\partial t}{\partial z}\right|_{i,j} \Delta z + \frac{1}{2}\left.\frac{\partial^2 t}{\partial z^2}\right|_{i,j} \Delta z^2 + \frac{1}{6}\left.\frac{\partial^3 t}{\partial z^3}\right|_{i,j} \Delta z^3 + \Lambda. \quad (16)$$

In the above formula, Δz is the grid spacing in the z-direction. After sorting it out, we get

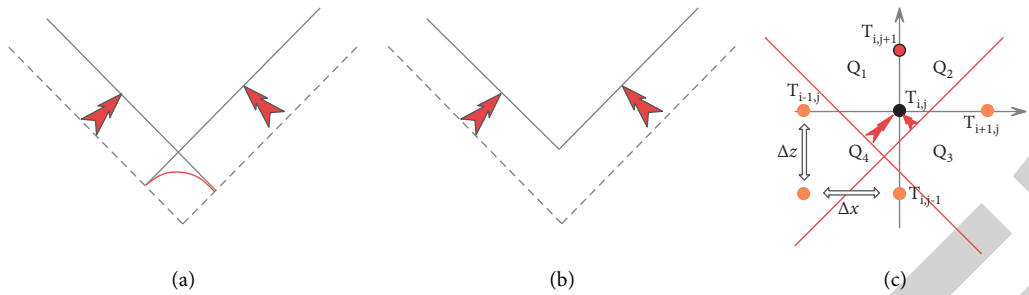


Figure 4: Schematic diagram of wavefront discontinuity and travel time of target point.

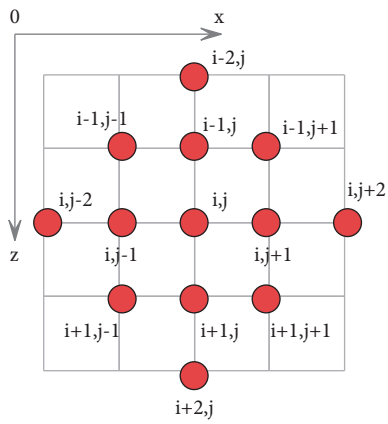


Figure 5: Schematic diagram of grid node location and orientation.

$$\left.\frac{\partial t}{\partial z}\right|_{i,j} = \frac{t_{i+1,j} - t_{i,j}}{\Delta z} + o(\Delta z), \tag{17}$$

where $b\ o(\Delta z)$ is the first-order infinitesimal of the grid spacing Δz. If we ignore it, we get

$$\left.\frac{\partial t}{\partial z}\right|_{i,j} \approx \frac{t_{i+1,j} - t_{i,j}}{\Delta z}. \tag{18}$$

The right-hand term of the above formula is used to replace the backward difference operator corresponding to the partial differential term. At the same time, since the difference operator ignores the first-order infinitesimal $o(\Delta z)$ of the grid spacing Δz when performing approximate calculation, the difference operator is called the first-order backward difference operator. According to the above analysis, the approximate first-order backward difference operator in the x-direction can be derived in the same way:

$$\left.\frac{\partial t}{\partial x}\right|_{i,j} \approx \frac{t_{i,j+1} - t_{i,j}}{\Delta x}. \tag{19}$$

According to the similar operations above, the first-order forward and backward difference operators of the travel time $T(i, j)$ of the target point in the x- and z-directions can be obtained:

$$D_{i,j}^{-x}t = \frac{t_{i,j} - t_{i,j-1}}{\Delta x}, D_{i,j}^{+x}t = \frac{t_{i,j+1} - t_{i,j}}{\Delta x},$$
$$D_{i,j}^{-z}t = \frac{t_{i,j} - t_{i-1,j}}{\Delta z}, D_{ij}^{-z}t = \frac{t_{i+1,j} - t_{i,j}}{\Delta z}. \tag{20}$$

The second-order difference operator of the fast-marching algorithm will be derived below. Similarly, we first establish a difference operator in the z-direction at the target point (i, j). Then, the function t is expanded by Taylor series at the value of point $(i+1, j)$ as

$$t_{i+2,j} = t_{i,j} + \left.\frac{\partial t}{\partial z}\right|_{i,j} 2\Delta z + \frac{1}{2}\left.\frac{\partial^2 t}{\partial z^2}\right|_{i,j} 4\Delta z^2 + \frac{1}{6}\left.\frac{\partial^3 t}{\partial z^3}\right|_{i,j} 8\Delta z^3 + \Lambda. \tag{21}$$

Then, through first-order Taylor series expansion (16) and first-order difference operator (20) deduced above, formula (21) can be simplified as

$$\left.\frac{\partial t}{\partial z}\right|_{i,j} = -\frac{3t_{i,j} - 4t_{i+1,j} + t_{i+2,j}}{2\Delta z} + o\left(\Delta z^2\right), \tag{22}$$

where $o(\Delta z^2)$ is the second-order infinitesimal of the grid spacing Δz. If we ignore it, we get

$$\left.\frac{\partial t}{\partial z}\right|_{i,j} \approx -\frac{3t_{i,j} - 4t_{i+1,j} + t_{i+2,j}}{2\Delta z}. \tag{23}$$

The right-hand term of formula (23) is the backward difference operator used to replace the partial differential term. At the same time, because the difference operator ignores the second-order infinitesimal $o(\Delta z^2)$ of the grid spacing Δz when it performs approximate calculation, so the difference operator is called the second-order backward difference operator. According to the above analysis, the approximate second-order backward difference operator in the x-direction can be derived in the same way:

$$\left.\frac{\partial t}{\partial x}\right|_{i,j} \approx -\frac{3t_{i,j} - 4t_{i,j+1} + t_{i,j+2}}{2\Delta x}. \tag{24}$$

According to the similar operations above, the first-order forward and backward difference operators of the travel time $T(i, j)$ of the target point in the x- and z-directions can be obtained:

$$D_{i,j}^{-x}t = \frac{3t_{i,j} - 4t_{i,j-1} + t_{i,j-2}}{2\Delta x}, D_{ij}^{-x}t = \frac{3t_{i,j} - 4t_{i,j+1} + t_{i,j+2}}{2\Delta x},$$
$$D_{i,j}^{-z}t = \frac{3t_{i,j} - 4t_{i-1,j} + t_{i-2,j}}{2\Delta z}, D_{i,j}^{+z}t = \frac{3t_{i,j} - 4t_{i+1,j} + t_{i+2,j}}{2\Delta z}. \tag{25}$$

Formulas (20) and (25) give the first-order and second-order upwind difference operators corresponding to the

partial differential term, respectively. Using the same method as above, the difference operator of any order in the upwind difference method can be derived.

Since the equations of the viscous solutions constructed by the difference operators of different orders will have different precisions and calculation formulas, we substitute the derived first-order and second-order difference operators into the simplified functional equation; that is, the expression is $|\Delta t| = [\max(D_{i,j}^{-x}t, -D_{i,j}^{+x}t, 0)^2 + \max(D_{i,j}^{-z}t, -D_{i,j}^{+z}t, 0)^2]^{1/2} = s_{i,j}$. In the equation, the first-order and second-order difference calculation formulas of the travel time of the target point are continuously deduced.

Then, for the first-order difference calculation formula, we take (i, j), $(i, j+1)$, $(i+1, j)$ as an example, and the position coordinates of these points are shown in the figure. We assume that the travel time value of the point $(i, j+1)$, $(i+1, j)$ is known, the travel time value at the target point (i, j) is the target to be calculated, and the slowness values corresponding to these three points are set as $s(i, j), s(i, j+1), s(i+1, j)$, respectively. Then, the travel time value at the target point (i, j) satisfies the first-order backward difference scheme in the x- and z-directions, and its expression is

$$\begin{aligned}\frac{\partial t}{\partial x} &= \frac{t_{i,j+!} - t_{i,j}}{\Delta x},\\ \frac{\partial t}{\partial z} &= \frac{t_{i+1} - t_{i,j}}{\Delta z}.\end{aligned} \tag{26}$$

Substituting formula (26) into the simplified $|\Delta t| = [\max(D_{i,j}^{-x}t, -D_{i,j}^{+x}t, 0)^2 + \max(D_{i,j}^{-z}t, -D_{i,j}^{+z}t, 0)^2]^{1/2} = s_{i,j}$, the quadratic equation satisfied by the target point $t(i, j)$ is

$$\left(\frac{t_{i,j+1} - t_{i,j}}{\Delta x}\right)^2 + \left(\frac{t_{i+1,j} - t_{i,j}}{\Delta z}\right)^2 = s_{i,j}^2. \tag{27}$$

We set the division grid spacing to be $h = \Delta x = \Delta z$ (a square grid is used for illustration here), then the expression is

$$\left(t_{i,j+1} - t_{i,j}\right)^2 + \left(t_{i+1,j} - t_{i,j}\right)^2 = \left(s_{i,j}h\right)^2. \tag{28}$$

By arranging formula (28), we get

$$2t_{i,j}^2 + 2\left(t_{i+1,j} + t_{i,j+1}\right)t_{i,j} + \left(t_{i+1,j}^2 + t_{i,j+1}^2 + \left(s_{i,j|+1}h\right)^2\right) = 0. \tag{29}$$

We solve (29) and select the larger value among the two calculated solutions, which is the first-order difference calculation formula of the travel time value at the target point (i, j), and the solution expression is

$$t_{i,j} = \frac{t_{i+1,j} + t_{i,j+1} + \sqrt{2\left(s_{i,j}h\right)^2 - \left(t_{i+1,j} - t_{i,j+1}\right)^2}}{2}. \tag{30}$$

In the same way, the travel time calculation formula of the x- and z-direction nodes in the four direction nodes of the target point (i, j) can be calculated. To sum up, the first-order difference calculation formula of the travel time can be calculated by using the travel time values of the target point (i, j) at the node $(i \pm 1, j)$, $(i, j \pm 1)$ in the four directions of up, down, left, and right:

$$\begin{cases} t_{i,j} = \dfrac{t_{i\pm1,j} + t_{i,j\pm1} + \sqrt{2\left(s_{i,j}h\right)^2 - \left(t_{i\pm1,j} - t_{i,j+1}\right)^2}}{2}, \\ t_{i,j} = t_{i\pm1,j} + s_{i,j}h \\ t_{i,j} = t_{i,j\pm1} + s_{i,j}h \end{cases} \tag{31}$$

Special emphasis needs to be made here for the above formula. The travel time value of the target point (i, j) cannot be calculated and updated by the travel time value of the four nodes at the same time. The basic principle of narrowband expansion must be followed; that is, according to the direction of narrowband propagation expansion, the formula that satisfies the new law in equation (31) is selected to calculate the travel time value of the target point. Moreover, the minimum travel time point is selected in the obtained multivalued solution, which is the true travel time value at the target point (i, j). In addition, it should be noted that the average value of node slowness can be used as the final slowness value in formula (31), and this operation detail can further ensure the calculation accuracy and its stability.

Similarly, for its second-order difference calculation formula, five points, namely, (i, j), $(i, j+1)$, $(i, j+2)$, $(i+1, j)$, $(i+2, j)$, are selected for illustration. The position coordinates of the five points in the Cartesian coordinate system. We assume that the travel time value at node $(i, j+1)$, $(i, j+2)$, $(i+1, j)$, $(i+2, j)$ is known, the travel time value at the target point (i, j) is the target to be calculated, and the slowness values corresponding to these five points are, respectively, set as $s(i, j), s(i, j+1), s(i, j+2)$, $s(i+1, j), s(i+2, j)$. Then, the travel time value at the target point (i, j) satisfies the second-order backward difference scheme in the x- and z-directions, and its expression is

$$\begin{aligned}\frac{\partial t}{\partial x} &= -\frac{3t_{i,j} - 4t_{i,j+1} + t_{i,j+2}}{2\Delta x},\\ \frac{\partial t}{\partial z} &= -\frac{3t_{i,j} - 4t_{i+1,j} + t_{i+2,j}}{2\Delta z}.\end{aligned} \tag{32}$$

Substituting formula (32) into the simplified $|\Delta t| = [\max(D_{i,j}^{-x}t, -D_{i,j}^{+x}t, 0)^2 + \max(D_{i,j}^{-z}t, -D_{i,j}^{+z}t, 0)^2]^{1/2} = s_{i,j}$, the quadratic equation satisfied by the target point $t(i, j)$ is

$$\left(-\frac{3t_{i,j} - 4t_{i,j+1} + t_{i,j+2}}{2\Delta x}\right)^2 + \left(-\frac{3t_{i,j} - 4t_{i+1,j} + t_{i+2,j}}{2\Delta z}\right)^2 = s_{i,j}^2. \tag{33}$$

The derivation process of the same-order calculation formula is similar. By solving formula (33) and selecting the solution with the larger value among the obtained multiple solutions, this value is the second-order difference calculation formula of the travel time value at the target point (i, j). The expression for its solution is

$$t_{i,j} = \frac{\left(4t_{i+1,j} - t_{i+2,j}\right) + \left(4t_{i,j+1} - t_{i,j+2}\right) + \sqrt{8\left(s_{i,j}h\right)^2 - \left(\left(4t_{i+1,j} - t_{i+2,j}\right) - \left(4t_{i,j+1} - t_{i,j+2}\right)\right)^2}}{6}. \tag{34}$$

Among the above five points, the travel time at point (i, j) satisfies the second-order difference in one of the x- and z-directions. At the same time, when the first-order difference is satisfied in the other direction, the travel time calculation formula at the point (i, j) is different. When the point (i, j) satisfies the second-order difference in the x-direction and the first-order difference in the z-direction, the calculation formula of the mixed-order difference when walking at the point (i, j) is

$$t_{i,j} = \frac{3\left(4t_{i,j+1} - t_{i,j+2}\right) + 4t_{i+1,j} + 2\sqrt{13\left(s_{i,j}h\right)^2 - \left(4t_{i,j+1} - t_{i,j+2} - 3t_{i+1,j}\right)^2}}{13}. \tag{35}$$

Similarly, when the point (i, j) satisfies the second-order difference in the z-direction and the first-order difference in the x-direction, then the travel time mixed-order difference calculation formula at the point (i, j) is

$$t_{i,j} = \frac{3\left(4t_{i+1,j} - t_{i+2,j}\right) + 4t_{i,j+1} + 2\sqrt{13\left(s_{i,j}h\right)^2 - \left(4t_{i+1,j} - t_{i+2,j} - 3t_{i,j+1}\right)^2}}{13}. \tag{36}$$

Similarly, the travel time calculation formula of the x- and z-direction nodes among the eight direction points around the target point (i, j) can also be calculated. To sum up, the second-order difference calculation formula of the travel time can be calculated by using the travel time values at the node $(i, j \pm 1)$, $(i, j \pm 2)$, $(i \pm 1, j)$, $(i \pm 2, j)$ in the eight directions around the target point (i, j) as formula (37).

The fast-marching algorithm used in the final numerical simulation of this article is all based on the second-order difference calculation formula:

$$\begin{cases} t_{i,j} = \dfrac{\left(4t_{i\pm1,j} - t_{i\pm2,j}\right) + \left(4t_{i,j\pm1} - t_{i,j\pm2}\right) + \sqrt{8\left(s_{i,j}h\right)^2 - \left(\left(4t_{i\pm1,j} - t_{i\pm2,j}\right) - \left(4t_{i,j\pm1} - t_{i,j\pm2}\right)\right)^2}}{6} \\ t_{i,j} = \dfrac{3\left(4t_{i,j\pm1} - t_{i,j\pm2}\right) + 4t_{i\pm1,j} + 2\sqrt{13\left(s_{i,j}h\right)^2 - \left(4t_{i,j\pm1} - t_{i,j\pm2} - 3t_{i+1,j}\right)^2}}{13}, \\ t_{i,j} = \dfrac{3\left(4t_{i\pm1,j} - t_{i\pm2,j}\right) + 4t_{i,j\pm1} + 2\sqrt{13\left(s_{i,j}h\right)^2 - \left(4t_{i\pm1,j} - t_{i\pm2,j} - 3t_{i,j+1}\right)^2}}{13}, \\ t_{i,j} = \dfrac{t_{i\pm1,j} - t_{i,j\pm1} + \sqrt{2\left(s_{i,j}h\right)^2 - \left(t_{i\pm1,j} - t_{i,j\pm1}\right)^2}}{2}, \\ t_{i,j} = t_{i+1,j} + s_{i,j}h, \\ t_{i,j} = t_{i,j\pm1} + s_{i,j}h. \end{cases} \tag{37}$$

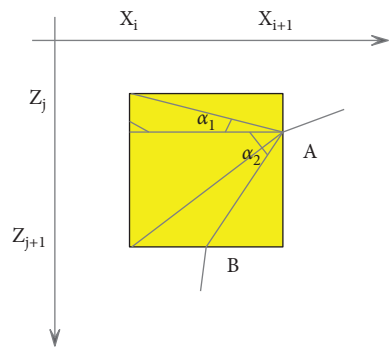


Figure 6: Travel time field ray path.

The reverse tracing method calculates the ray path according to the characteristic that the cloud computing information always propagates in the direction perpendicular to its wave front, that is, parallel to the direction of the maximum gradient of its travel time field. The calculation idea of this method is to take the position coordinate of the receiving point as the starting point and calculate the ray path in the reverse direction along the gradient ∇T direction of the travel time field until it ends at the source point.

If it is assumed that the travel time value at the node (x_i, z_i) is $t_{i,j}$, and the coordinates of the node position are shown in Figure 6, then the derivative of $t_{i,j}$ in the x- and z-directions can be obtained by the central difference scheme, which is approximately as follows:

$$\begin{cases} \dfrac{\partial t}{\partial x} \approx \dfrac{\left[\left(t_{i+1,j} + t_{i+1,j+1}\right) - \left(t_{i,j} + t_{i,j+1}\right)\right]}{2h}, \\ \dfrac{\partial t}{\partial z} \approx \dfrac{\left[\left(t_{i,j+1} + t_{i+1,j+1}\right) - \left(t_{i,j} + t_{i+1,j}\right)\right]}{2h}. \end{cases} \tag{38}$$

Among them, h is the grid spacing, so the incident angle of the ray at point (x_i, z_i) can be calculated, and its expression is

$$\theta_k = \tanh^{-1}\left[\left(\partial t/\partial z\right)/\left(\partial t/\partial x\right)\right] + \pi. \tag{39}$$

The above formula only expresses the case where the target node is on the grid. However, when the target point is not on the grid, such as point A in Figure 6, the ray position at the next node must be determined by calculating the two angles a_1, a_2 in the graph. The formulas for calculating the two angles are as follows:

$$\begin{cases} a_1 \approx \tanh^{-1}\left[\left(z_{j+1} - z_a\right)/h\right] \\ a_2 \approx \tanh^{-1}\left[\left(z_a - z_j\right)/h\right] \end{cases}, \tag{40}$$

where z_a represents the value of point A in the z-direction.

Next, the search method will be introduced. According to Fermat's principle, it can be known that cloud computing information always propagates along its shortest time-consuming path in the underground medium. If the ray path L_{SR} from the source point S to the receiving point R is set to be the shortest path and the travel time corresponding to L_{SR} is $t(S, R)$, and the point P is any point on L_{SR}, then the following formula holds

$$t(S, P) + t(P, R) = t(S, R). \tag{41}$$

The above equation is the travel time equation, and the search method is based on the travel time equation to find the minimum travel time path of the ray in a certain search area. For the convenience of expression, we set the search area as a function $D(P, n)$, where P in the function is the reference point in the search area, and n is the radius of the search area. Then, we take the source point R as the starting point to find a point A_1 in $D(P, n)$ that satisfies formula (39):

$$t(S, A_1) + t(A_1, R) - t(S, R) = \min_{p \in D(R,n)} \{t(S, P) + t(P, R) - t(S, R)\}. \tag{42}$$

According to the above method, a section of path $L_{A_1 R}$ is found, and then, the above operation is continued from point A_1 as the starting point until the last point is at the source point S, and the calculation is ended. By connecting the calculated multi-section paths, the entire real ray path is obtained.

4. Intelligent Planning of Travel Route Based on Cloud Computing Marching Algorithm

In Figure 7, the main feature is that an IaaS architecture of tourism cloud is laid out according to each user group of tourism, through which the virtualization of tourism resources can be realized. At the same time, the structure includes a schematic structure of the composition of the IaaS of the travel cloud, and a cloud computing model such as Amazon EC2 can also be rented according to the requirements of the travel cloud computing. Moreover, the energy consumption control mode of the travel cloud is also designed and laid out in this structure, as shown in Figure 8.

After constructing the above model system structure, the tourism data processing and tourism route intelligent planning of the system model are analyzed, and the results shown in the following Tables 1 and 2 are obtained.

It can be seen from the above experimental research that the intelligent planning system of travel route based on cloud computing and marching algorithm proposed in this article can play an important role in modern smart tourism.

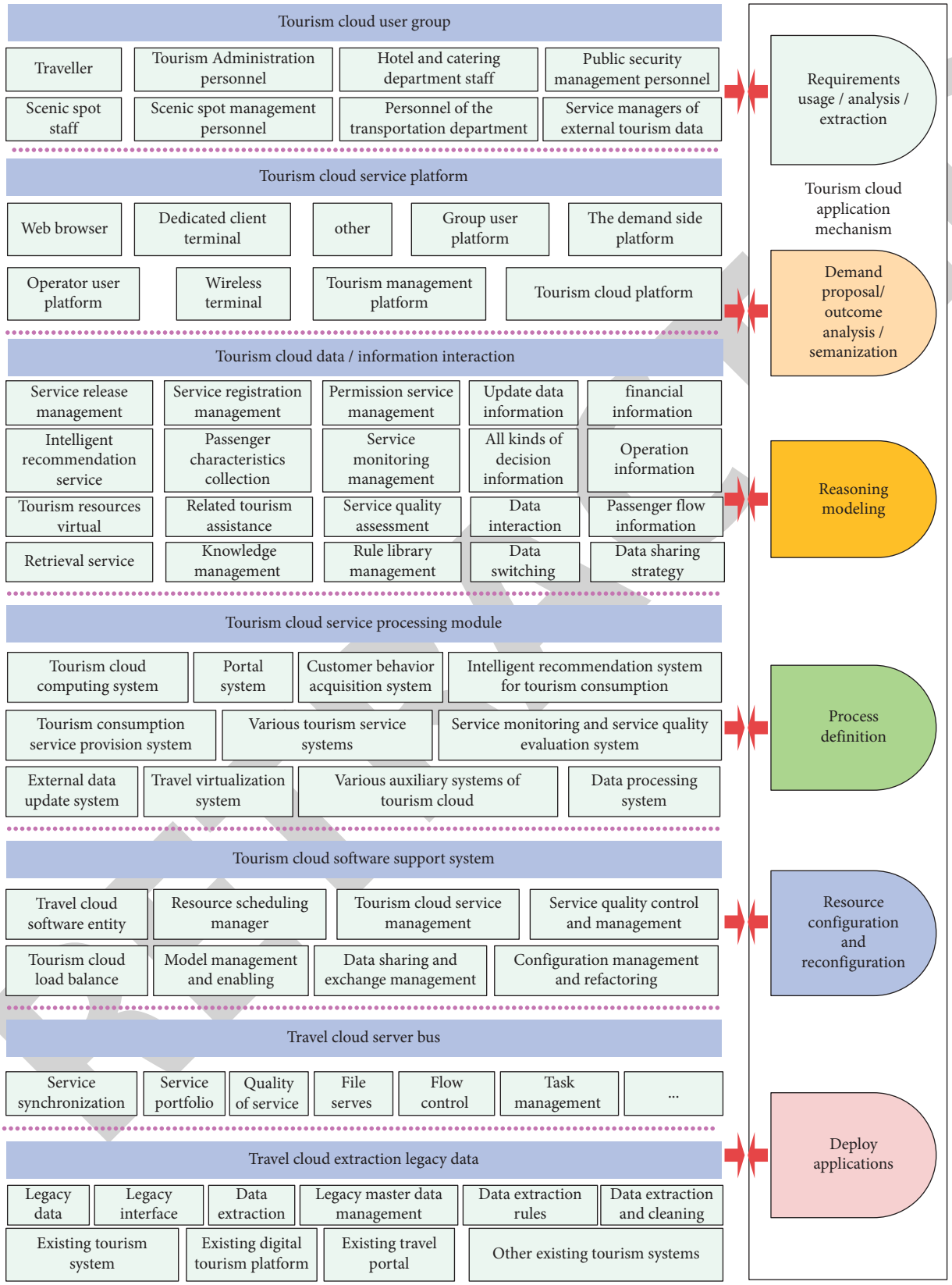


Figure 7: Architecture of tourism cloud technology.

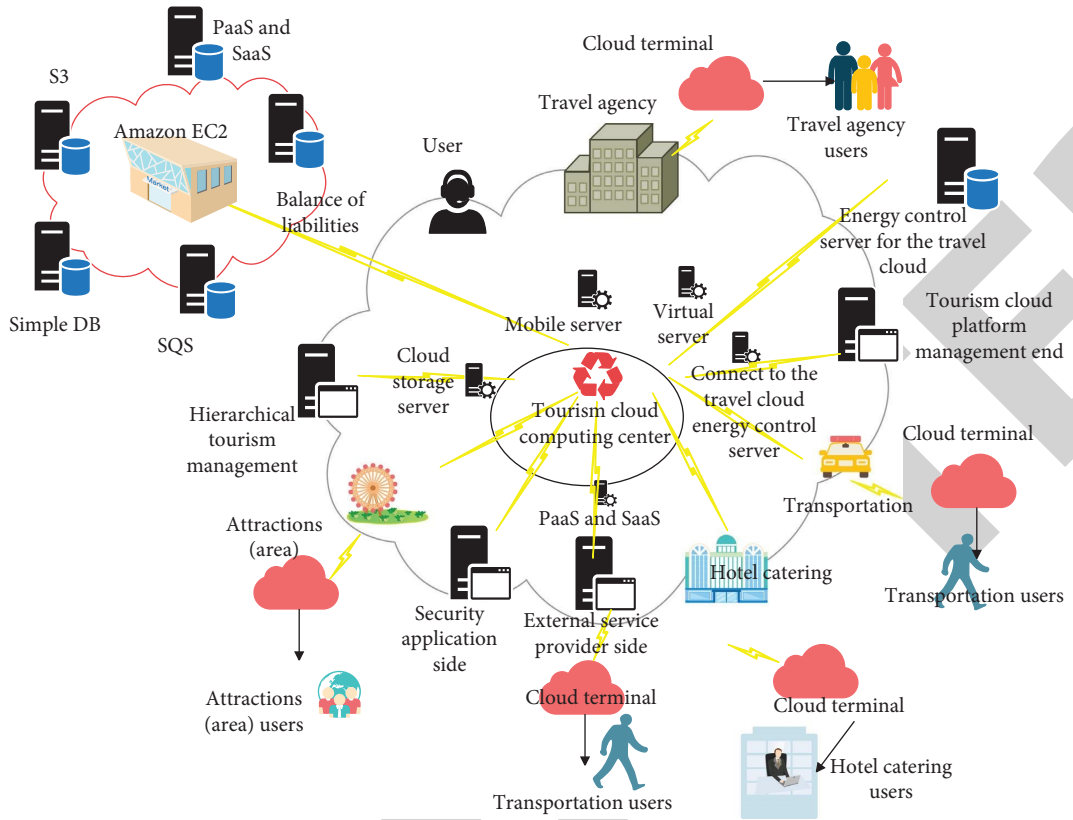


Figure 8: The structure of the tourism cloud system.

Table 1: Evaluation of tourism data cloud computing processing effect.

Num	Data processing
1	93.03
2	91.80
3	93.23
4	88.74
5	89.39
6	87.02
7	89.81
8	92.08
9	91.14
10	87.47
11	90.36
12	89.20
13	92.40
14	87.86
15	89.87
16	87.45
17	92.78
18	90.80
19	90.44
20	90.69
21	93.14
22	93.38
23	93.22
24	91.23
25	88.41
26	89.92
27	87.96

Table 1: Continued.

Num	Data processing
28	90.18
29	91.16
30	90.46
31	93.36
32	88.41
33	90.41
34	90.50
35	92.09
36	88.41
37	90.69
38	90.05
39	88.52
40	89.82
41	92.27
42	92.36
43	87.60
44	89.56
45	92.85
46	87.15
47	88.39
48	92.81
49	90.65
50	87.69
51	93.06
52	93.06
53	91.63
54	90.90
55	93.71
56	92.45
57	92.44
58	92.72
59	93.29
60	93.56
61	92.97
62	92.12
63	93.17
64	89.02
65	93.10
66	90.73

Table 2: Evaluation of the effect of intelligent planning of tourist routes.

Num	Travel plan
1	90.59
2	85.48
3	90.93
4	85.25
5	87.28
6	90.44
7	89.18
8	88.05
9	89.09
10	84.23
11	85.96
12	86.91
13	86.02
14	83.53
15	86.45

Table 2: Continued.

Num	Travel plan
16	89.71
17	82.61
18	85.20
19	89.23
20	88.41
21	90.25
22	88.92
23	86.84
24	85.49
25	90.04
26	83.66
27	83.65
28	87.88
29	90.91
30	85.31
31	84.57
32	86.08
33	89.62
34	86.70
35	85.95
36	85.36
37	84.82
38	86.76
39	88.67
40	90.66
41	89.78
42	90.61
43	88.83
44	87.82
45	85.81
46	88.85
47	87.87
48	89.88
49	82.17
50	88.07
51	90.22
52	86.14
53	88.96
54	85.61
55	83.99
56	85.24
57	83.44
58	82.04
59	84.88
60	85.30
61	87.06
62	86.14
63	88.18
64	85.89
65	89.03
66	86.47

5. Conclusion

At present, there are many tourists in the travel community who have posted help posts about travel itinerary arrangements. They have some basic requirements for travel itinerary planning, such as destination, travel time, number of days to visit, group of visitors, and itinerary preferences. In fact, these needs can be met through intelligent search or personalized recommendation technology. However, in order to plan the best travel route for tourists, it is necessary to consider the user's preference, travel distance, time and cost, etc., which is a relatively complex problem. This article combines cloud computing and marching algorithm to construct an intelligent planning system for travel routes and analyzes the intelligent planning of travel routes based on the current people's travel needs. The experimental results show

Hindawi
Security and Communication Networks
Volume 2024, Article ID 9852914, 1 page
https://doi.org/10.1155/2024/9852914

Retraction

Retracted: Prediction of High-Frequency Economic Data Based on Stochastic Fluctuation Model

Security and Communication Networks

Received 8 January 2024; Accepted 8 January 2024; Published 9 January 2024

This article has been retracted by Hindawi following an investigation undertaken by the publisher [1]. This investigation has uncovered evidence of one or more of the following indicators of systematic manipulation of the publication process:

(1) Discrepancies in scope

(2) Discrepancies in the description of the research reported

(3) Discrepancies between the availability of data and the research described

(4) Inappropriate citations

(5) Incoherent, meaningless and/or irrelevant content included in the article

(6) Manipulated or compromised peer review

The presence of these indicators undermines our confidence in the integrity of the article's content and we cannot, therefore, vouch for its reliability. Please note that this notice is intended solely to alert readers that the content of this article is unreliable. We have not investigated whether authors were aware of or involved in the systematic manipulation of the publication process.

Wiley and Hindawi regrets that the usual quality checks did not identify these issues before publication and have since put additional measures in place to safeguard research integrity.

We wish to credit our own Research Integrity and Research Publishing teams and anonymous and named external researchers and research integrity experts for contributing to this investigation.

The corresponding author, as the representative of all authors, has been given the opportunity to register their agreement or disagreement to this retraction. We have kept a record of any response received.

References

[1] X. Zhang, T. Qi, and D.-J. Kim, "Prediction of High-Frequency Economic Data Based on Stochastic Fluctuation Model," *Security and Communication Networks*, vol. 2022, Article ID 4109563, 13 pages, 2022.

Hindawi
Security and Communication Networks
Volume 2022, Article ID 4109563, 13 pages
https://doi.org/10.1155/2022/4109563

Research Article

Prediction of High-Frequency Economic Data Based on Stochastic Fluctuation Model

Xiaoyang Zhang,[1,2] Tianxiang Qi,[3] and Dong-Joo Kim[4]

[1]*Department of Social Economy and Management, Graduate School, Woosuk University, Wanju-gun 55338, Republic of Korea*
[2]*Handan University, Hebei, Handan 056001, China*
[3]*Department of Social Economy and Management, Graduate School, Woosuk University, Wanju-gun 55338, Republic of Korea*
[4]*Department of Rehabilitation Studies, Woosuk University, Wanju-gun 55338, Republic of Korea*

Correspondence should be addressed to Tianxiang Qi; qitianxiang@xafy.edu.cn

Received 14 March 2022; Revised 8 April 2022; Accepted 21 April 2022; Published 19 May 2022

Academic Editor: Fang Liu

In order to improve the effect of economic high-frequency data analysis, this paper combines the stochastic fluctuation model to carry out the forecast analysis of economic high-frequency data. Moreover, this paper uses the spider web model for data processing and makes a preliminary judgment on the extent to which futures/stock prices lead the spot through error correction model, impulse response, and variance decomposition. Furthermore, this paper studies the contribution of futures/stock price changes to the effective price through the common factor model so as to obtain its price discovery efficiency. In addition, this paper judges the efficiency of price discovery by studying the contribution of futures/stock price changes to the effective price. Finally, based on the research idea of futures/stock price discovery efficiency, an intelligent data analysis model is constructed. The experimental study shows that the economic high-frequency data prediction model based on the stochastic fluctuation model proposed in this paper has a good effect on the analysis and prediction of economic high-frequency data.

1. Introduction

The focus of the research on the market microstructure is the influence of the market trading system on the price formation process, so it is necessary to carefully examine the trading data and order book data generated during the trading day. This type of data is called high-frequency data or intraday data. Generally speaking, the information in the financial market is a continuous process of affecting price changes, and the discrete model will inevitably lead to the loss of information. The lower the data frequency is, the more information is lost.

Risk and reward are what people care about most when investing in assets. After a comprehensive analysis of risk and return, investors choose suitable financial assets for rational investment according to their affordability. Therefore, accurate and reasonable risk aversion has become the focus of research [1]. Theorists have always used the volatility of assets as a measure of risk. Under the assumption of satisfying the efficient market environment, when investors choose financial products, they have certain expectations about their price trends and future income. However, some uncertain market factors often cause the real price trend to deviate from this expectation, which leads to market risks and makes the price deviate from investors' expectations [2]. Volatility is a measure of risk, and the magnitude of volatility can express the uncertainty of asset prices. The greater the volatility, the greater the deviation between the expected return and the actual return. Therefore, there is a greater investment risk. The smaller the volatility, the smaller the deviation between the expected return of the asset and the actual return, and the smaller the corresponding risk [3].

There are two very classical methods for measuring fluctuation in time series analysis: one is Engle's ARCH model and its extended form, and the other is Taylor's SV

model and its extended form. These two kinds of methods have remarkable effect on low-frequency time series data, and their application is very successful. Due to the successful performance of ARCH model and SV model in the field of low-frequency financial time series modeling, people will naturally think: can ARCH model and SV model be directly applied to high-frequency time series? If not, we can modify and improve these two models. Can we apply them to high-frequency field? Andersen and Bollerslev (1997), the research pioneers in the field of high-frequency data volatility measurement in the stock market, have conducted a large number of empirical studies. Afterwards, it was found that the ARCH model and the SV model were unable to explain the driving factors of fluctuations and could not explain the reasons for continuous fluctuations. They could describe some features of high-frequency time series to a certain extent, but their accuracy was not high and the effect was unsatisfactory. Therefore, it is necessary to consider the statistical characteristics of high-frequency time series that are different from low-frequency time series and build a reasonable model for them according to the statistical characteristics.

In order to improve the effect of high-frequency economic data analysis, this paper combines the stochastic fluctuation model to carry out the prediction and analysis of high-frequency economic data and constructs an intelligent economic data analysis model to improve the effect of subsequent economic data analysis.

2. Related Work

With the continuous improvement of data collection and processing capabilities and the increasing availability of high-frequency data, the research on the realized volatility measurement based on high-frequency financial data has become a hot research topic in academia. Reference [4] proposes the concept of realized volatility (RV) and believes that the real volatility can be estimated by the sum of squares of intraday high-frequency returns. The realized variance is a consistent asymptotic estimator of the integral volatility as the sampling tends to infinity. This method makes the volatility change from an unobservable hidden variable to an explicit variable that can be directly measured by nonparametric methods, without the time lag brought by the classical algorithm, and can better measure the change of volatility in the time series. It has set off a wave of research on high-frequency data in the field of volatility. Due to the characteristics of the realized volatility variable, an important use is to use it as a reference for evaluating various previous conditional variance models, such as the ARCH model and its various extended forms. Reference [5] evaluated the accuracy of intra day performance data prediction of the arch model. Reference [6] compared the prediction effect of 330 ARCH extension models on IBM stocks. Another important use of realized volatility is that it can be used as time series observations of volatility to test various characteristics of volatility and predict the future. The traditional ARCH model needs to fit the model in order to obtain the potential volatility variables, which has great limitations in analysis. Reference [7] summarizes various characteristics of realized volatility based on the high-frequency data of the Dow Jones Industrial Index and proposes an ARFIMAX model for this sequence. Reference [8] proves ARFIMAX by comparing the forecasting effect of this model with FIGARCH and FIEGARCH. The model is significantly better than the latter two models. Reference [9] uses the Vector Error Correction Model (VECM) to forecast the volatility of the exchange rate market, which proves that the prediction effect of the model algorithm is significantly better than that of ARCH(1), GARCH(1,1), and the exponential smoothing method in RiskMetrics. However, the realized measure has to face the problems caused by the noise of market microstructure, the instantaneous jumping behavior of stock price, and the nontrading time period in practical application. One angle to address these issues is to investigate methods of various realized measures to reduce biased estimates of volatility. Reference [10] proposed Bipower varimion (BPV) as an estimate of the continuous component of volatility to overcome the impact of instantaneous and high-intensity jumping behavior of prices in high-frequency data on returns. Reference [11] conducted a Monte Carlo simulation test with BPV and found that the volatility jump component accounted for about 7% of the overall volatility. Literature [12] found that there are obvious price jumps in foreign exchange, stock indexes, and bonds, and combined RV and BPV to extract the volatility price jump component, and established HAR. The RV-CJ model proves that the model can improve the accuracy of out-of-sample prediction. Reference [13] proposes a realized kernel variance (realized kernel), which considers the correlation between intraday returns, which can effectively reduce the impact of microscopic noise on traditional RV. Reference [14] proposed the realized range volatility (Realized Range, RR) based on the range theory, which improved the utilization of high-frequency information and effectively controlled the influence of microscopic noise. Reference [15] proposed that Median Realized Volatility (MedRV) can effectively control the impact of stock price jumping behavior on volatility estimation and proved that this estimator has better small sample adaptability and convergence than BPV. Reference [16] proposed an optimal combination of realized volatility and overnight squared return for the non-24-hour stock market, forming an optimal linear combination realized volatility (LCRV). Reference [17] proposed a two-scale RV (two-scale Realized Volatility) based on different time scales and used subsampling for bias correction to weaken the negative impact of market microstructure noise. Reference [18] proposed a weighting method of adding the sample variance of the overnight rate of return and the sample variance of the rate of return calculated by the "opening price and closing price" of the day into the RV to eliminate the influence of the overnight rate of return. Another way to solve the noise is to study the optimal sampling frequency of high-frequency data and reduce the problem of microstructure noise by reducing the frequency. Reference [19] proposed the volatility characteristic map method; the principle is that the minimum sampling frequency that makes the characteristic curve stable is the

optimal frequency. Reference [20] proposed a method for calculating the optimal sampling frequency of realized volatility based on minimizing MSE. Reference [21] studied the optimal frequency selection problem based on RV linear prediction in time-varying microstructure noise processes.

3. Stochastic Volatility Data Analysis

Any probability distribution on the parameter space Θ is called a prior distribution. In this paper, $\pi(\theta)$ is used to represent the prior distribution of θ. Among them, $\pi(\theta)$ is the probability function of the random variable θ.

After obtaining the sample x, the posterior distribution of θ is the conditional distribution of θ under the given condition of $X = x$, which is denoted as $\pi(\theta|x)$. For the case of density, its density function is

$$\pi(\theta|x) = \frac{h(x,\theta)}{m(x)} = \frac{f(x\mid\theta)\pi(\theta)}{\int_\Theta f(x\mid\theta)\pi(\theta)\mathrm{d}\theta}. \tag{1}$$

Among them, $h(x,\theta) = f(x|\theta)\pi(\theta)$, which is the joint distribution of X and θ. However, $m(x) = \int_\Theta h(x,\theta)\mathrm{d}\theta = \int_\Theta f(x|\theta)\pi(\theta)\mathrm{d}\theta$ is the marginal distribution of X.

Equation (1) is the density function form of the Bayesian formula, which concentrates all the information about θ in the three kinds of information: population, sample, and prior. However, it is the result obtained after excluding all information unrelated to θ. If θ is a discrete random variable, the prior distribution is represented by the prior distribution sequence $\{\pi(\theta_i), \quad i = 1, 2, \ldots\}$. At this point, the posterior distribution has the following form:

$$\pi(\theta_i|x) = \frac{f(x\mid\theta_i)\pi(\theta_i)}{\sum_i f(x\mid\theta_i)\pi(\theta_i)\ (i = 1, 2, \ldots).} \tag{2}$$

If the population X from which the sample comes is also discrete, we only need to regard the density function $f(x|\theta_i)$ as the probability $P(X = x|\theta_i)$ of the event $\{X = x|\theta_i\}$. At this time, the sample X is in the form of a joint density function, and formula (2) is the Bayesian formula.

When the sample distribution is known, for theoretical needs, the prior distribution of the parameters is usually selected as the conjugate prior distribution, which is defined as follows.

We assume that $\mathscr{F}$ represents a family of distributions consisting of the prior distribution $\pi(0)$ of θ. If for any $\pi \in \mathscr{F}$ and sample value x, the posterior distribution $\pi(\theta_i|x)$ still belongs to $\mathscr{F}$, then $\mathscr{F}$ is said to be a conjugate prior distribution family. In this paper, the calculation of the posterior distribution can be simplified by using the conjugate prior distribution, and the calculation formula of the posterior density is given by

$$\pi(\theta|x) = \frac{f(x\mid\theta)\pi(\theta)}{f_m(x)} = \frac{f(x\mid\theta)\pi(\theta)}{\int_\Theta f(x\mid\theta)\pi(\theta)\mathrm{d}\theta}. \tag{3}$$

Among them, $\pi(\theta)$ is the prior density of θ, $f_m(x)$ is the marginal density of X, and $f(x|\theta)$ is the density function of the sample. In some cases, $f(x|\theta)$ can be replaced by the likelihood function $L(\theta|x)$. If it is regarded as the probability density of random variable X, it is replaced by $f(x|\theta)$. If it is regarded as the likelihood function of θ, it is replaced by $L(\theta|X)$. Since $f_m(x)$ has nothing to do with θ, this paper treats $f_m(x)$ as a constant independent of θ; thus, we get

$$\pi(\theta|x) = \frac{L(\theta\mid x)\pi(\theta)}{f_m(x)} \propto L(\theta\mid x)\pi(\theta). \tag{4}$$

Among them, "$\propto$" means "proportional to"; that is, the left- and right-hand sides of (4) differ only by a constant factor, and this constant has nothing to do with θ.

Therefore, for the case of the conjugate prior distribution, the solution of the posterior density is carried out according to the following steps:

(1) In this paper, the kernel of the likelihood function $L(\theta|x)$ of θ is written, that is, the factors in $L(\theta|x)$ that are only related to the parameter θ, and then the kernel of the prior density $\pi(\theta)$ is written, that is, the factors in $\pi(\theta)$ that are only related to the parameter θ.

(2) Similar to equation (3), the kernel of the posterior density is written; that is,

$$\begin{aligned}\pi(\theta|x) &\propto L(\theta|x)\pi(\theta) \propto \{L(\theta|x)\text{Nucleus of}\}\\ &\cdot \{\pi(\theta)\ \text{Nucleus of}\}.\end{aligned} \tag{5}$$

That is to say, the "kernel of the posterior density" is the product of the "kernel of the likelihood function" and the "kernel of the prior density."

(3) A regularization constant factor (which can be related to x) is added to the right-hand side of equation (4), and the posterior density can be obtained.

It is worth noting that the above simplified method is only valid for the case where the prior distribution is a conjugate distribution, and it does not consider the case where the prior part is a nonconjugate prior. After obtaining the kernel of the posterior distribution, if you cannot judge the type of the posterior distribution, you will not know how to add a regularization constant factor, and you will not be able to calculate the posterior density. At this time, the posterior density can only be calculated by formula (1).

After obtaining the posterior distribution of the parameter θ, the posterior mean of θ can be used as an estimator for the parameter θ, as follows:

$$\widehat{\theta} = E(\theta\mid x) = \int_\Theta \theta\pi(\theta\mid x)\mathrm{d}\theta = \frac{\int_\Theta \theta f(x\mid\theta)\pi(\theta)\mathrm{d}\theta}{\int_\Theta f(x\mid\theta)\pi(\theta)\mathrm{d}\theta}. \tag{6}$$

This process involves evaluating integrals in expressions. However, in some practical problems, the abovementioned integrals are high-dimensional integrals, and the posterior distribution of the parameter θ does not show an expression, which makes the numerical integration algorithm difficult to work. In recent years, a series of advanced computing methods have been developed to solve the difficult problem of Bayesian computing to a large extent. Among them, the most widely used is the Markov Chain Monte Carlo

(MCMC) sampling method, such as Gibbs sampling method. Before introducing the MCMC method, we first give the posterior density functions of the parameters of the standard SV model and SV-T model.

When performing Bayesian inference on the model, we need to set the prior distribution of the parameters first. When choosing a prior distribution, two aspects should be considered: rationality and ease of computation. In Bayesian inference, conjugate prior distributions are often used. In the standard SV model, considering the value range of the parameter ϕ, we set up $\phi_1 = \phi + 1/2$. We refer to the priors on the parameters of the standard SV model given by Kim et al. (1998) as follows:

$$\mu \sim N(0, 100), \quad \phi_1 \sim Be(20, 1.5), \ \tau \sim Ga(2.5, 0.025), h_0 \sim N\left(\mu, \tau^{-1}\right). \tag{7}$$

Among them, *Be* represents the beta distribution and *Ga* represents the gamma distribution. It is not difficult to obtain that the prior mean of the persistence parameter ϕ is equal to 0.86, and the prior mean of the precision parameter τ is equal to 100. Compared with the parameters of the SV model in practice, the set prior information is closer to the actual situation, which has a certain rationality. We deduce the posterior density of each parameter in the model according to the method in formula (5), as follows:

(1) The posterior density of μ is as follows:

$$\begin{aligned}
\pi(\mu|\phi, \tau, \mathbf{h}, \mathbf{y}) &= \frac{\pi(\mu, \phi, \tau, \mathbf{h}|\mathbf{y})}{\pi(\phi, \tau, \mathbf{h}|\mathbf{y})} \\
&\propto \exp\left(-\frac{\mu^2}{2}\right)\exp\left\{-\frac{\tau}{2}\sum_{t=1}^{n}\left[h_t - \mu - \phi\left(h_{t-1} - \mu\right)\right]^2\right\} \\
&\propto \exp\left\{-\frac{1}{2}\left[1 + n(1-\phi)^2\tau\right]\left[\mu - \frac{(1-\phi)\tau}{2 + 2n(1-\rho)^2\tau}\sum_{t=1}^{n}\left[h_t - \phi\left(h_{t-1}\right)\right]^2\right]\right\} \\
&\propto N\left(\frac{(1-\phi)\tau}{2 + 2n(1-\phi)^2\tau}\sum_{t=1}^{n}\left[h_t - \phi\left(h_{t-1}\right)\right]^2, \quad 1 + n(1-\phi)^2\tau\right).
\end{aligned} \tag{8}$$

(2) The posterior density of ϕ is as follows:

$$\begin{aligned}
\pi(\phi|\mu, \tau, \mathbf{h}, \mathbf{y}) &= \frac{\pi(\mu, \phi, \tau, \mathbf{h}|\mathbf{y})}{\pi(\mu, \tau, \mathbf{h}|\mathbf{y})} \\
&\propto \left(\frac{1+\phi}{2}\right)^{19}\left(\frac{1-\phi}{2}\right)\exp\left\{-\frac{\tau}{2}\sum_{t=1}^{n}\left[h_t - \mu - \phi\left(h_{t-1} - \mu\right)\right]^2\right\} \\
&\propto \left(\frac{1+\phi}{2}\right)^{19}\left(\frac{1-\phi}{2}\right)^{0.5}\exp\left\{-\frac{\tau}{2}\sum_{t=1}^{n}\left(h_{t-1} - \mu\right)^2\left[\phi - \frac{\sum_{t=1}^{n}\left(h_t - \mu\right)\left(h_{t-1} - \mu\right)}{\sum_{t=1}^{n}\left(h_{t-1} - \mu\right)^2}\right]^2\right\}.
\end{aligned} \tag{9}$$

(3) The posterior density of τ is as follows:

$$\begin{aligned}
\pi(\tau|\mu, \phi, \mathbf{h}, \mathbf{y}) &= \frac{\pi(\mu, \phi, \tau, \mathbf{h}|\mathbf{y})}{\pi(\mu, \phi, \mathbf{h}|\mathbf{y})} \\
&\propto \tau^{1.5}\exp\left(-0.025\tau\right)\tau^{n+1/2}\exp\left\{-\frac{\tau}{2}\sum_{t=1}^{n}\left[h_t - \mu - \phi\left(h_{t-1} - \mu\right)\right]^2 + h_0^2\right\} \\
&\propto \tau^{n+4/2}\exp\left\{-\frac{\tau}{2}\left[\sum_{t=1}^{n}\left(h_t - \mu - \phi\left(h_{t-1} - \mu\right)\right)^2 + h_0^2 + \frac{1}{20}\right]\right\}.
\end{aligned} \tag{10}$$

(4) The posterior density of h_t is as follows:

$$\pi(h_t|\mu,\phi,\mathbf{h}_{-t},\mathbf{y}) \propto \exp\left\{-\frac{y_t^2}{2\exp(h_t)} - \frac{1}{2}\left[\left(1+\phi^2\right)\tau h_t^2 - 2\tau(\mu+\phi(h_{t-1}-\mu)+\phi h_{t-1}-\phi\mu(1-\phi))h_t + h_t\right]\right\}. \tag{11}$$

Compared with the unknown parameters μ, φ, τ, and (h) of the SV model, the unknown parameters of the SV-T model have more degrees of freedom parameters ω. The prior of the degree of freedom ω of the SV-T model is $\omega \sim \chi^2(8)$, and the priors of other parameters μ, φ, τ, and (h) are consistent with those of the standard SV model. The posterior distribution density of each parameter of the SV-T model is as follows.

(1) The posterior density of μ is as follows:

$$\begin{aligned}\pi(\mu|\phi,\tau,\omega,\mathbf{h},\mathbf{y}) &= \frac{\pi((\mu,\phi,\tau,\omega,\mathbf{h}|\mathbf{y})}{\pi(\phi,\tau,\omega,\mathbf{h}|\mathbf{y})} \\ &\propto \exp\left\{-\frac{1}{2}\left[1+n(1-\phi)^2\tau\right]\left[\mu - \frac{(1-\phi)\tau}{2+2n(1-\rho)^2\tau}\sum_{t=1}^{n}\left[h_t-\phi(h_{t-1})\right]^2\right]\right\} \\ &\propto N\left(\frac{(1-\phi)\tau}{2+2n(1-\phi)^2\tau}\sum_{t=1}^{n}\left[h_t-\phi(h_{t-1})\right]^2,\quad 1+n(1-\phi)^2\tau\right).\end{aligned} \tag{12}$$

(2) The posterior density of ϕ is as follows:

$$\begin{aligned}\pi(\phi|\mu,\tau,\omega,\mathbf{h},\mathbf{y}) &= \frac{\pi(\mu,\phi,\tau,\omega,\mathbf{h}|\mathbf{y})}{\pi(\mu,\tau,\omega,\mathbf{h}|\mathbf{y})} \\ &\propto \left(\frac{1+\phi}{2}\right)^{19}\left(\frac{1-\phi}{2}\right)^{0.5}\exp\left\{-\frac{\tau}{2}\sum_{t=1}^{n}(h_{t-1}-\mu)^2\left[\phi - \frac{\sum_{t=1}^{n}(h_t-\mu)(h_{t-1}-\mu)}{\sum_{t=1}^{n}(h_{t-1}-\mu)^2}\right]^2\right.\end{aligned} \tag{13}$$

(3) The posterior density of τ is as follows:

$$\begin{aligned}\pi(\tau|\mu,\phi,\omega,\mathbf{h},\mathbf{y}) &= \frac{\pi(\mu,\phi,\tau,\omega,\mathbf{h}|\mathbf{y})}{\pi(\mu,\phi,\omega,\mathbf{h}|\mathbf{y})} \\ &\propto \tau^{n+4/2}\exp\left\{-\frac{\tau}{2}\left[\sum_{t=1}^{n}\left(h_t-\mu-\phi(h_{t-1}-\mu)\right)^2 + h_0^2 + \frac{1}{20}\right]\right\}.\end{aligned} \tag{14}$$

(4) The posterior density of ω is as follows:

$$\pi(\omega|\mu,\phi,\tau,\mathbf{h},\mathbf{y}) = \frac{\pi(\mu,\phi,\tau,\omega,\mathbf{h}|\mathbf{y})}{\pi(\mu,\phi,\tau,\mathbf{h}|\mathbf{y})} \propto \omega^{6-n/2}\exp\left(-\frac{\omega}{2}\right)\left(\frac{\Gamma((\omega+1)/2)}{\Gamma(\omega/2)}\right)^{n}\prod_{\mathbf{t}=1}^{n}\left(1+\frac{y_t^2\exp(-h_t)}{\omega}\right)^{-\omega+1/2}. \tag{15}$$

(5) The posterior density of h_t is as follows:

$$\pi(h_t|\mu,\phi,\tau,\omega,\mathbf{h}_{-t},\mathbf{y}) \propto \left(1+\frac{y_t^2\exp(-h_t)}{\omega}\right)^{-\omega+1/2} \exp\left\{-\frac{1}{2}\left[\tau\left(1+\phi^2\right)h_t^2 - 2\tau\mu + \phi\left(h_{t-1}-\mu+h_{t+1}-\mu\phi\right)h_t\right] + h_t\right\}. \tag{16}$$

It can be seen that the posterior distribution density of each parameter of the standard SV model and the SV-T model is a high-dimensional multivariate distribution, and the Bayesian calculation can be realized by the Markov Chain Monte Carlo (MCMC) sampling method. In the following, we briefly introduce the Markov chain Monte Carlo method and the Gibbs sampling method.

We assume that $\{X_n, n \geq 0\}$ is a random process that takes only countable values. If $X_n = i$, it means that the state of the process at time n is i, and $S = \{0, 1, 2, \ldots\}$ means the state set. If the following conditions are satisfied for any n, then $\{X_n, \quad n \geq 0\}$ is called a discrete-time Markov chain, which is abbreviated as Markov chain.

$$P\left(X_{n+1} = j|X_0 = i_0, \ldots, X_{n-1} = i_{n-1}, \quad X_n = i\right) = P\left(X_{n+1} = j|X_n = i\right). \tag{17}$$

It can be seen from the above formula that for the random process $\{X_n, n \geq 0\}$, the future state $\{X_{n+1} = j\}$ is only related to the current state $\{X_n = i\}$, and it has nothing to do with the past state $\{X_k = i_k, \quad k \leq n-1\}$.

The conditional probability $P(X_{n+1} = j|X_n = i)$ is called the single-step transition probability of the Markov chain. If the transition probability has nothing to do with n and is a fixed value, then the Markov chain is said to have a stable transition probability, which is denoted as p_{ij}. A Markov chain with a smooth transition probability is also called a time-homogeneous Markov chain, and $\mathbf{P} = (p_{ij}), \quad \forall i, j \in S$ is called the transition probability matrix of the Markov chain.

The conditional probability $P(X_{n+1} = j|X_n = i)$ is called the single-step transition probability of the Markov chain. If the transition probability has nothing to do with n and is a fixed value, then the Markov chain is said to have a stable transition probability, which is denoted as p_{ij}. A Markov chain with a smooth transition probability is also called a time-homogeneous Markov chain, and $\mathbf{P} = (p_{ij}), \quad \forall i, j \in S$ is called the transition probability matrix of the Markov chain.

3.1. Stationarity. We assume that the Markov chain has a transition probability matrix $\mathbf{P} = (p_{ij})$. If a probability distribution $\pi = \{\pi_i, \quad i \geq 0\}$ satisfies $\pi = \sum \pi_i p_{ij}$, then it is called the stationary distribution of the Markov chain.

It is not difficult to see that if the initial state X_0 of the process has a stationary distribution $\pi = \{\pi_i, \quad i \geq 0\}$, that is, $P(X_0 = j) = \pi_j$, then there is

$$P\left(X_1 = j\right) = \sum_i P\left(X_1 = j|X_0 = i\right)P\left(X_0 = i\right) = \sum_i \pi_i p_{ij} = \pi_j. \tag{18}$$

By induction, we get

$$P\left(X_n = j\right) = \sum_i P\left(X_n = j|X_{n-1} = i\right)P\left(X_{n-1} = i\right) = \sum_i \pi_i p_{ij} = \pi_j. \tag{19}$$

Thus, for all n, X_n has the same distribution π; that is, $\{X_n, \quad n \geq 0\}$ is stationary as a random process.

3.2. Irreducibility. We assume that a Markov chain $\{X_n\}$ with countable state space S and transition probability matrix $\mathbf{P} = (p_{ij})$ is called irreducible. If for any two states $i, j \in S$, the probability of this chain transitioning from state i to state j is positive. That is, for a certain $n \geq 1$, there is

$$P_{ij}^{(n)} = P\left(X_n = j|X_0 = i\right) > 0. \tag{20}$$

By definition, a Markov chain with "irreducibility" means that any other state can always be reached from any state.

3.3. Aperiodic. We assume that a state i of a Markov chain has period k. If it is possible to return to state i after a multiple of k steps, that is

$$k(i) = gc\ d\{n\colon P(X_n = j|X_0 = i) > 0\}. \tag{21}$$

Among them, $gc\ d$ denotes the "maximum number of conventions." If the maximum number of times it returns to any state is 1, a Marshall chain is acyclic. A nonperiodic Marschall chain is guaranteed not to get trapped in a loop.

3.4. Normal Relapse. For always-returning state i, we assume that $T_i = inf\, n \geq 1\colon X_n = i|X_0 = i$ is the moment of returning to state i for the first time. If it satisfies the following formula, state i is said to be normal. When $\mu_i = \infty$, the state i is said to be zero-returning.

$$\mu_i = E(T_i) < \infty. \tag{22}$$

3.5. Ergodicity. We assume that the state of a Markov chain is called ergodic. If it is aperiodic and normal, and all states of the Markov chain are traversal, then the Markov chain is said to be ergodic.

To sum up, from the basic theory of Markov chain, we can know that the Markov chain we need to construct must be irreducible, normal recursive, and aperiodic. However, a Markov chain that satisfies these regular conditions has a unique stationary distribution.

The theoretical basis for Bayesian analysis using the Markov Chain Monte Carlo MCMC method is based on some of the following limit theorems.

Theorem 1 is as follows. We assume that $\{X_n, \quad n \geq 0\}$ is a Markov chain with a countable state space S whose transition probability matrix is **P**. Further, we assume that it is irreducible, aperiodic, and has a stationary distribution $\pi = \{\pi_i\colon i \in S\}$. Then, for any initial distribution π of X_0, we have

$$\sum_{j \in S} \left| P(X_n = j) - \pi_j \right| \longrightarrow 0, \quad n \longrightarrow \infty. \tag{23}$$

In other words, for larger n, the distribution of X_n will be close to π. For general state spaces, similar results hold. Under suitable conditions, when $n \longrightarrow \infty$, the distribution of X_n will converge to π.

Theorem 2 (the theorem of large numbers for the Markov chain) is as follows: We assume that $\{X_n, n \geq 0\}$ is a Markov chain with countable state space S, and its transition probability matrix is **P**. Further, we assume that it is irreducible and has a flat distribution with a stationary distribution $\pi = \{\pi_i\colon i \in S\}$. Then, for any initial distribution of any bounded function $h\colon S \longrightarrow \mathbf{R}$ and initial value X_0, we have

$$\frac{1}{n} \sum_{i=0}^{n-1} h(X_i) \longrightarrow \sum_j h(j)\pi_j, \quad n \longrightarrow \infty. \tag{24}$$

When the state space is uncountable, the Markov chain $\{X_n, \quad n \geq 0\}$ is irreducible and there is a stationary distribution π; there is also

$$\frac{1}{n} \sum_{i=0}^{n-1} h(X_i) \longrightarrow \int_S h(x) \mathrm{d}\pi(x), \quad n \longrightarrow \infty. \tag{25}$$

The conclusion of this theorem is very useful. For example, we assume a probability distribution π on a set S and a real function $h(\theta)$ on S. We assume that we want to calculate the integral $\mu = \int_S h(\theta) \mathrm{d}\pi(\theta|\mathbf{x})$; then, we can construct a Markov chain whose state space is S. At the same time, its stationary distribution π is the target posterior distribution $\pi(\cdot|x)$ starting from an initial value θ_0, running this chain for a period of time, such as $0, 1, 2, \ldots, n-1$, and then generating random samples $\theta_0, \theta_1, \theta_2, \ldots, \theta_n - 1$. From the Markov chain theorem of large numbers, it can be known that

$$\overline{\mu}_n = \frac{1}{n} \sum_{i=0}^{n-1} h(\theta_i). \tag{26}$$

The above formula is a consistent estimate of the required integral μ. When it is difficult to sample directly from the posterior distribution $\pi(\theta|x)$, a suitable Markov chain is constructed, and its stationary distribution is the target sampling distribution. Furthermore, the sample paths of the Markov chain are used to calculate the distribution features of interest. This method is called the Markov Chain Monte Carlo (MCMC) method.

In practical computing, most Bayesian computing problems need to deal with a high-dimensional multivariate posterior distribution. Randomly generating samples from such high-dimensional distributions is often difficult. However, Gibbs sampling is particularly suitable for this situation. The most attractive part of this method is that it can generate an irreducible and aperiodic Markov chain with the target high-dimensional posterior distribution as a stationary distribution only by sampling from a series of univariate distributions.

We assume that $\mathbf{X} = (X_1, \ldots, X_d)$ is a random variable in $\mathbb{R}^d$, and its joint distribution $f(x)$ is the target sampling distribution. It is a random variable of dimension d-1, as follows:

$$\mathbf{X}_{-j} = \left(X_1, \ldots, X_{j-1}, X_{j+1}, \ldots, X_d\right). \tag{27}$$

Subsequently, the conditional density of $X_j|\mathbf{X}_{-j}$ is denoted as $f(x_j|x_{-j})$; then, the Gibbs sampling method is to extract candidate points from these d distributions, thus solving the difficulty of direct sampling from $f(x)$. The specific algorithm is as follows:

(1) The algorithm gives the initial value of $X(0)$.

(2) For $t = 1, 2, \ldots, T$:

(i) The algorithm sets up $t = 1, 2, \ldots, T$.
(ii) For each component $x_1 = X_1(t-1)$,
(a) The algorithm extracts the candidate point $X_j^*(t)$ from $f(\mathbf{X}_j|\mathbf{x}_{-j})$;

(b) $x_j = X_j^*(t)$ is updated.
(iii) The algorithm establishes $\mathbf{X}(t) = (X_1^*(t), \ldots, X_d^*(t))$.
(iv) As t increases, the algorithm repeats step (i).

In algorithm step (ii), each component is updated sequentially:

$$\begin{aligned} x_1(t) &\sim f\left(x_1 | x_2(t-1), \ldots, x_d(t-1)\right), \\ x_2(t) &\sim f\left(x_2 | x_1(t), x_3(t-1), \ldots, x_d(t-1)\right), \\ &\cdots \\ x_d(t) &\sim f\left(x_d | x_1(t), \ldots, x_{d-1}(t)\right). \end{aligned} \tag{28}$$

It is relatively straightforward to draw samples from the univariate distribution $f(x_j | x_1(t), x_2(t), \ldots, x_{j-1}(t), x_{j+1}(t-1), \ldots, x_d(t-1))$. Because $f(x_j | \mathbf{x}_{-j}) \propto f(x)$, except x_j which is a variable, all other variables are constants.

What is special about Gibbs sampling is that a fully conditional distribution can determine a unique joint distribution. The well-known Hammersley–Clifford theorem reveals this law.

We assume that the joint density distribution of the random variable $\mathbf{X} = (X_1, \ldots, X_d)$ is $f(x_1, \ldots, x_d)$, and the edge density function of X_i is $f_i(x_i)(i = 1, \ldots, d)$. If $f_i(x_i) > 0 (i = 1, \ldots, d)$, which means $f(x_1, \ldots, x_d) > 0$, then the joint density distribution f is said to satisfy the positive condition.

Theorem 3 (Hammersley–Clifford theorem) is as follows: Under positive conditions, the joint density distribution f satisfies the following:

$$f(x_1, \ldots, x_d) \propto \prod_{j=1}^{d} \frac{f\left(x_j | x_1, \ldots, x_{j-1}, x_{j+1}', \ldots, x_d'\right)}{f\left(x_j' x_1, \ldots, x_{j-1}, x_{j+1}', \ldots, x_d'\right)}. \tag{29}$$

For any x and x' in the support set S of f, we have

$$\begin{aligned} f(x_1, \ldots, x_d) &= f(x_d | x_1, \ldots, x_{d-1}) f(x_1, \ldots, x_{d-1}) \\ &= \frac{f(x_d | x_1, \ldots, x_{d-1})}{f(x_d' | x_1, \ldots, x_{d-1})} f(x_1, \ldots, x_{d-1}, x_d') \\ &= \frac{f(x_d | x_1, \ldots, x_{d-1})}{f(x_d' | x_1, \ldots, x_{d-1})} \frac{f(x_{d-1} | x_1, \ldots, x_{d-2}, x_d')}{f(x_{d-1}' | x_1, \ldots, x_{d-2}, x_d')} \\ &\quad \times f(x_1, \ldots, x_{d-1}', x_d') \\ &= \ldots \\ &= \prod_{j=1}^{d} \frac{f\left(x_j | x_1, \ldots, x_{j-1}, x_{j+1}', \ldots, x_d'\right)}{f\left(x_j' | x_1, \ldots, x_{j-1}, x_{j+1}', \ldots, x_d'\right)} f(x_1', \ldots, x_d'). \end{aligned} \tag{30}$$

Taking the Gibbs sampling of the SV model as an example, we assume that the parameter set $\theta = (\mu, \phi, \tau)$ and the initial value of the logarithmic volatility $\mathbf{h}$, which is denoted as $\Omega^{(0)} = (\mu^{(0)}, \phi^{(0)}, \tau^{(0)}, \mathbf{h}^{(0)})$. Then, a single Gibbs sampling is as follows:

(1) The algorithm extracts $h^{(1)}$ from $\pi(h_t | \mu^{(0)}, \phi^{(0)}, \tau^{(0)}, \mathbf{h}_{-\mathbf{t}}^{(0)}, \mathbf{y})$.
(2) The algorithm extracts $\tau^{(1)}$ from $\pi(\tau | \mu^{(0)}, \phi^{(0)}, \mathbf{h}^{(1)}, \mathbf{y})$.
(3) The algorithm extracts $\varphi^{(1)}$ from $\pi(\phi | \mu^{(0)}, \tau^{(1)}, \mathbf{h}^{(1)}, \mathbf{y})$.
(4) The algorithm extracts $\mu^{(1)}$ from $\pi(\mu | \phi^{(1)}, \tau^{(1)}, \mathbf{h}^{(1)}, \mathbf{y})$.

After the above iterations, the initial value is updated to $\Omega^{(1)} = (\mu^{(1)}, \phi^{(1)}, \tau^{(1)}, \mathbf{h}^{(1)})$, and by repeating the Gibbs sampling process k times, we can get $(\Omega^{(1)}, \Omega^{(2)}, \ldots, \Omega^{(k)})$. Under the condition of regularity, when the number of iterations k is large enough, $\Omega^{(k)}$ is equivalent to a random draw in the posterior joint distribution. In practice, Gibbs sampling requires enough iterations to reach a stationary state. However, the sample composed of m data before reaching the stationary state after discarding Gibbs sampling is $(\Omega^{(m)}, \Omega^{(m+1)}, \ldots, \Omega^{(k)})$. In the Monte Carlo estimation of parameters, the posterior mean of the parameter is estimated by the mean of the following k-m samples.

4. Prediction of High-Frequency Economic Data Based on Stochastic Fluctuation Model

The cobweb model is a classic model in Western economics. The model is mainly divided into three cases, and the different elasticity of supply and demand is still discussed. When the elasticity of supply of commodities is less than the elasticity of demand, the nonequilibrium price will converge according to the spider web model and finally reach the equilibrium price. In the case where the elasticity of supply of commodities is greater than the elasticity of demand, the conclusion is just the opposite: the nonequilibrium price will continue to diverge, the fluctuation will become larger and larger, and it will deviate from the equilibrium price. When

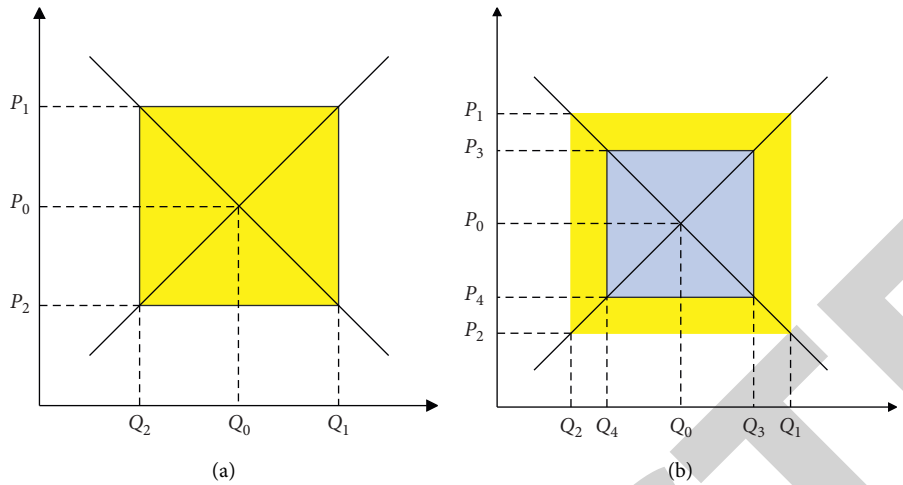


Figure 1: Cobweb model. (a) Cobweb model without futures/stock market. (b) Cobweb model with futures/stock markets.

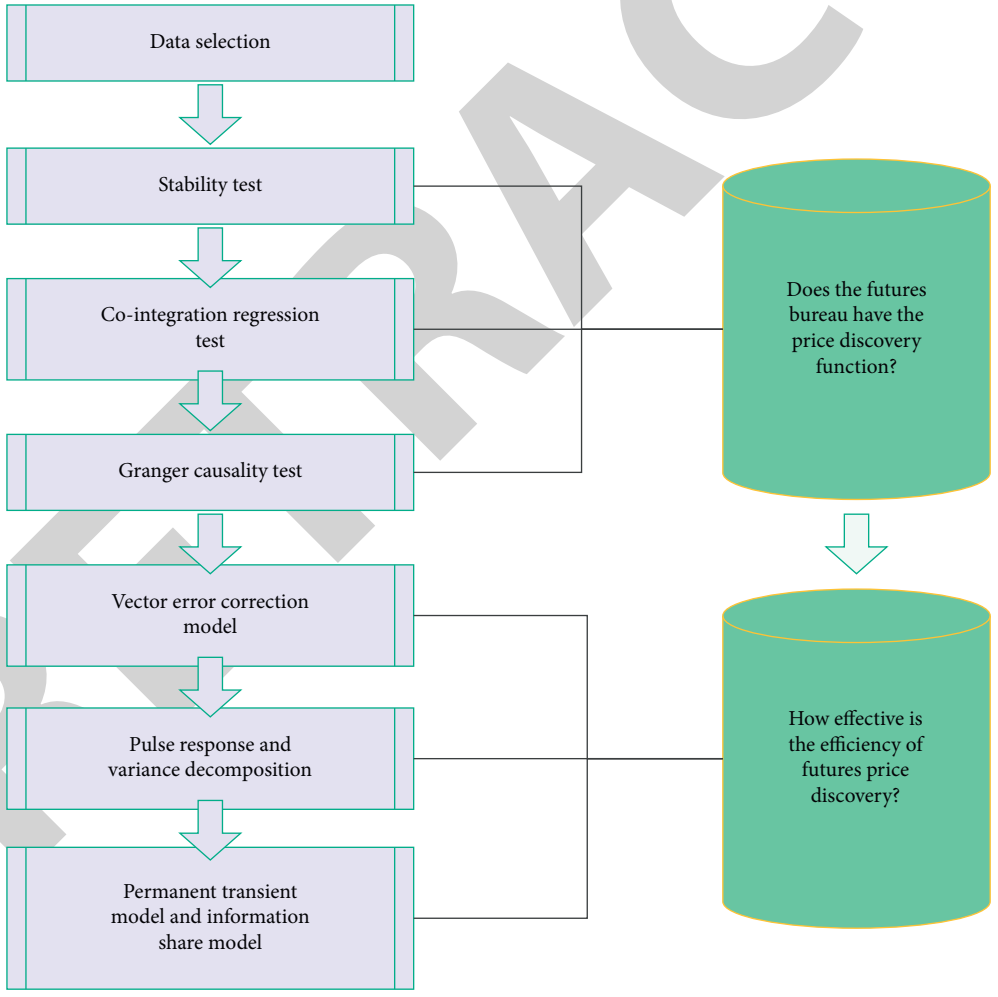


Figure 2: Structure diagram of empirical research.

the elasticity of supply of commodities is equal to the elasticity of demand of commodities, according to the cobweb model, prices will enter a cycle and cannot be adjusted to the equilibrium price level. We take the example of commodity supply elasticity equal to commodity demand elasticity for analysis. First, we consider the case where there is no futures/stock market, as shown in Figure 1.

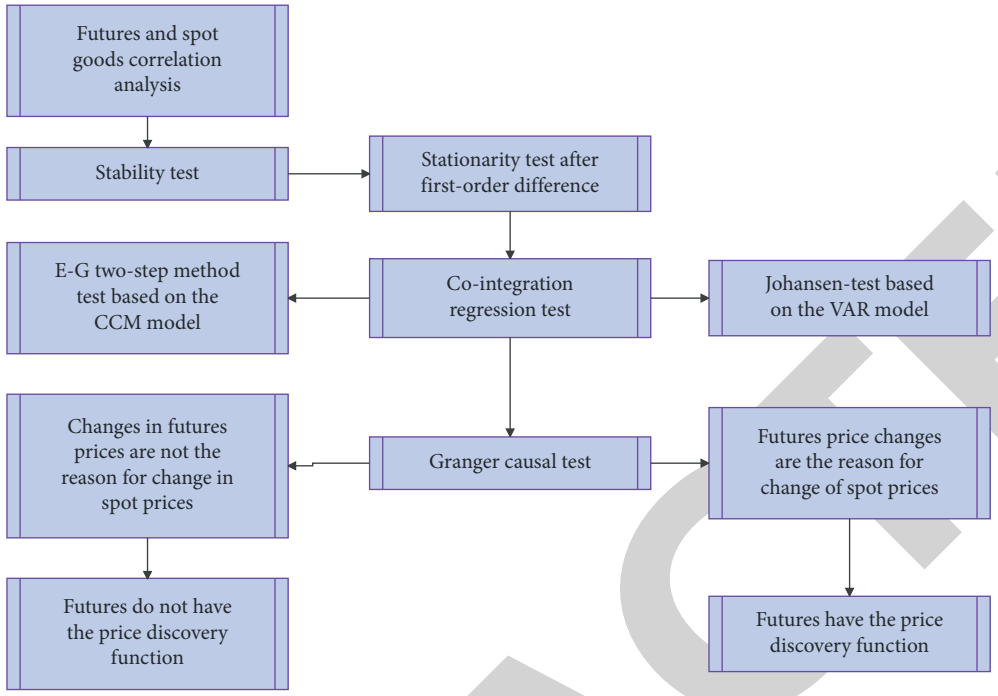


Figure 3: The empirical structure idea to test whether futures/stocks have price discovery function.

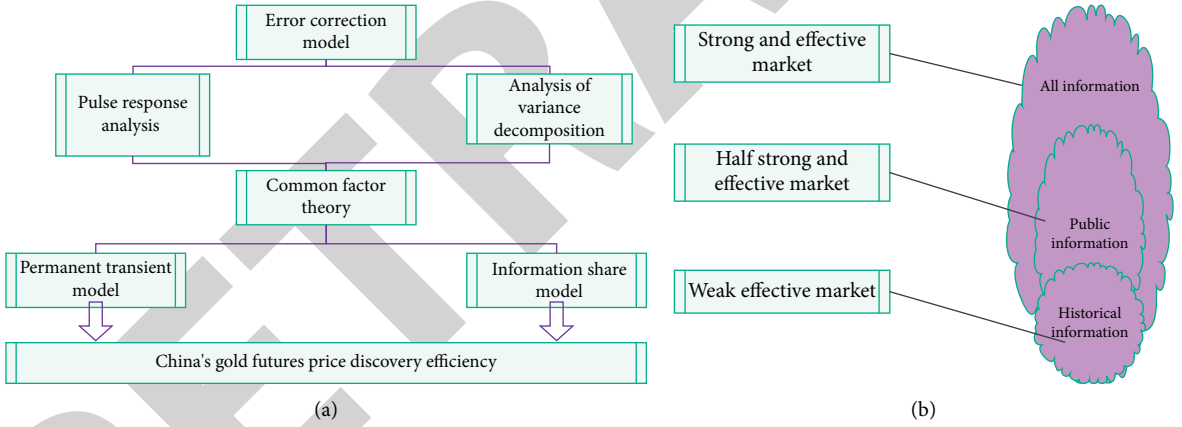


Figure 4: Financial market information processing. (a) Structure idea diagram of the empirical test of futures/stock price discovery efficiency. (b) Information and efficient markets.

This paper makes a preliminary judgment on the degree to which futures/stock price changes lead the spot by means of error correction model, impulse response, and variance decomposition. Furthermore, the contribution of futures/stock price changes to the effective price is studied through the common factor model so as to obtain its price discovery efficiency. Our empirical research design ideas are shown in Figure 2.

The empirical idea to test whether futures/stocks have the function of price discovery is shown in Figure 3.

The price discovery efficiency is judged by studying the contribution of futures/stock price changes to the effective price. The research idea of futures/stock price discovery efficiency is shown in Figure 4(a).

On the basis of information and securities price reflection, three different levels of efficient markets are proposed, namely, weak efficient market, semistrong efficient market, and strong efficient market, as shown in Figure 4(b).

The benchmark model used is an on-frequency forecasting model with low-frequency (weekly) stock squared returns as predictors. Specifically, our analytical framework can be shown in Figure 5.

After the above model is constructed, the effect of high-frequency data fluctuation is analyzed for the economic high-frequency data prediction model based on the stochastic fluctuation model, and the prediction effect of economic high-frequency data is evaluated. Moreover, this paper carries out research in combination with the

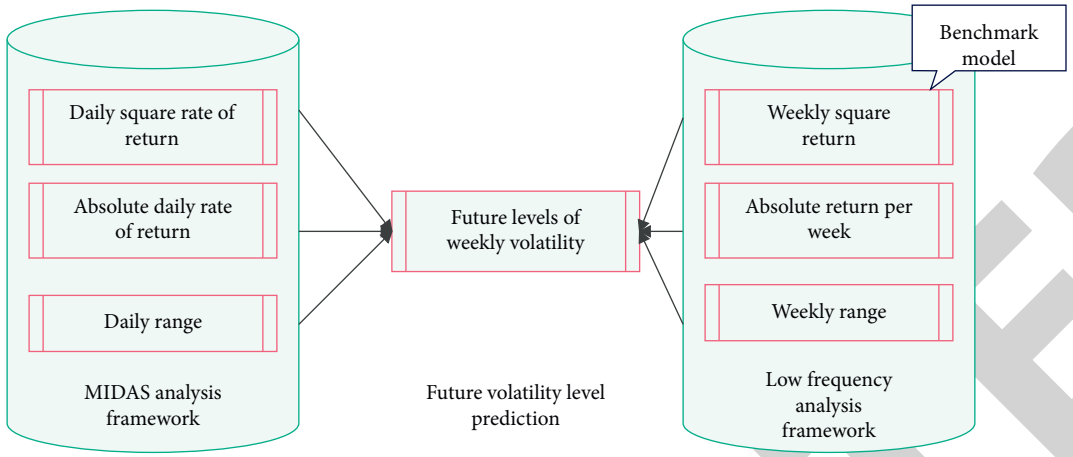


Figure 5: Prediction model framework.

Table 1: Data fluctuation analysis of economic high-frequency data prediction model based on stochastic fluctuation model.

Number	Analysis of economic fluctuations
1	78.5
2	85.4
3	83.5
4	88.9
5	84.7
6	87.8
7	91.0
8	82.5
9	84.9
10	83.4
11	88.7
12	84.9
13	86.4
14	83.4
15	79.3
16	86.7
17	88.2
18	90.4
19	85.3
20	89.1
21	80.1
22	80.7
23	81.5
24	86.9
25	85.6
26	90.7
27	80.0
28	78.2
29	79.2
30	88.6
31	78.6
32	80.3
33	78.5
34	86.2
35	85.2
36	81.2
37	86.1
38	89.9
39	87.2

Table 1: Continued.

Number	Analysis of economic fluctuations
40	82.7
41	89.7
42	87.7
43	85.3
44	88.7
45	89.0
46	90.5
47	87.5
48	86.1
49	89.8
50	85.5
51	87.0
52	86.1
53	79.2
54	84.9

Table 2: Prediction effect of economic high-frequency data prediction model based on stochastic fluctuation model.

Number	High-frequency data prediction
1	79.9
2	83.8
3	75.8
4	74.7
5	87.9
6	86.7
7	84.4
8	85.6
9	83.0
10	86.3
11	84.6
12	79.2
13	76.6
14	81.0
15	77.5
16	78.8
17	86.5
18	76.5
19	75.7

Table 2: Continued.

Number	High-frequency data prediction
20	74.4
21	81.9
22	81.2
23	78.8
24	82.6
25	81.9
26	75.5
27	85.3
28	86.8
29	74.2
30	79.7
31	82.9
32	78.4
33	84.3
34	86.4
35	78.8
36	84.2
37	74.1
38	81.2
39	79.8
40	79.8
41	81.0
42	84.4
43	86.1
44	74.5
45	74.1
46	84.1
47	80.4
48	74.8
49	86.9
50	80.7
51	82.9
52	81.5
53	83.5
54	75.7

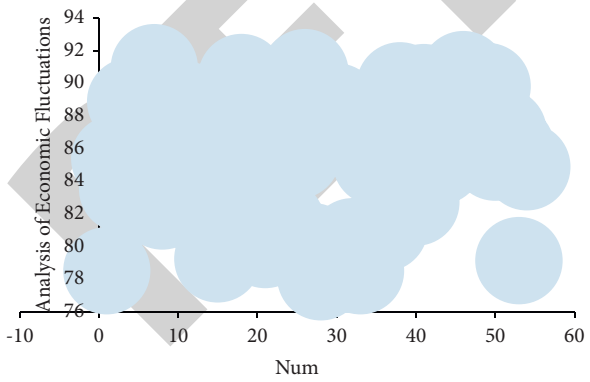


Figure 6: Data fluctuation analysis effect diagram of economic high-frequency data prediction model based on stochastic fluctuation model.

simulation test and counts the relevant test results and obtains the test results shown in Tables 1 and 2 and Figures 6 and 7.

It can be seen from the above experimental research that the economic high-frequency data prediction model based on the stochastic fluctuation model proposed in this paper has a good effect on the analysis and prediction of economic high-frequency data.

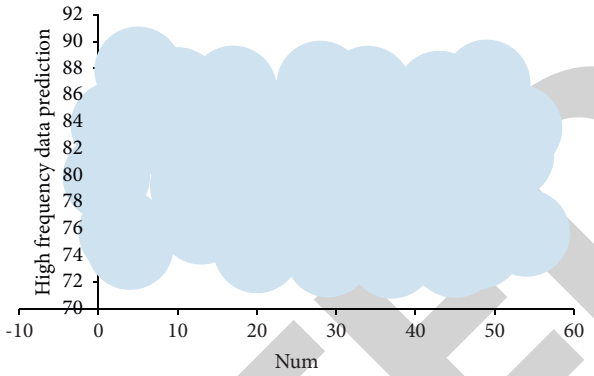


Figure 7: Prediction effect of economic high-frequency data prediction model based on stochastic fluctuation model.

5. Conclusion

High-frequency data studied in the field of financial market microstructure refers to the type of data as opposed to data on a daily or longer time interval. It is the transaction price, transaction volume, and other data collected during the trading day, and it is mainly the data collected in hours, minutes, or seconds. The UHF data refers to the data collected in real time during the transaction process of financial products such as securities and foreign exchange. Obviously, UHF data is data at unequal intervals. High-frequency and ultra-high-frequency data contain more real-time information about the securities trading process and more accurately capture every tiny change in the market. Using high-frequency and ultra-high-frequency data to study security price behavior has many advantages over using low-frequency data. In order to improve the effect of economic high-frequency data analysis, this paper combines the stochastic fluctuation model to carry out the forecast analysis of economic high-frequency data. The experimental research results show that the economic high-frequency data prediction model based on the stochastic fluctuation model proposed in this paper has a good effect on the analysis and prediction of economic high-frequency data.

Data Availability

The labeled dataset used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that they have no coflicts of interest regarding the publication of this paper.

References

[1] J. Fichtner, E. M. Heemskerk, and J. Garcia-Bernardo, "Hidden power of the Big Three? Passive index funds, re-concentration of corporate ownership, and new financial risk," *Business and Politics*, vol. 19, no. 2, pp. 298–326, 2017.

[2] C. Cueva, R. E. Roberts, T. Spencer et al., "Cortisol and testosterone increase financial risk taking and may destabilize

Hindawi
Security and Communication Networks
Volume 2024, Article ID 9860176, 1 page
https://doi.org/10.1155/2024/9860176

Retraction

Retracted: An Intrusion Detection Model Based on Improved ACGAN in Big Data Environment

Security and Communication Networks

Received 8 January 2024; Accepted 8 January 2024; Published 9 January 2024

This article has been retracted by Hindawi following an investigation undertaken by the publisher [1]. This investigation has uncovered evidence of one or more of the following indicators of systematic manipulation of the publication process:

(1) Discrepancies in scope

(2) Discrepancies in the description of the research reported

(3) Discrepancies between the availability of data and the research described

(4) Inappropriate citations

(5) Incoherent, meaningless and/or irrelevant content included in the article

(6) Manipulated or compromised peer review

The presence of these indicators undermines our confidence in the integrity of the article's content and we cannot, therefore, vouch for its reliability. Please note that this notice is intended solely to alert readers that the content of this article is unreliable. We have not investigated whether authors were aware of or involved in the systematic manipulation of the publication process.

Wiley and Hindawi regrets that the usual quality checks did not identify these issues before publication and have since put additional measures in place to safeguard research integrity.

We wish to credit our own Research Integrity and Research Publishing teams and anonymous and named external researchers and research integrity experts for contributing to this investigation.

The corresponding author, as the representative of all authors, has been given the opportunity to register their agreement or disagreement to this retraction. We have kept a record of any response received.

References

[1] J. Liao, "An Intrusion Detection Model Based on Improved ACGAN in Big Data Environment," *Security and Communication Networks*, vol. 2022, Article ID 6821174, 9 pages, 2022.

Hindawi
Security and Communication Networks
Volume 2022, Article ID 6821174, 9 pages
https://doi.org/10.1155/2022/6821174

Research Article

An Intrusion Detection Model Based on Improved ACGAN in Big Data Environment

Jianfeng Liao

Department of Computer, Wenhua University, Wuhan, Hubei 430074, China

Correspondence should be addressed to Jianfeng Liao; jazz9812@163.com

Received 22 February 2022; Revised 12 March 2022; Accepted 21 March 2022; Published 9 May 2022

Academic Editor: Zhiping Cai

With the development of big data technology, network intrusion problems against server vulnerabilities emerge one after another. To improve the accuracy of intrusion detection, this paper designs an intrusion detection platform based on the ACGAN (auxiliary classifier generative adversarial network) model in a big data environment. Firstly, by introducing a self-attention mechanism, the global characteristics of attack samples are extracted to improve the quality of generated samples. Then, by adding a gradient penalty, the model's convergence speed and training stability are improved. Finally, this method enhances and expands the attack samples and verifies the dataset. The experimental results show that compared with other comparison methods, the overall detection accuracy of this system is higher, and the false-positive rate and false-negative rate are lower.

1. Introduction

With the rapid development of computer and network technology, people's life depends more and more on the convenience brought by electronic equipment. Still the accompanying computer security problems are becoming more and more acute. According to the statistics of vulnerability data of Windows platform in recent years, the amount of vulnerability submission of Windows host system generally shows an upward trend year by year [1], and the intrusions launched against host vulnerabilities emerge one after another. How to effectively detect intrusion has become one of the focuses of network security research [2]. Generally speaking, according to the source of detection data, intrusion detection can be divided into network-based intrusion detection and host-based intrusion detection. Network-based intrusion detection uses the original IP packet as the data source to detect intrusion. Host-based intrusion detection generally finds intrusion by detecting systems, events, and system logs [3].

With the application of machine learning technology in various research fields, the intrusion detection model based on machine learning has gradually become the current research trend [4]. However, compared with deep learning models, traditional machine learning models such as Bayesian algorithms and decision trees have some deficiencies in data processing and feature association with unclear features or complex internal constraints [5]. Therefore, intrusion detection based on the deep learning model has become one of the research hotspots. Javaid et al. [6] proposed a self-learning technology based on deep learning, which learns good feature representation from unmarked data and then classifies intrusion. Yin et al. [7] used recurrent neural network for intrusion detection to improve the accuracy of detection. Qu et al. [8] proposed an intrusion detection model based on deep confidence network. Shone et al. [9] proposed an asymmetric deep autoencoder (NADE) based on unsupervised feature learning. It can be seen that the current intrusion detection system based on deep learning mainly focuses on the automation of high-dimensional data feature extraction, dimensionality reduction of high-dimensional data features, and improving the ability of sample recognition. Also, most studies use NSL-KDD as their training and testing datasets [10].

Although intrusion detection based on deep learning can effectively detect malware, malicious behavior, and malicious code, there are still the following limitations. (1)

In the training process, the attack samples are far less than the standard samples, resulting in the imbalance of the detection model and the inability to detect malicious attacks correctly. (2) With the development of malicious attack technology, the attack methods of attackers are constantly changing. Learning through the known intrusion knowledge base will make the model unable to detect the unknown attack data [11]. Therefore, researchers introduced generative adversarial networks (GANs) to generate useable attack data and enhance the training dataset to improve the performance of the detection model [12].

Jin et al. [13] proposed a self-evolving GAN model based on the game idea. At present, the model has been successfully and widely used in image classification and sample generation. It is mainly used to solve the problems of unstable training, pattern collapse, and sample generation. It has been studied to expand the samples of the malicious code base through the GAN to solve the problem of aging attack samples caused by the evolution of intrusion means [12]. Some GAN-based detection models have also been proposed, such as t-GAN [14] for detecting malicious code, t-DCGAN [15] for improving the stability of t-GAN model training process, BOT GAN [16] for detecting botnets, and CF-GAN [17] for detecting online payment fraud.

Aiming at the problem of low diagnostic accuracy, this paper proposes a data enhancement method based on ACGAN. The two-dimensional convolution network model is adopted to effectively reduce the amount of network training parameters and improve the convergence speed of the network. At the same time, gradient punishment is used instead of weight clipping to overcome the problems of gradient disappearance and mode collapse and enhance the stability of model training. By introducing the attention mechanism into the generator and discriminator of ACGAN, the global features of the samples are fully extracted, and the generation quality and learning efficiency of the model are improved. Experiments show that this method can balance the impact of unstable data on classification accuracy and effectively reduce the misjudgment rate.

2. Related Work

2.1. Generating Countermeasure Network. GAN consists of opposing deep convolution networks, generator A, and discriminator D, respectively. A receives a set of noise satisfying the joint Gaussian distribution $U_k(k)$, and k is its input vector. The mapping relationship between $U_k(k)$ and actual data distribution $U_{\text{data}}(i)$ is established through a multilayer neural network [18], and new samples as close to the actual data as possible are generated. Then, it is sent to D and the actual sample to distinguish whether the data is the real quantity or the generated quantity. G and D compete with each other, forming a dynamic process of the zero-sum game [19]. When both losses reach the minimum, Nash equilibrium is reached. (1) shows the objective function of GAN:

$$\min_A \min_D Q(D, A) = E_{i\sim U_{\text{data}}}[\log_2 D(i)] + E_{k\sim U_k}[\log_2(1 - D(G(k)))], \tag{1}$$

where $E[\cdot]$ is the expectation of the corresponding distribution, $A[k]$ generates data for the generator, and $D[\cdot]$ is the judgment result of the discriminator.

The loss functions L_A, L_D of generator and discriminator are as follows:

$$\begin{aligned} L_A &= E_{k\sim U_k}[\log_2(1 - D(A(k)))], \\ L_D &= E_{i\sim U_{\text{data}}}[\log_2 D(i)] + E_{k\sim U_k}[\log_2(1 - D(A(k)))]. \end{aligned} \tag{2}$$

2.2. Auxiliary Classification Generation Countermeasure Network. The traditional GAN employs unsupervised learning, and the mode is too accessible, resulting in an uncontrollable training process. CGAN adds the auxiliary classification label c to the generator and discriminator, uses c to guide the direction of data generation, and realizes supervised learning [20]. ACGAN is improved based on conditional generation countermeasure network. The label information only acts on the generator, and the auxiliary classifier (C) is introduced into the discriminator to distinguish the category of samples. Therefore, the loss function of ACGAN can be divided into loss function L_S representing the authenticity of data and loss function L_C representing the accuracy of data classification:

$$\begin{aligned} L_S &= E_{i\sim U_{\text{data}}}[\log_2 D(i)] + E_{k\sim U_k}[\log_2((1 - D(A(k))))], \\ L_C &= E_{c\sim U_{\text{data}}}[\log_2 D(c)] + E_{c\sim U_k}[\log_2(1 - D(A(c)))]. \end{aligned} \tag{3}$$

2.3. Self-Attention Generation Confrontation Network. Most GANs are based on a convolutional neural network. Because the local acceptance domain of convolution calculation has a fault limit, it can only calculate the data features in a specific neighbourhood. Still it cannot mine the feature relationship between long-distance spatial regions, so the calculation efficiency is low. SAGAN adds a self-attention module in G and D, which can realize the modelling of remote sample dependency. The generator can mine feature information from all locations to generate sample details. At the same time, the discriminator can judge whether the feature details of the distant parts in the proper and false samples are consistent. It can master more comprehensive sample information and improve the network's overall performance. Figure 1 shows the feature calculation flow of self-attention module.

In Figure 1, ⊗ represents matrix multiplication, and each row is activated using softmax. After the sample features from the previous hidden layer i are multiplied by different weight matrices, they are first converted into the sum of two feature spaces $f(i)$ and $b(i)$ to calculate the attention map, the correlation of two feature spaces.

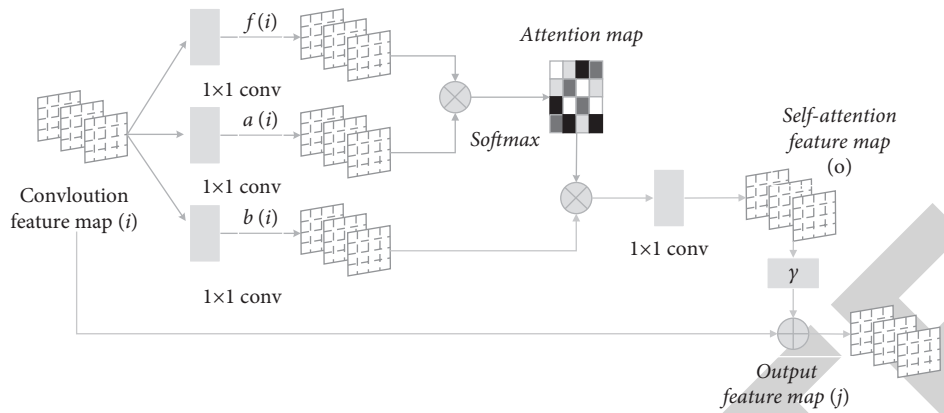


Figure 1: Feature calculation of self-attention module.

$$\begin{aligned}\mathbf{f}(i) &= M_f i,\\ \mathbf{b}(i) &= M_b i,\\ \mathbf{a}(i) &= M_a i,\\ \beta_{y,x} &= \frac{\exp\left(s_{xy}\right)}{\sum_{x=1}^{T}\exp\left(s_{xy}\right)},\\ \mathbf{s}_{xy} &= \mathbf{f}^T(i_x)\mathbf{a}\left(i_y\right),\end{aligned} \tag{4}$$

where $\beta_{y,x}$ indicates the influence degree of the x region on the synthetic y region, that is, the correlation degree of the two. s_{xy} is the incidence matrix. After matrix multiplication of the attention map $\beta_{y,x}$ and the feature space $h(i)$, the output features of the self-attention module are obtained.

$$o_x = \pm\sum_{x=1}^{N}\beta_{y,x}h\left(i_x\right). \tag{5}$$

The final output is shown in (6), where γ is the weight coefficient. Set up the initial value of γ as 0, and the weight gradually increases with the iterative process. Starting from domain informatics, the model gradually assigns the weight to other remote feature details to realize the integration of domain information and remote features.

$$j_x = \gamma o_x + i_x. \tag{6}$$

After adding the attention mechanism, the loss is weighted according to the influence of data points on the classification effect. The loss function is expressed as

$$\begin{aligned}L_D &= -E_{(i,j)\sim u_{\text{data}}}[m(0,-1+D(i,j))]\\ &\quad - E_{k\sim u_k, j\sim u_{\text{data}}}[m(0,-1+D(A(k)),j)],\\ L_G &= -E_{k\sim u_k, j\sim u_{\text{data}}}D(A(k),j).\end{aligned} \tag{7}$$

3. Algorithm Model

3.1. Improved ACGAN Model. ACGAN can control the direction of sample generation in the generation process through an auxiliary classifier to generate high-quality results. However, due to the limited size of the convolution kernel, we can only learn the relationship between the local region of the sample. The learning efficiency of the model is low, and details may be lost. Based on the supervision idea of ACGAN, the self-attention mechanism is added to A and D to help the model capture the relationship between the long-distance features of the sample. Using Wasserstein distance measure to generate the difference between samples and real samples, an improved ACGAN model is constructed to generate high-quality attack samples for diagnosis. The weight clipping can meet the 1-Lipschitz condition. However, due to the restriction of weight, the ability of network learning decreases. Also, the weight clipping is easy to set improperly, which will lead to gradient explosion or disappearance. A gradient penalty term is established, as shown in (8), to replace the weight clipping to realize the 1-Lipschitz condition to solve the above problems. The gradient penalty is a soft constraint, which will control the gradient around 1. The controllability is strong, the model is stable, and the above gradient problem is alleviated. At the same time, L1 regularization is added to the generator to improve the generalization ability of the generated model and alleviate overfitting.

$$L_{gu} = \lambda E_{\hat{i}}\sim u_{\hat{i}}\left(\|\nabla D(\hat{i})\|_2 - 1\right)^2, \tag{8}$$

where $\hat{i}$ represents the interpolation sample between the real image and the generated image. Therefore, the loss function of the improved ACGAN framework is divided into three parts, that is, generator loss L_A, discriminator loss L_D, and classification loss L_C, respectively.

$$\begin{aligned}L_A &= -E_{k\sim u_k}[D(A(k),c)],\\ L_{gu} &= E_{i\sim u_{\text{data}}}[D(i,c)] - E_{k\sim u_k}[D(A(k),c)]\\ &\quad + \lambda E_{\hat{i}}\sim u_{\hat{i}}\left(\|\nabla D(\hat{i})\|_2 - 1\right)^2,\\ L_C &= E_{c\sim U_{\text{data}}}[\log_2 D(c)] + E_{c\sim U_k}[\log_2(1-D(A(c)))],\end{aligned} \tag{9}$$

where the generator and discriminator must meet the 1-Lipschitz condition, that is, $D_{m\,L}\leqslant 1$, and $A_{m\,L}\leqslant 1$.

3.2. Improved ACGAN Structure. The improved ACGAN model framework is shown in Figure 2.

The deconvolution layer adopts batch normalization and ReLU activation function, and the output deconvolution layer adopts tanh activation function. The 100-dimensional random noise k and 4-dimensional label c are connected to the input generator, and the dimension expansion is realized through 3-layer deconvolution and then input to the self-attention layer. The feature details are enriched by calculating the self-attention feature map, and then the samples are output after two layers of deconvolution.

The discriminator model adopts a structure symmetrical to the generator model. The output layer uses the softmax activation function to classify the data. To adapt to the GP gradient penalty term, the discriminator removes spectrum normalization and batch normalization. For each convolution layer, LeakyReLU is used as the activation function, and dropout is added to reduce the calculation parameters of the model and alleviate overfitting.

3.3. Diagnostic Training Steps. The ACGAN-based data enhancement framework proposed in this paper is used for attack sample diagnosis. The process is shown in Figure 3.

(1) The attack samples are obtained from the experiment, preprocessed, and normalized to obtain the actual dataset. By establishing the mapping relationship between the noise sample distribution u_k (k) and the actual sample distribution u_{data} (i), the generator will generate a batch of sample data mixed with the actual attack samples and send them to the discriminator. The discriminator discriminates between true and false and backpropagates the gradient information to update the parameters of the network.

(2) As a round of training process, the above steps update the generator once after updating the discriminator z times. The two update alternately until they reach Nash equilibrium.

(3) Use the sample data generated in step (2) to expand the original unbalanced dataset, obtain the balanced sample dataset, and send it to the classifier for diagnosis.

4. Design of Intrusion Detection Platform

4.1. Establishing Database Intrusion Detection Model. Because the designed intrusion detection system pays attention to real-time intrusion monitoring, setting up a database intrusion detection model is necessary. The core of the model is a hybrid detection engine, which has the functions of anomaly detection and misuse detection. The audit data can be transferred to the intrusion detection platform for real-time audit and reanalysis. Judge whether the data are expected, abnormal, or attacked, respond to the operation results, and report to the administrator. The management personnel carries out the subsequent processing. The detection model based on this is shown in Figure 4.

As can be seen from Figure 4, the functions of the main components of the detection model are as follows. In the event generation function, the detection log needs to wait for the generation of detection records before data collection, but the detection records are created and stored in the detection log. Extracting detection records from the database can realize the parallelization of data detection and data acquisition. The anomaly detection unit and intrusion detection unit use the serial mode of detection to read the data from the data collector, respectively, and then detect in combination with the rules in each detection rule base. The behavior pattern rule database is the exception detection storage module, which can generate and gradually update the behavior pattern of normal users according to the data mining algorithm of association rules. The recorder can cache the action results generated by the intrusion detection unit and the anomaly detection unit. The alarm can take the abnormal behavior detected by the intrusion detection unit and the abnormal detection unit as the alarm signal and send it to the reflection platform. The alarm takes corresponding actions according to the abnormal behavior.

4.2. Setting Up Database Security Mechanism Based on Cloud Computing. Cloud computing can identify all kinds of information in the database and establish the security mechanism of the database. Firstly, the security mechanism of the intrusion detection system of the database includes a configuration layer, which can ensure that the data can be accessed only with appropriate authorization. Secondly, the database's security principal can connect to the server and request access or control one or more database objects after passing the security account authentication. Because multiple databases created by different users are often stored on one server, even if a user passes the security account authentication, it is impossible to access all databases, which further limits the user's access scope and operation type. Therefore, database security is realized through an authorization mechanism. Only the owner of the database can access the objects in the database, which also plays an important role in the security and stability of the database. Unauthenticated user connection requests need to be authenticated using Windows authentication.

4.3. Designing the Main Functions of the Database Intrusion Detection Platform. The anomaly detection unit is designed based on relevant rules. Using data mining algorithm, the user's behavior can be preliminarily detected and stored in the behavior pattern rule base in the form of rules. In the learning stage, the influencing factors of rule generation include support and confidence. In the detection stage, the factors affecting rule generation also include generating abnormal data. Security experts create the rules of the rule base based on experience and detection strategy. Disk space management can be configured in the space management module. The space management module can display disk usage, space used value, and free space value. Set the number of records stored in the event library simultaneously. You can adjust the amount of data recorded in the event library

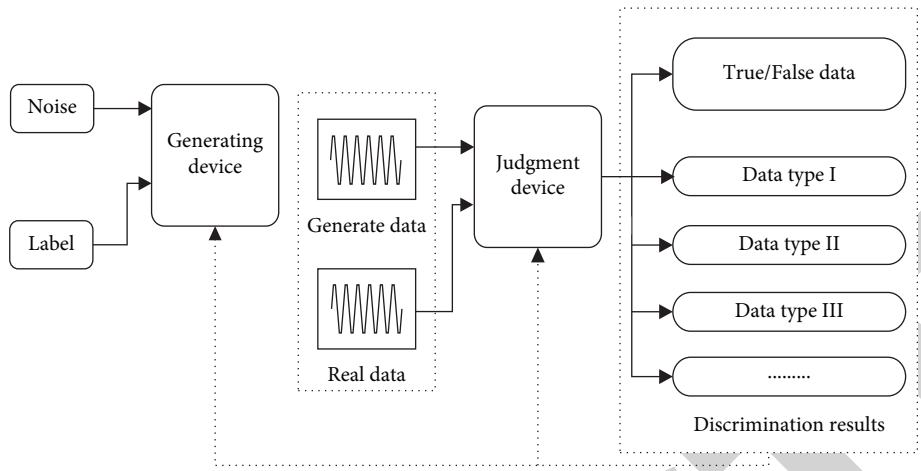


Figure 2: Improved ACGAN framework.

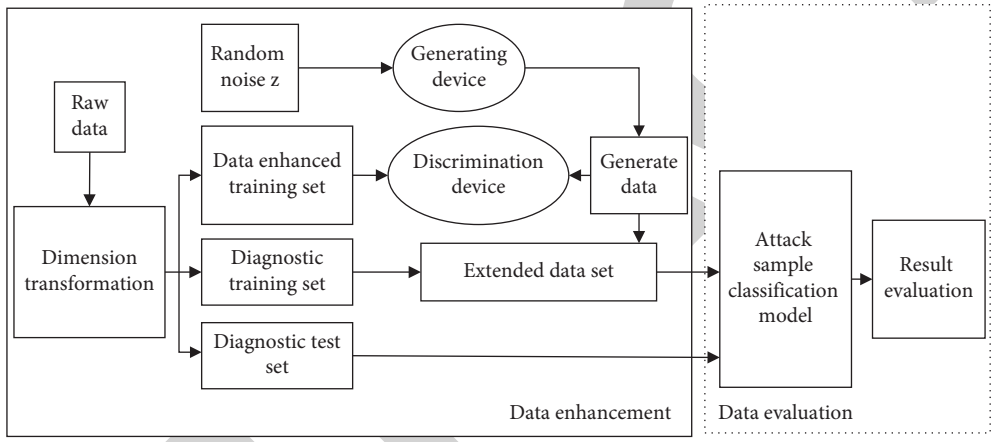


Figure 3: Fault diagnosis process.

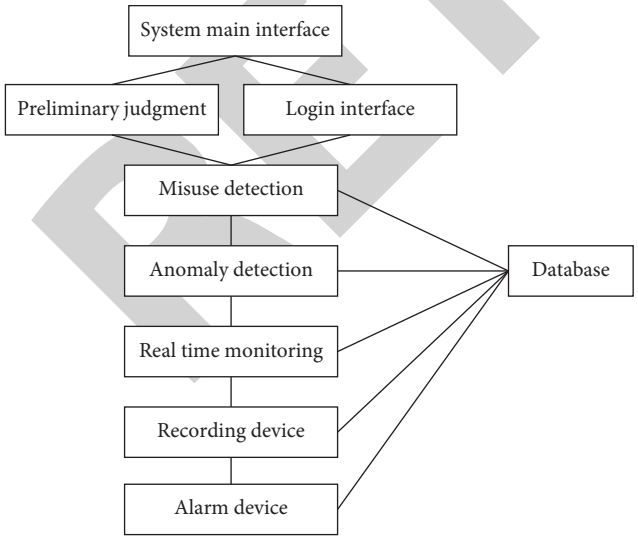


Figure 4: Database intrusion monitoring model.

between the maximum upper limit and the maximum lower limit. The detection and maintenance module can query the status of historical events in the database's intrusion detection time and anomaly detection results and count the times of each intrusion or anomaly in a specific unit time.

4.4. Realizing Database Intrusion Detection. Considering the future upgradeability and maintainability of the system and the portability, the system designed in this paper adopts graphical user interface (GUI). The interface of database intrusion detection system is divided into login interface and main interface. To create a graphical user interface, first create a framework and add various Swing components based on the framework. Before adding components, you need to get the ContentPane container of JFrame first and then add all components. The login interface requires the system administrator to enter the correct user name and login password to enter the main interface to ensure system security. The menu bar is mainly used for real-time monitoring, detection and maintenance, window configuration management, and attack information transmission. At present, the mining technology based on Boolean association rules can only be used in a transactional database. Therefore, numerical association mining technology is more widely used than Boolean association rules. When studying related association rules in a relational database, the database

can contain binary attributes and many classifications or numerical attributes. To realize data mining, we first convert these attributes into Boolean attributes and then map each subset to an entity. Users can use the system by entering the system console. If the display fails to match, it means that the user does not exist or the password is entered incorrectly, and the system console cannot be accessed.

5. Experiment and Analysis

To validate the intrusion detection model, build a simulated experimental environment and use the deep learning framework based on tensorflow-GPU1.13 Keras2.2.4 to simulate. The operating system is Windows10, Intel i5-6300HQ 4-core processor is used, the memory size is 8 GB, and NVIDIA GTX960 graphics card is used to speed up the running speed of GPU.

5.1. Data Digitization and Normalization. The dataset used in the experiment is the UNSW-NB15 dataset, which is the latest dataset in intrusion detection. The dataset was created by the Australian Cyber Security Centre (ACSC) in 2015, which covers a large number of low occupancy intrusion and deeply structured network traffic information. It represents the current network traffic mode and adjusts the training and test sets. It is more suitable for simulating the current complex network environment and getting better test results. The dataset has 9 different types of modern attacks and 49 features. There are 5 more attack types than NSL-KDD, including 2540044 samples. It contains 9 types of attacks: Fuzzers, DoS, Analysis, Reconnaissance, Exploit, Shell code, Worm, Backdoor, and Generic. Each piece of data has 47-dimensional characteristics, one specific attack category identifier, one attack, and a normal category identifier.

(1) The unique heat coding is used for digitizing the character features.

To convert character-type features according to the data set protocol type, service, and status, it is necessary to convert character-type features into numerical features through one-hot encoding. Protocol type includes three categories of TCP, UDP, and ICMP, which are converted to numerical type. The features are three-dimensional features [1, 0, 0], [0, 1, 0], [0, 0, 1]. For service, there are 70 cases, so the values are converted to 70-dimensional features, and for the state, there are 11 cases. Therefore, the values are converted to 11 dimensions. After numerical processing, the whole dataset becomes 130-dimensional numerical features, of which the first 128 dimensions are features. The last two dimensions are class labels.

(2) *Normalization Processing.* After processing the character features, the features in the dataset are divided into continuous and discrete attributes, making the differences between different features extensive. Therefore, it is necessary to normalize the eigenvalues in the dataset to the [−1, 1] interval. In this paper, the min-max standardization method is used for normalization, which only compresses the data. It does not change the original information of the data. The conversion formula is as follows, where $j_{\min}$ and $j_{\max}$ represent the maximum and minimum values of the original eigenvalues, respectively, and y represents the eigenvalues before conversion.

$$j' = \frac{j - j_{\min}}{j_{\max} - j_{\min}}. \tag{10}$$

5.2. Evaluation Index. To verify the detection performance of different models, it is necessary to calculate according to the detection sample category and actual category of the model. This paper mainly uses accuracy (ACC), mean square error (MSE), false-positive rate (FPR), and false-negative rate (FNR) to evaluate the model. It is assumed that n_x represents the actual category of the x-th sample, n_x' represents the detection category of the x-th sample, and the sample set is t. There are w missing events and f false events. When $n_x = n_x'$, it means that the model detection is accurate. Then, the accuracy on the sample set t is

$$\mathrm{ACC} = \frac{1}{t}\sum_{x=1}^{t} L\left(n_x = n_x'\right), \tag{11}$$

where $L(i)$ represents the detection function. When all the detection result categories in the sample set are the same as the actual category of the sample, the accuracy is 1. Mean square error is a method to measure the average value of error and evaluate the change degree of data. The calculation formula is defined as

$$\mathrm{MSE} = \frac{1}{t}\sum_{x=1}^{t}\left(n_x - n_x'\right)^2. \tag{12}$$

The false-positive rate is defined as

$$\mathrm{FPR} = \frac{f}{t}. \tag{13}$$

The underreporting rate is defined as

$$\mathrm{FNR} = \frac{w}{t}. \tag{14}$$

Because of the complexity of network intrusion detection data, it is difficult to define the standard of evaluating the model. Therefore, this paper comprehensively compares the test results of each model through ACC, MSE, FPR, and FNR to verify the accuracy and stability of the model.

5.3. Results and Analysis. Using ACGAN to expand the attack samples of Analysis, Shellcode, Backdoor, and Worm in the training set, respectively, analyze the impact of the expansion proportion of different training sets on the detection rate of a few classes. When the proportion is 0%, 40%, 80%, and 120%, conduct four groups of comparative experiments. The results are shown in Table 1. The experiment shows that the accuracy rate is the highest when the

Table 1: Accuracy of different expansion ratios (%).

Data expansion ratio (%)	Analysis (ACC)	Shellcode (ACC)	Backdoor (ACC)	Worm (ACC)	Overall (ACC)
0	62.22	61.45	60.77	59.45	93.15
40	65.21	65.67	64.55	64.12	95.11
80	67.05	68.87	68.32	75.12	96.55
120	65.66	67.12	68.11	69.37	95.72

expansion ratio is 80%, so 80% is selected for this expansion ratio.

In order to prove the effect of the intrusion detection model, the same training set and test set are selected, and three different algorithms are used to compare with the algorithm in this paper. The comparison of model performance results is shown in Table 2.

In order to verify whether the algorithm performance is improved after ACGAN expands a few samples, it is compared with the algorithms in literature [21], literature [22], and literature [23]. As can be seen from Figure 5, the classification accuracy is improved by 1.39% after supplementing a few samples through the ACGAN model.

Figure 6 compares the mean square error of the algorithms in this paper, literature [21], literature [22], and literature [23]. As can be seen from Figure 6, the mean square error of the algorithm in this paper is the lowest. Compared with the literature [21], it is reduced by 87.36%. Compared with the literature [22], it is reduced by 75.21%. Compared with the literature [23], it is reduced by 39.59%. Therefore, the network intrusion detection model based on this algorithm greatly reduces the error of network intrusion detection.

The same training and test set are selected to verify the advantages of the network intrusion detection model proposed in this paper. The complexity of this model is compared with the CNN, LSTM model, and DBN model. The results are shown in Figure 7. It can be seen from the figure that with the increase of the number of test samples, the detection time of the model in this paper is less than that of LSTM and DBN models, and the time difference gradually increases. Compared with the CNN model, the detection time is slightly higher, but the overall difference is limited. Then, we compare the test results of this method with other machine learning methods, as shown in Table 3.

By comparing with the current commonly used intrusion detection algorithms, it can be seen that some classical machine learning algorithms, such as SVM and KNN, have poor experimental results and high overall false alarm rates. In contrast, the deep learning algorithm is better than SVM and KNN in overall indicators. Still, the detection rate for rare attacks is not high. Compared with other methods, the overall accuracy of the algorithm proposed in this paper is improved by 7.8%, the false-positive rate is reduced by 8.89%, and the false-negative rate is reduced by 12.05%. Also, for rare attacks such as Analysis, Shell code, Backdoor, and Worm, the accuracy rates of this method are 89.21%, 87.48%, 87.21%, and 85.48%, respectively, which are 20.57%, 21.24%, 20.19%, and 30.85% higher than those of other methods. It can be proved that the system performance of this method is excellent and innovative.

Table 2: Model comparison (%).

Model	Accuracy rate	False-positive rate	Underreporting rate
RF	81.41	8.4652	13.1277
PCA-RF	88.72	6.2107	10.2784
SDAE-RF	94.68	2.1988	6.6621
Proposed	98.55	1.2257	3.1028

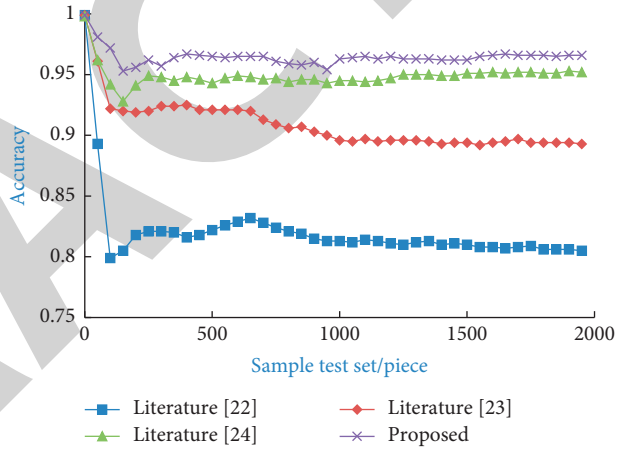


Figure 5: Algorithm accuracy comparison.

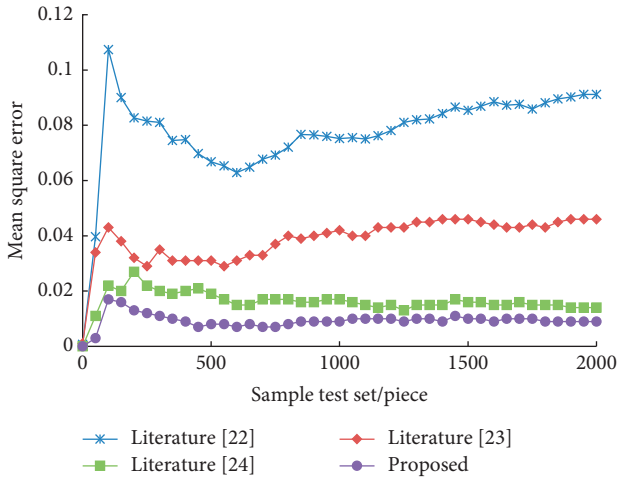


Figure 6: Algorithm mean square error comparison.

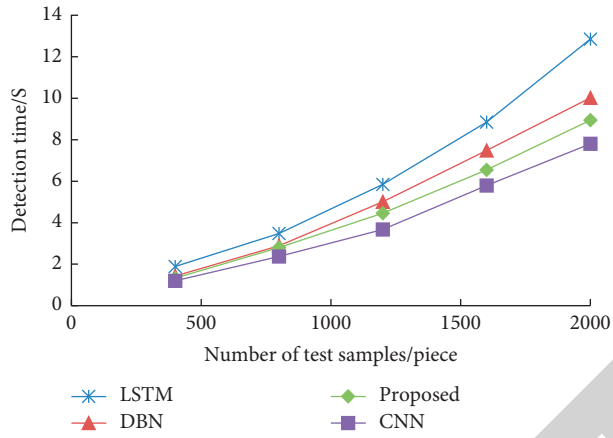


Figure 7: Comparison of detection time under different number of samples.

Table 3: Comparison with other methods (%).

Model	SVM	KNN	CNN	LSTM	DBN	Proposed
Analysis (ACC)	66.44	65.29	69.91	70.43	71.11	89.21
Shellcode (ACC)	61.23	62.24	68.26	69.23	70.26	87.48
Backdoor (ACC)	63.67	63.54	68.88	68.23	70.77	87.21
Worm (ACC)	50.11	51.76	57.25	55.31	58.71	85.48
Accuracy rate	76.65	89.12	93.88	96.24	95.85	98.15
False-positive rate	17.23	17.64	4.61	5.51	3.58	0.82
Underreporting rate	19.16	26.21	6.21	9.29	8.53	1.83

6. Conclusion

Aiming at the problems of network intrusion detection in the era of big data, this paper proposes an intrusion detection platform based on the ACGAN model in big data environment. Firstly, this paper proposes an ACGAN sample enhancement framework based on a two-dimensional convolution structure and introduces self-attention mechanism to expand the data volume of attack samples. The improved ACGAN introduces self-attention mechanism in G and D to fully extract the global features of the samples, so as to improve the generation quality of the model. At the same time, the gradient penalty mechanism is introduced to overcome the problems of gradient disappearance to speed up the convergence of the model. The experimental results show that the intrusion detection model in this paper has achieved good detection accuracy, false-positive rate, and false-negative rate. At present, the model is only tested in the dataset, and the effect is good. It also needs to be tested in the actual network environment to verify the real performance of the model in the actual network environment.

Data Availability

The labeled dataset used to support the findings of this study is available from the corresponding author upon request.

Conflicts of Interest

The author declares that there are no conflicts of interest.

Acknowledgments

This study was supported by Wenhua University.

References

[1] K. Nayak, D. Marino, P. Efstathopoulos, and T. Dumitraş, "Some vulnerabilities are different than others," in *Proceedings of the International Workshop on Recent Advances in Intrusion Detection*, pp. 426–446, Springer, Switzerland, Europe, September 2014.

[2] A. Mishra, K. Nadkarni, and A. Patcha, "Intrusion detection in wireless ad hoc networks," *IEEE Wireless Communications*, vol. 11, no. 1, pp. 48–60, 2004.

[3] R. Gassais, N. Ezzati Jivan, J. M. Fernandez, and D. Aloise, "Multi-level host-based intrusion detection system for Internet of things," *Journal of Cloud Computing*, vol. 9, no. 1, pp. 1–16, 2020.

[4] J. Kim, Y. Shin, and E. Choi, "An intrusion detection model based on a convolutional neural network," *Journal of Multimedia Information System*, vol. 6, no. 4, pp. 165–172, 2019.

[5] A. Mohan, A. K. Singh, B. Kumar, and R. Dwivedi, "Review on remote sensing methods for landslide detection using machine and deep learning," *Transactions on Emerging Telecommunications Technologies*, vol. 32, no. 7, 2021.

[6] A. Javaid, Q. Niyaz, and W. Sun, "A deep learning approach for network intrusion detection system," in *Proceedings of the 9th EAI Inter- national Conference on Bio-inspired Information and Commu- nications Technologies (formerly BIONETICS)*, pp. 21–26, EAI, New York, NY, USA, December 2016.

[7] C. Yin, Y. Zhu, J. Fei, and X. He, "A deep learning approach for intrusion detection using recurrent neural network," *IEEE Access*, vol. 5, pp. 21954–21961, 2017.

Hindawi
Security and Communication Networks
Volume 2024, Article ID 9897316, 1 page
https://doi.org/10.1155/2024/9897316

Retraction

Retracted: Research on Tourism Route Recommendation Strategy Based on Convolutional Neural Network and Collaborative Filtering Algorithm

Security and Communication Networks

Received 8 January 2024; Accepted 8 January 2024; Published 9 January 2024

This article has been retracted by Hindawi following an investigation undertaken by the publisher [1]. This investigation has uncovered evidence of one or more of the following indicators of systematic manipulation of the publication process:

(1) Discrepancies in scope
(2) Discrepancies in the description of the research reported
(3) Discrepancies between the availability of data and the research described
(4) Inappropriate citations
(5) Incoherent, meaningless and/or irrelevant content included in the article
(6) Manipulated or compromised peer review

The presence of these indicators undermines our confidence in the integrity of the article's content and we cannot, therefore, vouch for its reliability. Please note that this notice is intended solely to alert readers that the content of this article is unreliable. We have not investigated whether authors were aware of or involved in the systematic manipulation of the publication process.

In addition, our investigation has also shown that one or more of the following human-subject reporting requirements has not been met in this article: ethical approval by an Institutional Review Board (IRB) committee or equivalent, patient/participant consent to participate, and/or agreement to publish patient/participant details (where relevant).

Wiley and Hindawi regrets that the usual quality checks did not identify these issues before publication and have since put additional measures in place to safeguard research integrity.

We wish to credit our own Research Integrity and Research Publishing teams and anonymous and named external researchers and research integrity experts for contributing to this investigation.

The corresponding author, as the representative of all authors, has been given the opportunity to register their agreement or disagreement to this retraction. We have kept a record of any response received.

References

[1] S. He, "Research on Tourism Route Recommendation Strategy Based on Convolutional Neural Network and Collaborative Filtering Algorithm," *Security and Communication Networks*, vol. 2022, Article ID 4659567, 9 pages, 2022.

Hindawi
Security and Communication Networks
Volume 2022, Article ID 4659567, 9 pages
https://doi.org/10.1155/2022/4659567

Research Article

Research on Tourism Route Recommendation Strategy Based on Convolutional Neural Network and Collaborative Filtering Algorithm

Shan He

Department of Foreign Languages and Tourism, Henan Institute of Economics and Trade, Zhengzhou, Henan 450000, China

Correspondence should be addressed to Shan He; happy9262022@163.com

Received 2 March 2022; Revised 3 April 2022; Accepted 12 April 2022; Published 7 May 2022

Academic Editor: Fang Liu

With improving people's living standards, tourism has become essential leisure and entertainment. At present, it has begun to shift from a quantity-oriented tourism method to a quality-oriented tourism method. It is difficult for passengers to choose the route that suits them from the numerous routes. Given the above problems, this study proposes a travel route recommendation algorithm that combines a convolutional neural network and collaborative filtering. The algorithm uses a convolutional neural network to extract the latent features in the customer and travel itinerary data and then uses the matrix factorization method based on collaborative filtering to perform score prediction. The experimental results show that the algorithm can meet the travel requirements of different customers. At the same time, the recommendation accuracy of the tourist route is improved, and technology and method are provided for realizing the personalized recommendation service of the tourist route.

1. Introduction

At present, the introduction of various tourism products has made the amount of tourism information extremely large, and it is difficult for users to quickly locate the products they are interested in from a large amount of tourism information [1]. In order to compete for tourists and increase revenue, travel companies need to continuously meet the needs of tourists and formulate travel routes that meet the interests of tourists [2]. Tourism recommendation system is an essential means to solve the problem of tourism information overload. It can actively push tourism routes that meet tourists' interests and help them make decisions quickly [3].

Tourist route recommendation algorithms mainly include four categories: content-based recommendation, collaborative filtering-based recommendation [4], knowledge-based recommendation, and social media-based recommendation [5]. Content-based travel route recommendation recommends similar routes to tourists based on the travel products they choose [6]. Recommend optional tours for tourists for a limited time. Tourist route recommendation based on collaborative filtering recommends the routes selected by tourists with similar interests according to the tourists' route preferences [7]. Knowledge-based travel route recommendation introduces tourism domain knowledge into the route recommendation system to improve the accuracy of route recommendation [8]. Travel route recommendation based on social media introduces the tourist relationship in social media into the route recommendation process [9].

The current route recommendation is generally based on the location of tourists, using geographic information systems and mobile devices to recommend surrounding routes or places [10]. But since tourist travel is often limited by climatic time, and users' interests also change, time is crucial for route selection [11]. Literature [12] recommends routes based on spending the least amount but reaching more destinations within a certain period. Literature [13] designed a personalized similarity model and used the user's heterogeneous travel information to make recommendations at a specific location at a particular moment. Literature [14] uses a time-dependent network to solve the problem of

random changes in the number of tours and attractions and selects the next attraction through conditional probability. Literature [15] proposed a time-sensitive travel route recommendation method based on dynamic transition graphs. Literature [16] designed a two-step greedy heuristic algorithm to predict the next destination. It considers space-time conflicts and solves the problem of sparse data. Literature [17] proposed a multiconstraint K-greedy algorithm based on the opening hours of scenic spots, ticket GIS coordinates, scenic spot evaluation information, etc., which can recommend better tourist routes for tourists. However, in the actual route selection process, whether a user will select a route is often affected by the theme of the route and the user's interest [18].

With the rapid development of smart mobile devices and the Internet, the problem of tourist information overload has emerged. Let tourists spend a lot of time and energy screening travel information, significantly reducing customer travel medical examination. The emergence of a travel recommendation system can assist tourists to quickly and accurately select resources that match their needs from the overloaded information. This study proposes a travel route recommendation algorithm integrating convolutional neural networks and collaborative filtering. The algorithm first converts the user comment data into words and extracts the hidden features in the user and travel route data through a convolutional neural network. Then, the collaborative filtering recommendation based on users and travel routes is completed. The algorithm can recommend scientific and reasonable travel routes for users to meet their travel needs in different situations.

2. The Algorithm Proposed in This Study

2.1. Problem Description. The collaborative filtering algorithm mines the hidden features of tourists or tourist routes according to the data of tourists' interest and preference for tourism. Then its correlations are calculated and score predictions are made. Finally, a recommendation is generated. In general, data is often very sparse. The current collaborative filtering is difficult to extract the deeply hidden features in the data.

For example, suppose there are w tourists and t travel routes. The sample data is in the form of a 4-tuple (userx, itemy , c_{xy}, r_{xy}), where r_{xy} represents the rating of tourists x on the tourist route y, which is an integer value from 1 to 5. c_{xy} represents the comment of tourist x on the tourist route y, which is a piece of text with different lengths. R is an $w * t$ rating matrix and C is an $w * t$ review matrix, where $r_{xy} \in R^{w \times t}, c_{xy} \in C^{w \times t}$, as shown in Table 1.

In Table 1, each row represents the ratings and reviews published by a tourist. Each column represents the ratings and reviews received by a tourist route. ? means no rating comment information. The matrices R and C can be obtained from Table 1.

Therefore, the problem to be solved in this study is to integrate the convolutional neural network into the collaborative filtering algorithm based on the rating matrix $R^{w \times t}$ and the comment matrix $C^{w \times t}$, Mining hidden features of tourists and tourist routes and predicting tourists' ratings for unrated routes.

Table 1: Rating and comment data.

User	Item			
	Item_1	Item_2	...	Item_w
User_1	r_{00}, c_{00}	?	?	?
User_2	?	r_{22}, c_{22}	?	?
...	?	?	r_{xy}, c_{xy}	?
User_w	?	?	?	?

2.2. Collaborative Filtering Model Design. The collaborative filtering algorithm model that integrates the convolutional neural network preprocesses the data, including removing invalid data and retaining comment and rating data. Then, each travel itinerary merges all its review data separately for each tourist and average the rating data. Then, the combined review data is converted into a vector-based on the text vectorization technology. The vectorized tourist and tourism data are sent to the convolutional neural network for training. Based on the convolutional neural network, the latent features of all comments of the tourist user x are extracted as the latent feature representation p_x of the tourist. Similarly, extract a particular travel route item, the implicit features of all reviews, as the feature representation q_y of the item. Then, based on the matrix decomposition method in collaborative filtering, the inner product of the transpose of p_x and q_y is performed to obtain the predicted score $r_{xy}^{'} = p_x q_x^T$. Finally, the Adam optimization method is used to train the model to minimize the error between the predicted score $r_{xy}^{'}$ and the real score r_{xy}.

The model structure is shown in Figure 1, including the input layer, convolution layer, pooling layer, fully connected layer, and output layer. The input layer receives the vectorized review text as the input feature x, and the average score as the input feature y. The convolution layer performs convolution calculation on the input features by sliding the convolution kernel and obtaining the feature map. The pooling layer uses the maximum pooling method to reduce the dimension of the feature map calculated by the convolution layer and retains the more essential features in the network. The fully connected layer maps the learned latent features to the sample space then passes to the output layer to generate the output.

The model is divided into upper, middle, and lower parts (see Figure 1): tourist submodel, matrix decomposition model, and tourist route submodel, respectively. The input data format of the tourist sub-sub-model is $(vec_x^{user} \bar{r}_x^{item})$, which is regarded as a multiclassification problem. A 5-class prediction is made on the review data vector of a tourist. The category is $\bar{r}_x^{user}$ and is extracted from the fully connected layer during the training process as the latent feature r_x. The input data format of the travel route submodel is $(vec_x^{item}, (\bar{r}_x^{item})$ which is also regarded as a multiclassification problem. That is, the comment vec y, of an item is used for 5-category prediction. The category is $\bar{r}_x^{item}$, and during the training process, the hidden feature q_x of the tourist route is

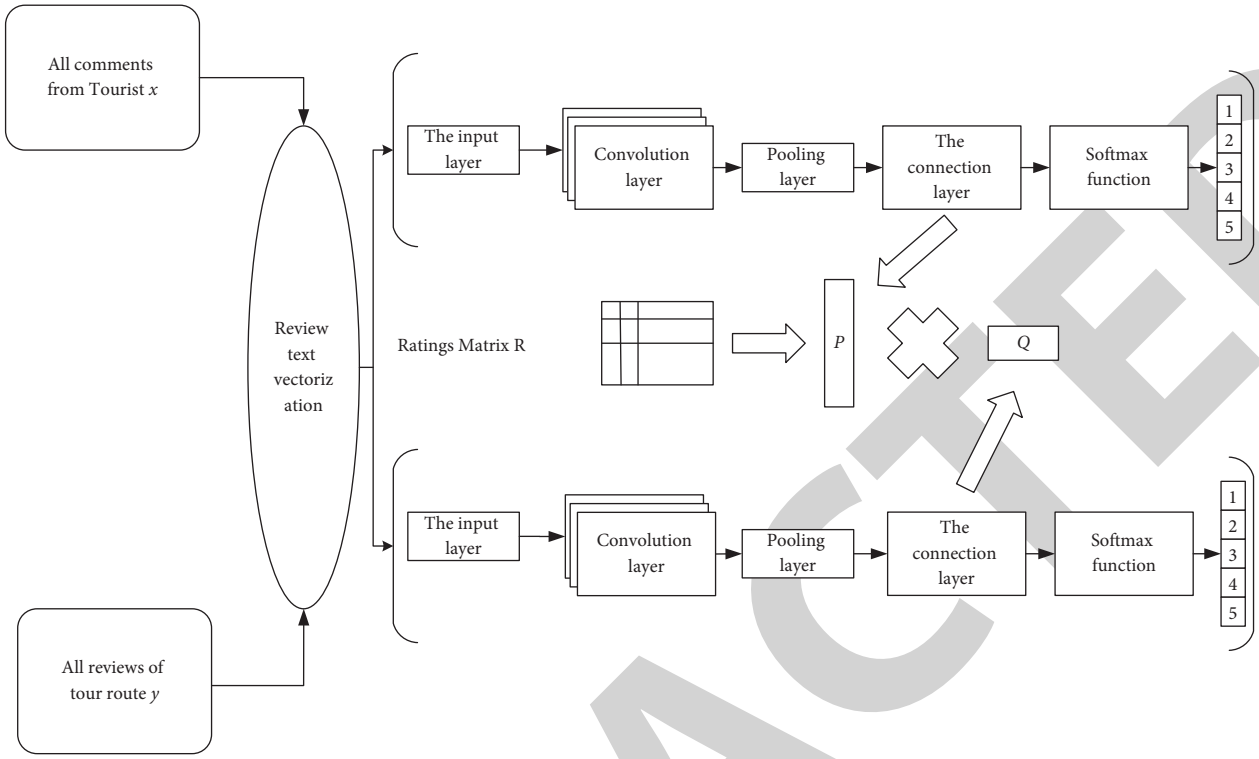


Figure 1: Structure of LSTM network.

extracted from the fully connected layer. The middle part is the matrix decomposition submodel, which takes the latent features p_x of tourists learned in the submodel of tourists and the latent features q_x of items learned in the submodel of tourist routes as inner products. Get the predicted score $r'_{xy} = p_x q_y^T$. Based on the Adam optimization method training, the whole model and the submodel minimize tourists. The prediction error of the travel route submodel and matrix factorization model calculates the error between the predicted score r_{xy}' and the real score r_{xy}.

Score prediction is realized based on nonnegative matrix factorization (NMF). The matrix $R \in R_+^{w\times t}$ is decomposed into two submatrices $W \in R_+^{w\times z}$ and $T \in R_+^{z\times t}$ by NMF. All $R, w,$ and t, terms are on negative terms because the following relationship can be derived: $R \approx \mathrm{W} \times \mathrm{T}$. In the context of recommender systems, $R_+^{w\times t}$ represents an $m * t$ nonnegative matrix. W can be understood as a tourist route. T is the latent factor. Z is the number of nondecomposable factors of R. In real recommendation problems, there are no negative terms (travel routes, tourists, ratings). The nonnegative constraints on W and T improve the interpretability of the collaborative filtering system.

The NMF is initialized based on the tourist route latent factor. The goal of the model is to find two lower-ranked nonnegative matrices $W_{Iq} \in R_+^{w\times z}$ and $T \in R_+^{z\times t}$ to predict ratings, calculated as $R = W_{Iq}T$. Set up a constraint between R and $W_{Iq}N$ as the objective function.

$$\left\|R - W_{Iq}T\right\|^2 = \sum_{px}\left(R_{px} - \left(W_{Iq}T\right)_{px}\right)^2. \tag{1}$$

In the formula, W_{Iq} represents the latent factor matrix initialized based on the contextual features of the tourist route.

Overfitting may occur in the prediction process, so the F-norm regular term is added to the objective function, and the objective function is rewritten as

$$\begin{aligned} &\frac{1}{2}\rho_w \sum_t^w \left(W_{Iq}\right)_{p2} + \frac{1}{2}\rho_t \sum_t^T T_{x2}, \\ &R - W_{Iq}T^2 = \sum_{px}\left(R_{px} - \left(W_{Iq}T\right)_{px}\right)^2 +, \end{aligned} \tag{2}$$

where ρ_w is the regular term of feature vector $(W_{Iq})_p$ and ρ_t is the regular term of T_x.

The eigenmatrices W_{Iq} and T are obtained by minimizing the objective function. The mathematical model is defined as

$$(W, T) = \min\left\|R - W_{Iq}T\right\|^2, \tag{3}$$

where $W > 0$ and $T > 0$.

Initialize the matrix T to a random matrix of size $z \times t$: $T = \mathrm{random}^{z\times t}$, where z is the minimum factor of the rating matrix. Calculate the minimum value of the objective function by iteratively updating W and T. The mathematical formula of iteration is

$$W_{pz} \leftarrow W_{pz}\frac{\left(T^N R\right)_{pz}}{\left(T^N T W_{Iq}\right)_{pz}},\ T_{zx} \leftarrow T_{zx}\frac{\left(W_{Iq}^N R\right)_{zx}}{\left(W_{Iq}^N W_{Iq} T\right)_{zx}}. \tag{4}$$

Inputs: the scoring matrix R of the dataset, the maximum number of iterations Maxiter, the threshold.
Output: feature matrices W and T.

(1) Preprocess auxiliary information of tourist routes to obtain sentence matrix.
(2) Use CNN to extract the feature vector of the sentence matrix.
(3) Initialization: $T = \text{random}_{z\times t}, W = I_q = W_{Iq}$.
(4) for z from 1 to Maxiter do /* Minimize the objective function $\min\|R - WT\|^2, W \geq 0, T \geq 0$*/
(5) for p from 1 to W do
(6) $W_{pz} \leftarrow W_{pz}(T^N R)_{pz}/(T^N T W_{Iq})_{pz}$.
(7) endfor
(8) for x from 1 to T do
(9) $T_{zx} \leftarrow T_{zx}(W_{Iq}^N R)_{pz}/(W_{Iq}^N W_{Iq} T)_{pz}$.
(10) endfor
(11) Rerr = $RMSE(R - WT)^2$// Calculate the objective function
(12) if Rerr < threshold
(13) Break
(14) Endif.
(15) Endfor.
(16) Return.

Algorithm 1: Recommendation algorithm based on nonnegative maximal matrix.

The predicted rating of tourist p for tourist route x can be calculated as

$$R'_{px} = W_p T_x. \tag{5}$$

In the formula, R'_{px} is the predicted score.

Algorithm 1 summarizes the algorithm of the recommendation system in this study. The algorithm iteratively updates the two latent factor matrices W and T until convergence is achieved.

2.2.1. Text Vectorization. Text vectorization uses word embedding to map text to w-dimensional vectors. First, for each tourist, all the review data are merged separately for each travel itinerary and average their scores. The raw data is processed into visitor review rating data and item review rating data. The user data format is as follows.

$(\text{user}_x, c_{x0} \oplus c_{x1} \oplus \cdots \oplus c_{xt}, 1/t \sum_{j=1}^{t} r_{xy}$, the travel route data format is: $\text{item}_x, c_{0y} \oplus c_{1y} \oplus \cdots \oplus c_{wy}, 1/w \sum_{x-1}^{w} r_{xy})$, where $\oplus$ means that the text is concatenated with spaces. Arrange the above formula as formulas (6) and (7).

$$\left(\text{user}_x, d_x^{\text{user}}, \bar{r}_x^{\text{user}}\right), \tag{6}$$

$$\left(\text{item}_y, d_y^{\text{item}}, \bar{r}_y^{\text{item}}\right), \tag{7}$$

where d_x^{user} represents all the reviews of tourist user_x on $\text{item}_1 \sim \text{item}_t$ and $\bar{r}_x^{\text{user}}$ represents the mean of all ratings of tourist user_x on $\text{item}_1 \sim \text{item}_t$. Then, based on the text vectorization technique, the merged review data is represented by a vector as vec_x^{user}. It is defined as formulas (8) and (9).

$$vec_y^{\text{user}} = Doc2VecC\left(d_x^{\text{user}}\right), \tag{8}$$

$$vec_y^{\text{item}} = Doc2VecC\left(d_y^{\text{item}}\right), \tag{9}$$

where the Doc2VecC function returns a w-dimensional vector, which represents each document d_x^{user} as a simple average of word embeddings, and ensure that the generated vector representation can capture the semantic information of the document during training learning. After text vectorization, the sample data of tourist x can be expressed as

$$\left(\text{user}_x, vec_x^{\text{user}}, \bar{r}_x^{\text{user}}\right). \tag{10}$$

The data of travel route y is represented as

$$\left(\text{user}_x, vec_x^{\text{user}}, \bar{r}_x^{\text{user}}\right). \tag{11}$$

2.2.2. Convolutional Layer. The convolutional layer is the core of the convolutional neural network, which is used to perform convolution calculations on the input sample features and extract important features. In the model in this study, the convolution layer receives the text vectors vec_x^{user} and vec_x^{item} of user $user_x$ to tourist route $item_y$ as input features. Then perform operation reshape on it and convert it to the size of $k * k$, where $k * k = m$. Suppose there are t neurons in the convolution layer, and each neuron n passes through the sliding convolution kernel F_n. Perform convolution calculations on the input samples and obtain new feature maps. The convolution kernel is also called a filter. The convolution computation in each convolution kernel slides across the width and height of the input data. Calculate the inner product of the entire convolution kernel and the input data anywhere. Assuming that the size of the convolution kernel is s, that is, $F_n \in R^{s\times s}$, the nth feature map can be calculated by the following formula:

$$w_n = f\left(vec_x^{\text{user}} * F_n + h_x\right). \tag{12}$$

Among them, $*$ represents the convolution calculation, h_x represents the bias term, which is a real number, and f is a nonlinear activation function. It can introduce nonlinear

factors into the model and solve the problem that linear models are difficult to represent as features. Commonly used activation functions are Sigmoid function, Tanh function, and ReLU function. The calculation formulas of the three activation functions are as follows:

$$\begin{aligned} \mathrm{Re}LU(i) &= \max(0, i), \\ Tanh(i) &= \frac{e^{i} - e^{-i}}{e^{i} + e^{-i}}, \\ \mathrm{Sigmoid}(i) &= \frac{1}{1 + e^{-i}}. \end{aligned} \tag{13}$$

2.2.3. Pooling Layer. The pooling layer is mainly used to reduce the dimension of the feature map calculated by the convolution layer. Retain the more essential features in the network while controlling the "overfitting" phenomenon to a certain extent. Suppose the feature graph $W_n = \{w_1, w_2, \ldots, w_{k-s+1}\}$ is obtained in the n-th convolution layer. The maximum pooling takes the maximum value in W_n, and u_n represents the pooling result of the n-th convolutional layer, which is given by

$$u_n = \max(W_n) = \max\{w_1, w_2, \ldots, w_{k-s+1}\}. \tag{14}$$

2.2.4. Fully Connected and Output Layer. The fully connected layer receives the output of the pooling layer. Suppose there are w neurons in the fully connected layer. After the fully connected layer ReLU activation function, a fixed-size vector p_x is obtained, which is the implicit feature of the tourist user $_x$. Similarly, the implicit feature vector q_y of the tourist route item $_y$ can also be obtained. The calculation formula is as follows:

$$\begin{aligned} q_y &= \mathrm{Re}LU\left(m_{\mathrm{item}_y} P_{\mathrm{item}_y} + h_{\mathrm{item}_y}\right), \\ p_x &= \mathrm{Re}LU\left(m_{\mathrm{user}_x} P_{\mathrm{user}_x} + h_{\mathrm{user}_x}\right), \end{aligned} \tag{15}$$

where $p_x, q_y \in R^w$, P_{user_x} and P_{item_y} represent the pooling layer outputs of the tourist and tourist route submodels, respectively. m_{user_x} and m_{item_y} are the weights of the fully connected layers of the tourist and tourist route submodels, respectively, and h_{user_x} and h_{item_y} are the corresponding biases.

2.2.5. Matrix Factorization. Matrix decomposition uses matrix multiplication to decompose the user-item rating matrix into two low-dimensional user feature matrices and item feature matrices. In the model-based collaborative filtering algorithm, the model of tourists and tourist routes is constructed. From historical data such as ratings of tourists and tourist routes, learn the feature matrix of users and the feature matrix of items. Then the two feature matrices are multiplied to get the predicted score matrix. Finally, fit the predicted score matrix and the actual score matrix.

This study constructs a tourist submodel and an item submodel based on the convolutional neural network. From the reviews posted by tourists and all the reviews received by the tourist routes, the latent features p_x of tourists and the latent features q_y of tourist routes is learned. Then calculate the inner product of the implicit feature matrix of tourists and the implicit feature matrix of the tourist route. The predicted score matrix $r'_{xy} \in R$ is obtained, and the calculation formula is as follows:

$$r'_{xy} = p_x q_y^N. \tag{16}$$

Fit the predicted score and the actual score by the Adam optimization method. For tourist routes with ratings, make their predicted ratings as close to the actual ratings as possible. From this, it can be assumed that an unrated tour will have an actual rating close to the predicted rating. The calculation formula is shown in the below formula.

$$r_{xy} \approx r'_{xy} = p_x q_y^N. \tag{17}$$

3. Experimental Results and Analysis

3.1. Dataset. The travel data comes from a travel company owned by an airline. It includes 25,714 travel records of 4,731 tourists on 1,439 tourist routes, and each tourist contains at least three routes that they have participated in. Each record includes tour group number, tourist name, gender, ID number, line departure time, line price, and detailed introduction to attractions. It is an implicit feedback dataset. As long as a tourist has participated in a certain route, it is considered that the tourist likes this route. The dataset is split into a training set (train), a validation set (validation), and a test set (test) in a ratio of 7 : 2 : 1. The training set is used to train the model, the validation set is used for parameter selection, and the test set is used to evaluate the model.

3.2. Evaluation Indicators. This study uses Precision, Recall, F1 value, and Normalized Discounted Cumulative Gain (NDCG) as the algorithm evaluation criteria.

Precision: The recommendation accuracy refers to the ratio of the number of travel routes that tourists like to the total number of recommended travel routes among the recommended travel routes.

$$\mathrm{Precision} = \frac{\sum_{p \in P} |R(p) \cap N(p)|}{\sum_{p \in P} |R(p)|}. \tag{18}$$

In the formula, $R(p)$ represents the list of recommended items for tourist p according to the behavior of tourist p on the training set, and $N(p)$ represents the list of items that tourist p likes on the test set.

Recall rate (Recall): The recall rate of the recommendation system represents the ratio between the number of travel routes that tourists like among the recommended travel routes and the number of travel routes that tourists like. The calculation process of the recall rate is as follows:

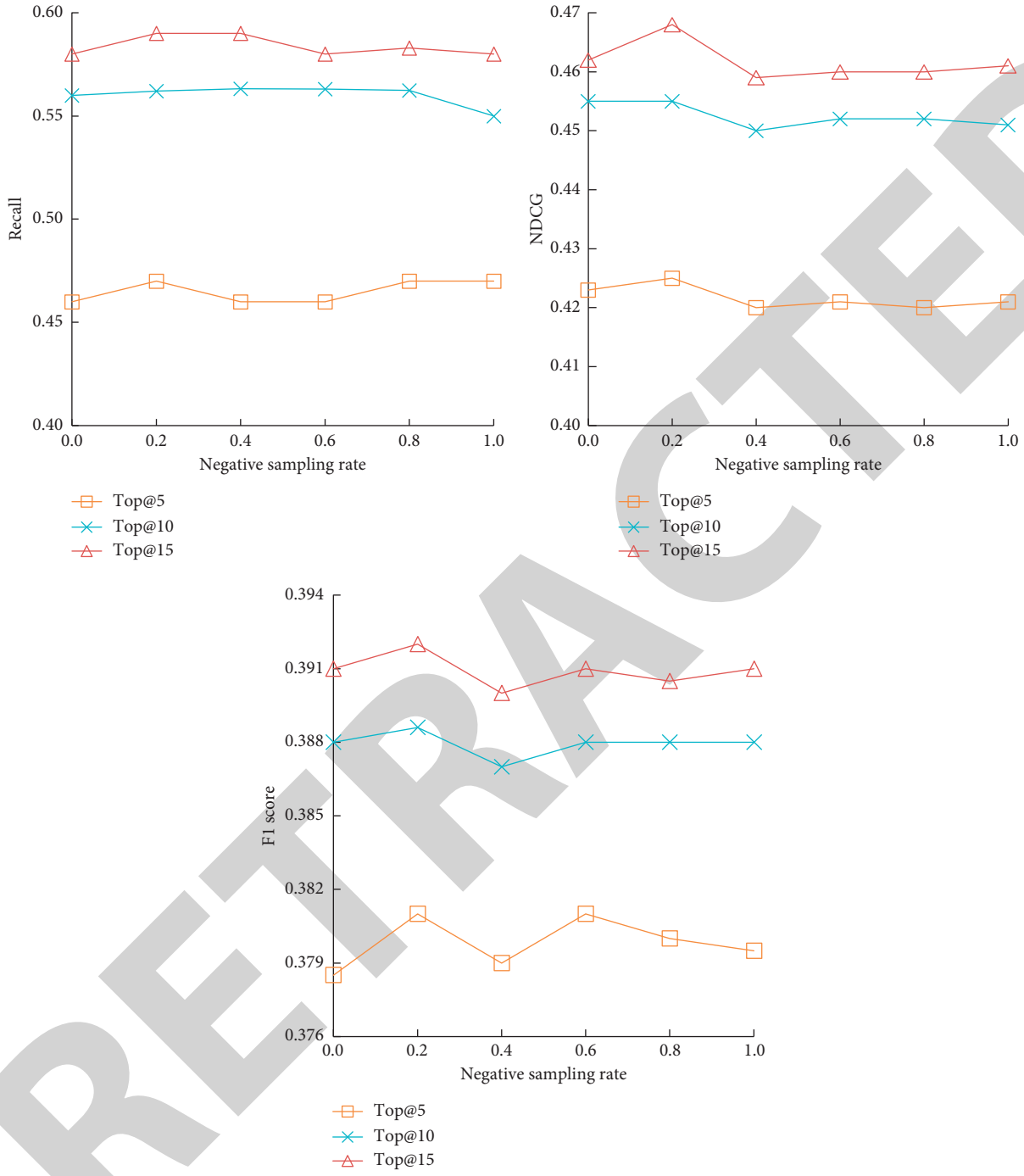


Figure 2: Effect of negative sampling rate.

$$\text{Recall} = \frac{\sum_{p \in P} |R(p) \cap N(p)|}{\sum_{p \in P} |N(p)|}. \tag{19}$$

F1 score: It is a comprehensive index of precision and recall. The larger the value of F1, the better the algorithm's performance. The F1 value is defined as follows:

$$F1 = \frac{2 \times \text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}}. \tag{20}$$

NDCG@K is used to sort the predicted probability value of each travel route in the recommended list. If the predicted probability value of the top travel route in the recommended list is more significant, the greater the value of NDCG, the better the recommendation effect of the model.

$$NDCG@K = \frac{1}{|P|} \sum_{p \in P} NDCG_p@K, \tag{21}$$

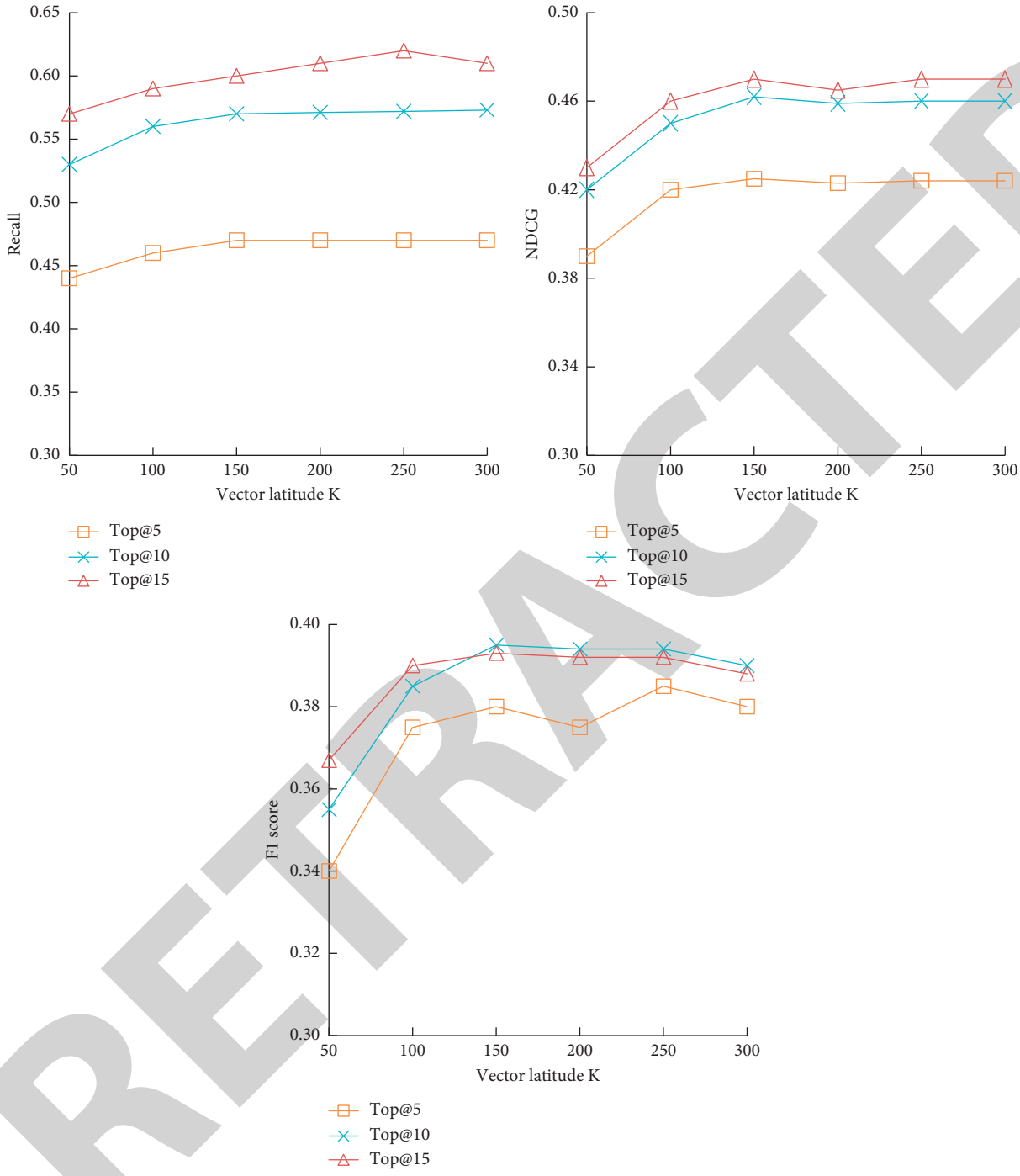


Figure 3: Effect of dimension size.

where P represents the number of tourists in the test set and $\sum_{p \in P} TDCA_p@K$ is the sum of the NDCG values of each tourist.

3.3. Parameter Training

3.3.1. Effects of Negative Sampling Rates. The negative sampling rate indicates how many disliked items are sampled for each traveler. At a fixed negative sampling rate, the number of disliked lines sampled for each tourist is different. The larger the negative sampling rate, the more unfavorable routes are sampled for the same tourist. There are many negative samples in the optimization process. If the value of the negative sampling rate is smaller, the number of lines that are not liked is extracted, and there will be fewer negative samples. Therefore, it is discussed in the experiment how many negative samples are drawn for each tourist, making the model perform the best. The grid search method is used in the experiment, and the negative sampling rate is

Table 2: Comparison of the proposed with other methods.

Method	Recall			NDCG			F1 score		
	Top@5	Top@10	Top@15	Top@5	Top@10	Top@15	Top@5	Top@10	Top@15
Proposed	0.508	0.564	0.596	0.469	0.497	0.506	0.405	0.418	0.419
Literature [19]	0.491	0.545	0.584	0.452	0.483	0.493	0.385	0.407	0.405
Literature [20]	0.472	0.531	0.582	0.446	0.465	0.475	0.382	0.394	0.407
Literature [21]	0.467	0.526	0.551	0.425	0.446	0.457	0.376	0.383	0.389

selected according to the algorithm's performance. With fixed regularization parameters and latent factors, the search range for negative sampling rates is {0.0, 0.2, 0.4, 0.6, 0.8, 1.0}, and the performance results are shown in Figure 2.

It can be seen from Figure 2 that as increases, the three evaluation indicators of Top@5, Top@10, and Top@15 first increase and then decrease, later tend to remain unchanged. The results confirm that the model performance first increases and then decreases as the number of negative samples increases. The larger the number of negative samples, the slower the model's training will be. Therefore, to balance model performance and efficiency, the negative sampling rate is taken as 0.2.

3.3.2. Influence of Vector Dimension. The vector dimension represents the length of the latent features of tourists and travel itineraries. The larger the vector dimension, the richer the information representation of tourists and tourist routes, but the more significant computation. The smaller the vector dimension, the less accurate, but the faster the learning speed. Therefore, in the case of balancing accuracy and calculation amount, a more appropriate dimension size is generally set through experiments. Set the vector dimension search range to {0, 20, 40, 60, 80, 100}, and the experimental results are shown in Figure 3. It can be seen from Figure 3 that with the increase of vector dimension, the NDCG and F1 indicators proliferate. When the vector dimension reaches more than 40, the growth rate slows down, and the algorithm performance tends to be stable. The growth of the Recall indicator is not as dramatic as that of NDCG and F1, but it still increases first and then decreases. After reaching 40, the growth rate slows down, so the vector dimension is taken as 40.

3.4. Experimental Results and Comparative Analysis. To further illustrate the effect and prediction performance of the algorithm in this study, the algorithm in this study is compared with other traditional recommendation algorithms. The performance comparisons of the four algorithms in Recall@K, NDCG@K, and F1 are shown in Table 2.

It can be seen from Table 1 that as N increases, Recall@K, NDCG@K, and F1@K all increase. Among them, the growth rate of Recall@K is particularly obvious. Such results validate the fact that in reality, the more routes are offered to tourists, and the more routes will be chosen to satisfy tourists' interests. However, there are many recommended routes, and the routes that tourists are most interested in may not always be at the top of the recommended list. Based on the two methods of network representation learning, the results of our algorithm and literature [19] are better than that of literature [20] and literature [21]. This is because the network representation learning method is used to learn route and passenger vector representation, making better data information. A good uniform representation is obtained. It is difficult for literature [20] and literature [21] to fuse and fully utilize this information. The proposed is better than literature [19]. It shows that using the word vector method to add information about the co-occurrence of tourists, common liking of route pairs, and a shared dislike of route pairs can get a better vector representation of routes and passengers. However, literature [19] only utilizes the feature information of scenic spots to learn the vector representation. The performance of literature [20] is better than that of literature [21] because literature [20] makes good use of extra data information. Literature [21] only uses the interaction matrix of tourists and routes.

4. Conclusion

With the rapid development of smart tourism under the Internet, more and more people are accustomed to choosing travel routes on major travel websites. At present, there is a lot of recommended information about travel routes on travel websites, and all of them are mainly display information. Choosing a travel route that meets the interests of tourists from many travel information has become an urgent problem for the platform to solve. This study proposes a travel itinerary recommendation algorithm combining convolutional neural networks and collaborative filtering. The algorithm convolutional neural network consists of an input layer, a convolutional layer, a pooling layer, a fully connected layer, and an output layer. The algorithm first vectorizes the information about tourists and tourist routes and obtains the implicit feature map through volume and neural network. Then use the collaborative filtering algorithm to complete the line recommendation. This study uses the evaluation criteria of Recall, Normalized Discounted Cumulative Gain (NDCG), and F1 score. The experimental results show that the proposed algorithm has higher recommendation accuracy and recall. At the same time, the search accuracy and convergence speed of the optimal solution are significantly improved. At present, users will choose a variety of transportation modes during travel. Urban traffic conditions are complex, and different modes of transportation have a great impact on the travel experience. In the following work, the influence of travel mode on travel route recommendation will be considered. How to apply

Hindawi
Security and Communication Networks
Volume 2024, Article ID 9816525, 1 page
https://doi.org/10.1155/2024/9816525

Retraction

Retracted: Application of Long-Term and Short-Term Memory Neural Network in Technical Evaluation of Hurdle Track and Field

Security and Communication Networks

Received 8 January 2024; Accepted 8 January 2024; Published 9 January 2024

This article has been retracted by Hindawi following an investigation undertaken by the publisher [1]. This investigation has uncovered evidence of one or more of the following indicators of systematic manipulation of the publication process:

(1) Discrepancies in scope
(2) Discrepancies in the description of the research reported
(3) Discrepancies between the availability of data and the research described
(4) Inappropriate citations
(5) Incoherent, meaningless and/or irrelevant content included in the article
(6) Manipulated or compromised peer review

The presence of these indicators undermines our confidence in the integrity of the article's content and we cannot, therefore, vouch for its reliability. Please note that this notice is intended solely to alert readers that the content of this article is unreliable. We have not investigated whether authors were aware of or involved in the systematic manipulation of the publication process.

In addition, our investigation has also shown that one or more of the following human-subject reporting requirements has not been met in this article: ethical approval by an Institutional Review Board (IRB) committee or equivalent, patient/participant consent to participate, and/or agreement to publish patient/participant details (where relevant).

Wiley and Hindawi regrets that the usual quality checks did not identify these issues before publication and have since put additional measures in place to safeguard research integrity.

We wish to credit our own Research Integrity and Research Publishing teams and anonymous and named external researchers and research integrity experts for contributing to this investigation.

The corresponding author, as the representative of all authors, has been given the opportunity to register their agreement or disagreement to this retraction. We have kept a record of any response received.

References

[1] Z. Liu, "Application of Long-Term and Short-Term Memory Neural Network in Technical Evaluation of Hurdle Track and Field," *Security and Communication Networks*, vol. 2022, Article ID 3095032, 11 pages, 2022.

Hindawi
Security and Communication Networks
Volume 2022, Article ID 3095032, 11 pages
https://doi.org/10.1155/2022/3095032

Research Article

Application of Long-Term and Short-Term Memory Neural Network in Technical Evaluation of Hurdle Track and Field

Zhenming Liu

School of Sports and Physical Education, Shandong Sport University, Jinan, Shan Dong 250102, China

Correspondence should be addressed to Zhenming Liu; liuzhenming@sdpei.edu.cn

Received 23 February 2022; Revised 18 March 2022; Accepted 4 April 2022; Published 6 May 2022

Academic Editor: Fang Liu

In order to study the application of long-term and short-term memory neural networks in the technical evaluation of hurdle track and field, firstly, the related contents of long-term and short-term memory neural networks and hurdle track and field sports are analyzed, the variation characteristics of kinematics and surface electromyography of swinging leg in the landing link of lower hurdle are analyzed, and the relationship between surface electromyography and kinematics parameters is analyzed. Then, the kinematics and surface EMG data of three male hurdlers in the hurdle team and two men in the College of Physical Education were collected when completing the technical link of pressing down and landing. The subject data were processed and analyzed by using the Simi motion video analysis system and DASY lab10.0 EMG analysis software. Finally, SPSS13.0 and origin are used to analyze the average, standard deviation, and correlation of the data results and draw a graph. Experiments show that neural network theory and finite element method, as the new forces of sports biomechanics, have been used to diagnose track and field technology. With the popularization of this method, it will play a greater role in the research of track and field technology.

1. Introduction

Hurdle has always been a popular research project in China. Since Liu Xiang won the world championship, people have exerted the pursuit of hurdle research to the extreme. However, due to the limitation of experimental conditions and experimental environment, previous research can only stop at motion and dynamics. However, there is relatively little research on the power source of the human body—muscles, especially the mutual coordinated effort between muscles and the influence of myoelectricity on muscle effort is even rarer [1].

The performance of the 110-meter hurdles consists of four technical links: starting with the first hurdle, hurdle step, inter-hurdle run, and the lower hurdle to the end of the tenth hurdle. Among the four components, the technical link of the hurdle step is the most important one. The hurdle step is a big step to connect the hurdle running technology. The quality of hurdle step technology directly affects the rhythm and speed of hurdle running technology after the next hurdle and determines whether we can achieve ideal results in this project. Therefore, the key to improving the performance of modern hurdles is to improve the hurdle step technology. The hurdle step technology is more complex, which can be divided into swing leg technology and starting leg technology. The main task of the kick-off leg in the hurdle step technology is to complete the kick-off. The quality of the kick-off leg will affect the kick-off angle and speed and will have a certain impact on the quality of the kick-off technology of the hurdle step [2]. The swinging leg runs through the whole hurdle step technology, which will not only affect the size of the starting angle, the starting speed, and the height of the center of gravity but also affect the flying time of the hurdle step, the distance between the swinging leg and the landing place, and the support angle of the swinging leg when landing to affect the horizontal movement speed of the center of gravity when landing and the connection between hurdle step technology and hurdle running technology. Therefore, the key to improving the technical level of the hurdle step is to improve the technology of swinging legs. The artificial neural network has good robustness (Figure 1), self-organization, self-

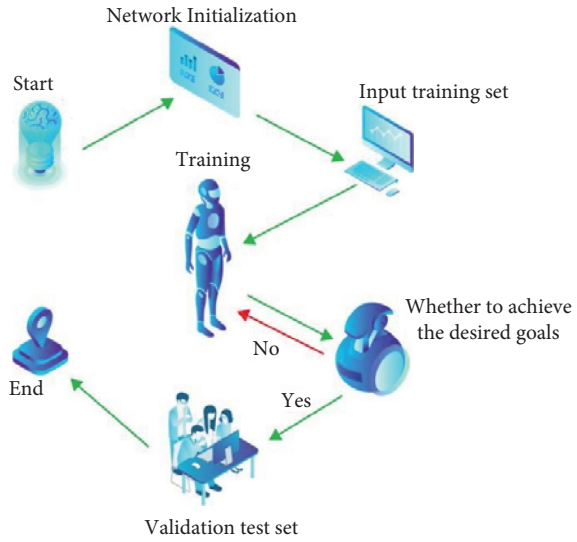


Figure 1: Long- and short-term memory neural network.

adaptability, parallel processing ability, distributed storage, and excellent fault tolerance and nonlinear approximation ability. At present, artificial neural network algorithm has been widely used in hardware fault detection, medical diagnosis, medical image processing, and other complex tasks of the complex system, classification, and prediction, and achieved good results.

The technology of swinging leg can be divided into four stages: jumping stage, attacking hurdle stage, falling hurdle stage, and landing stage. In these four stages, the quality of the hurdle technique is directly related to the time of the hurdle and the distance of the swinging leg landing place, which will determine the length of the hurdle step flying time and the quality of the combination of stride and run and ultimately affect the performance of athletes. Therefore, we can see that improving the quality of swing leg pressing technology will be the key to improving athletes' performance [3].

Based on the above analysis, this paper establishes the learning sample of the neural network according to the quality training level and special sports performance of China's excellent male hurdlers and puts forward the men's Hurdle Training Model Based on the neural network. The training model does not need to determine the mathematical expression of the training model in advance, more objectively reflects the mapping relationship between the special sports performance and various subordinate training indicators in men's hurdles, and shows high prediction accuracy.

2. Literature Review

Wen and others believe that hurdle running is a relatively common event in sports. It is the coordinated action of people on themselves, upper and lower limbs, and trunk muscles. It is required to complete the action quickly and keep the body in the air for a short time, but it also needs to create the necessary conditions for running between hurdles in the process; it is mainly composed of three parts: jumping over the hurdle, flying over the hurdle, and pressing the hurdle to the ground. The following three parts are emphatically analyzed in order to provide help for technological progress [4]. Illa and others believe that the position of athletes' take-off has an important impact on their performance. At present, according to the survey, there are still some problems with China's athletes in terms of take-off distance and take-off angle. On the one hand, the take-off point is too far, resulting in too long take-off distance and too small take-off angle, which will reduce the strength of athletes' legs and seriously restrict the effect of hurdles. On the other hand, the starting point is too close, resulting in a too close starting distance and too large starting angle, which reduces the speed in the horizontal direction and reduces the speed of hurdles [5]. Zuo and others believe that when athletes cross the hurdles, they have strict requirements for jumping legs. During the whole movement process, athletes should keep their shoulders and hips upright, and pedal back quickly after crossing the hurdles and landing, to make the athletes' body center of gravity move forward quickly along the straight track. After the pedal action is completed, they should attack the hurdles quickly; this is a movement action completed without certain support of the body [6]. Chen et al. believe that artificial neural network has good robustness, self-organization, adaptability, parallel processing, distributed storage, and other characteristics, as well as excellent fault tolerance and nonlinear approximation [7]. At present, Du and others believe that artificial neural network algorithms are widely used in complex tasks such as hardware damage detection, medical diagnosis, classification, and prediction of complex clinical image processing systems and have achieved good results [8]. Jane and others developed a dynamic chain model to explain the interactions between damage risk factors and their contributions to damage [9]. Yan et al. summarized the early warning research on sports injury risk. The predecessors conducted a lot of research on sports injury risk factors and developed a qualitative model, but there was no quantitative evaluation research. Due to its good performance, early warning of sports injury risk is very important [10]. Chen et al. argue that artificial neural network algorithms are better at solving such problems, but using neural network algorithms requires a database of samples to train them. The quality of the sample database directly affects the accuracy of the neural network algorithm. Demand data from a sample database provides information on all factors related to early warning of sports injury risk in athletes and their corresponding warning levels [11].

3. Method

An artificial neural network suffers from its huge number of parameters and is limited by the depth of the network and does not consider the information relationship between pixels. In order to solve the defects of the artificial neural network, CNN abandoned the full connection mode of the artificial neural network, adopted the mode of the image matrix, and introduced the ideas of "local perception, weight sharing, and downsampling," which greatly improved its

performance and application scenarios. CNN is mainly composed of a convolution layer, pooling layer, and full connection layer. If the input layer and output layer are added, a simple and complete CNN model can be constructed.

3.1. Convolution Layer. The main purpose of convolution operation in a convolution neural network is to extract some features by using a convolution kernel. The convolution kernel is equivalent to a filter. The feature map can be obtained by calculating the weighted average between the weight of the convolution kernel and the pixels in each small window region of the image. The convolution layer has a very strong feature learning ability. With the increase of network depth, the extracted features often gradually change from low-level features to high-level features. In addition, unlike the fully connected network, the convolution neural network is connected between each neuron between layers. The convolution kernel in the convolution neural network is only connected with some local areas in the input data, and the same convolution kernel in the same layer shares the weight parameters, which greatly reduces the number of network parameters. Figure 2 shows the calculation process of convolution operation [12].

In Figure 2, the size of the sliding window is the same as that of the convolution kernel. Multiply and sum the elements in the convolution kernel and the corresponding position elements in the sliding window. When performing a convolution operation, it is necessary to pay attention to the two parameters of convolution step size and peripheral filling. Convolution step size refers to the one-time sliding distance of the sliding window. With the continuous convolution operation, its output size will become smaller, and some data at the edge of input data are not used, resulting in the loss of some features. In order to solve the problem that the output size becomes smaller, a peripheral padding operation is proposed. The main purpose of this operation is to prevent the decline of data output size and the loss of features. Its specific operation is to carry out zero padding around the input data and control the size of output data by controlling the number of layers of data peripheral padding. The output calculation formula of data after convolution operation is

$$M_{\text{conv}} = \left[\frac{n+2p-f}{s}+1\right] * \left[\frac{n+2p-f}{s}+1\right], \quad (1)$$

where n represents the size of the input data matrix, f represents the size of the convolution kernel, s represents the convolution step size, and p represents the number of layers filled around the data matrix.

3.2. Pooling Layer. The feature map extracted by the convolution layer will have redundant data information. The purpose of pooling is to remove these redundant data and leave the most important data information, to reduce the size of feature data and achieve the effect of dimension reduction at the same time. The pooling layer plays a certain role in

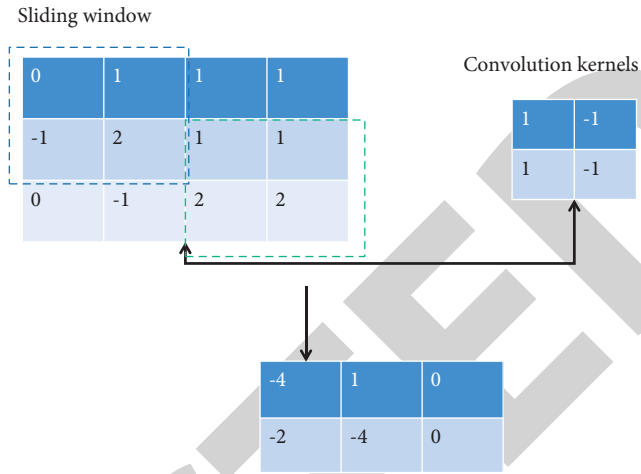


Figure 2: Operation diagram of convolution calculation.

preventing overfitting. The common forms of pooling layer include maximum pooling and average pooling. Generally, the effect of maximum pooling operation is better. The calculation operation of the maximum pooling layer and average pooling layer is shown in Figure 3, in which the size of the pooling layer core is $2 * 2$ and the step size is 20.

3.3. Full Connection Layer. Each neuron in the fully connected (FC) layer is connected to all neurons in the anterior layer. The full connection layer in a convolutional neural network plays the role of "Classifier." For example, for an image classification task with three categories, the feature map obtained after feature extraction through the input image needs multiple full connection layers to integrate it and reconnect it to form a new three-dimensional vector, in which each dimension represents a category; that is, the purpose of constructing a "Classifier" is achieved. However, not all convolution neural networks must have a full connection layer. The convolution layer can be used to replace the full connection layer. This convolution neural network is called a full convolution neural network [13].

The most common structure of the convolution neural network model is to connect the pooling layer behind the convolution layer. Its purpose is to reduce the dimension of the input data after convolution operation, reduce the redundant data information, and retain the important information. Then, it is repeated several times to extract the high-dimensional features of the data and finally output through the feature integration of the whole connection layer. The most common and simplest convolutional neural network model structure is shown in Figure 4.

3.3.1. Structure Composition of Long-Term and Short-Term Memory Neural Network. LSTM (Long Short-Term Memory Neural Network) is a new type of RNN-based deep machine learning neural network. In this model, the LSTM cell contains a memory cell that attempts to store information for a long time. The entrance to this memory unit is controlled by some special doors. Controlled functions

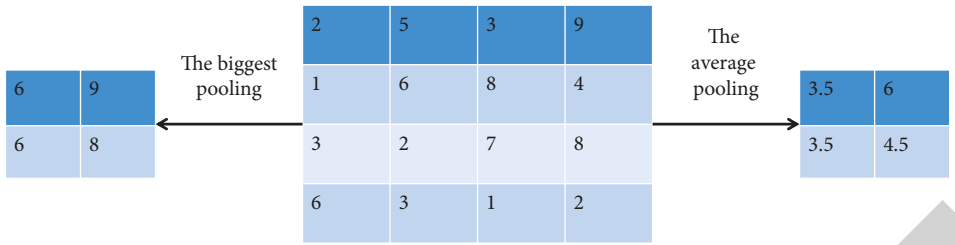


Figure 3: Calculation diagram of maximum pooling and average pooling.

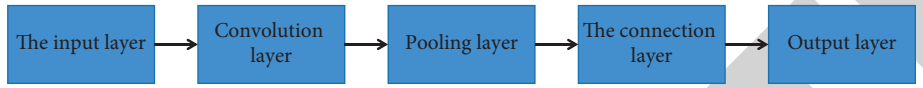


Figure 4: Common convolutional neural network structure.

include save, write, and read. These gates are logic units responsible for weighting the edges that connect the rest of the neural network to memory cells. The memory unit itself is a linear neuron with internal connections. Specifically, each of the three doors has three entrances. Forget about exit doors and gates. Correction parameters are used to select and memorize the gradient decreasing error function. When you open the gate of forgetting, the connection weight itself is 1, and the memory part writes the content to itself. When the output of the forget gate is 0, the memory cell will delete the previous content. The output gate allows the rest of the neural network to write to the memory cell when the output value is 1, while the input gate allows the memory cell to read the memory cell to the rest of the neural network when the output value is 1 [14]. The structure of the model is shown in Figure 5.

Clell is the memory of the state of nerve cells. There is a parameter called the state to record a state. Forget Gate: select and fix the state of the last neuron. For each memory cell, three sets of weights are prepared from the input, including the fully hidden state of the previous time step. Insert one in the input node at the bottom of the image above. I put one on the forgotten door and showed it on the right. Another entry exit door is visible from the top left. Each black node is associated with an activation function; a typical activation function is a sigmoid function. The most important node of the cell is the internal state, where the first dimension is weighted over a period and then returns to itself. The self-adhesive edge of the internal state is called the Fixed Error Conveyor or CEC.

For example, in the past, entry gates determined when to activate activation states in memory cell slots, while output gates determined when to activate outgoing memory cells, which was determined by training. Finally, forget gates are used to learn to forget the final state of a neuron completely or partially or completely. The same is true after delivery. The output gate learns when the error flows to the storage unit, while the input gate learns when the error flows out of the storage unit and transmits it to the rest of the neural network. The same goes for forgetting doors. The formulas for each part are given in the order of calculation-general algorithm:

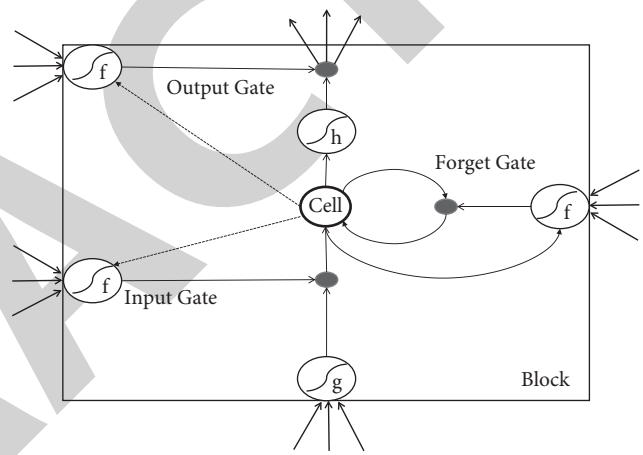


Figure 5: Model structure.

$$a_l^t = \sum_{i=1}^{I} W_{il} X_i^t + \sum_{h=1}^{H} W_{hl} b_h^{t-1} + \sum_{c=1}^{c} W_{cl} S_c^{t-1},$$
$$b_I^t = f\left(a_l^t\right). \tag{2}$$

3.3.2. Operation Process of Long-Term and Short-Term Memory Neural Network. The forward propagation calculation process of LSTM is as follows.

(1) Update the output of the forgetting gate. The formula is

$$f(t) = \sigma\left(W_f h_{t-1} + U_f x_t + b_f\right). \tag{3}$$

(2) Update the two-output status information of the input gate. The formula is

$$i(t) = \sigma\left(W_i h_{t-1} + U_i x_t + b_i\right). \tag{4}$$

(3) Update the cell status. The formula is

$$C(t) = C(t-1) f(t) + i(t) a(t). \tag{5}$$

(4) Update the output gate. The formula is

$$\sigma(t) = \sigma\left(W_o h_{t-1} + U_o x_t + b_o\right). \quad (6)$$

The backpropagation calculation process of LSTM is as follows.

In LSTM, there are two hidden states, $h(t)$ and $c(t)$, respectively. Therefore, two $\delta(t)$ are defined, and the formula is

$$h(t) = o(t)\tan\ h(C(t)). \quad (7)$$

The backpropagation calculation process of LSTM is as follows.

① In LSTM, there are two hidden states, $h(t)$ and $c(t)$, respectively. Therefore, two RTs are defined, and the formula is

$$\begin{aligned} \delta_h(t) &= \frac{\partial L}{\partial h(t)}, \\ \delta_c(t) &= \frac{\partial L}{\partial C(t)}. \end{aligned} \quad (8)$$

② The loss function $L(t)$ adopts the cross line loss function, and the formula is

$$L(t) = \begin{cases} l(t) + L(t+1) & \text{if } t < \tau \\ l(t) & \text{if } t = \tau \end{cases}. \quad (9)$$

③ $\delta h(\tau)$ and $\delta c(\tau)$ of the last index position τ of the sequence obtained by combining ① and ② are given as follows:

$$\begin{aligned} \delta h(\tau) &= \frac{\partial L(\tau)\partial O(\tau)}{\partial O(\tau)\partial h(\tau)} \\ &= V^T(\hat{y}(\tau) - y(\tau)), \\ \delta_c(\tau) &= \frac{\partial L(\tau)}{\partial h(\tau)}\frac{\partial h(\tau)}{\partial c(\tau)} \\ &= \delta_h(\tau) o(\tau)\left(1 - \tanh^2(C(\tau))\right). \end{aligned} \quad (10)$$

④ $\delta h(t)$ and $\delta C(t)$ are inversely derived from $\delta h(t+1)$ and $\delta C(t+1)$, and the gradient of each parameter is calculated. The derivation formula of $\delta h(t)$ and $\delta C(t)$ is

$$WS\delta_h(t) = V^t(\hat{y}(t) - y(t)) + \delta_h(t+1)\frac{\partial h(t+1)}{\partial h(t)}. \quad (11)$$

⑤ Calculate the gradient of the network parameter W_f, and the formula is

$$\frac{\partial L}{\partial W_f} = \sum_{t=1}^{\tau}\left[\delta_c(t)C(t-1)F(t)(1 - f(t))\right](h(t-1))^T. \quad (12)$$

Repeat the above steps until the error of the network is lower than the set threshold.

Once the neural network model of the first data series is built, a series of predicted values for the first data series can be obtained. These predicted values may be slightly different from the original data, and these bias ratios can be combined in a neural network model: take the predicted value as a neural network input sample and the actual value as a neural network output sample. Approve a specific structure; then train, the neural network to obtain several weights and thresholds corresponding to the corresponding nodes [15].

4. Experimental Analyses

There are 3 male hurdlers on the hurdle team and 2 male hurdlers in the Institute of physical education. The basic information about the athletes is shown in Table 1. Athletes are in good health, without muscle injury and other diseases, and are in a normal training state.

4.1. Experimental Method. The EMG measuring instrument used in the experiment is a 16 lead biovision multifunctional exercise bioelectricity measurement and analysis system imported from Germany, and the software version is dasylab10.0. In this experiment, the EMG of surface muscle is collected by EMG measuring instrument. In the experiment, the sampling frequency of the EMG measuring instrument is 1000 Hz and the magnification is 10000. The obtained data are processed by DASYLab 10.0 EMG analysis software [16]. The EMG electrode used in the experiment is a disposable ECG electrode (silver/silver chloride) produced by Renhe Medical Equipment Co., Ltd. The diameter of the electrode adhesion area is 30 mm, and the diameter of the conductive area is 10 mm.

4.1.1. Treatment Method of Sticking Position. Before the sEMG test, firstly scrape the surface skin with a razor, then Polish the skin of relevant muscles with fine gauze, clean the skin surface with a 75% alcohol cotton ball, and remove the oil on the skin surface. After the alcohol is evaporated, the illumination electrode and detection electrode are placed on the muscle abdomen of the muscle, and the placement direction is consistent with the long axis of the muscle fiber. The diameter of the electrode is 0.5 cm and the electrode spacing is 2 cm.

4.1.2. Data Processing and Statistical Methods. The experimental data were processed and analyzed by the Simi motion video analysis system and DASYLab 10.0 EMG analysis software. Finally, SPSS13.0, origin 7.5, and Excel12003 are used to analyze the average value, standard deviation, and correlation of the data results and draw the graph.

4.2. Experimental Steps and Processes

4.2.1. Before Experiment. The staff shall register the height, weight, history of injury, and other basic information of the subjects and inform the subjects of the whole experimental process so that the subjects can be familiar with the whole

Table 1: Basic information of subjects.

Athletes	Age (*y*)	Height (cm)	Weight (kg)	Years of exercise (*y*)	Sport level
Zhu XX	20	186.4	78	8	Master
Song XX	20	189.2	70	7	Class a
Hu XX	20	186	73.5	7	Class a
Zhang XX	19	185	75	6	Class a
South XX	20	187.9	78.3	8	Class a

process of the experiment. It is beneficial for the subjects to cooperate with the experiment.

4.2.2. Commissioning of Experimental Instruments and Equipment. Set the sampling frequency of MotionPro to 100 Hz and debug the acquisition range. Connect, debug, and check the EMG equipment and check whether the equipment operates normally [17].

4.2.3. Preparation of Subjects before Test. Warm-Up. The subject carries out a warm-up exercise to open the muscles, especially the muscles on the exerting side, to prevent the subject from being injured during the experiment. At the same time, carry on the simulation exercise with the data acquisition instrument to get familiar with the action process and make the experimental data closer to the real value.

Dress. Subjects are required to wear track and field clothes. Reduce the influence of external factors.

Marking. Mark each joint (shoulder, elbow, wrist, skeleton, knee, and step) and head, hand, and foot with marking points.

Sticking Electrode. Scrub the measured muscle skin oil with alcohol and scrape off its hair. Stick the electrode to the muscle belly of the measured muscle along the direction of the muscle fiber, and connect the acquisition line. Then, the elastic foam bandage is used to fix it, to avoid the shaking of electrodes and amplifiers in the test process and affect the true value of the collection.

4.2.4. Action Requirements of Subjects during Test. The subjects were asked to start after hearing the command and cross four standard height hurdles while maintaining high speed. The staff collected the relevant data in the third column 3 times. If the collected data is checked to be accurate, the subjects will be replaced and the steps will be carried out. After the experimental data of all subjects are collected and archived, the data will be analyzed.

4.2.5. Experimental Data Processing. In this study, the surface electromyography instrument was used to collect, process, and analyze the electromyographic activity signals of the muscles related to the technical link of the lower hurdle landing of the hurdle swing leg (biceps femoris long head, Hemi key muscle, rectus femoris, gluteus maximus, and tensor fascia lata), to confirm the activity characteristics of the muscles in the technical link of the lower hurdle landing of the hurdle swing leg. The signal collected by the electromyograph is the original electromyography, which must be processed in the following steps before quantitative analysis [18].

The original EMG is filtered first: high pass 20 Hz and low pass 400 Hz to eliminate the noise. After full-wave rectification, the negative wave is transformed into a positive wave. Finally, integrate EMG (iEMG), take out the iEMG of the landing link of the lower hurdle, calculate the muscle contribution through iEMG, and take the envelope as the analysis index. The score is the sum of the electromyographic contribution of a muscle in a certain time. It can reflect the degree of muscle participation in completing a certain action and the importance of the muscle in the action.

4.3. Kinematic Data Processing Results. As a speed project, speed is the decisive factor affecting the performance of a short-span project. The coordination between the angular velocity of the skeleton joint and the angular velocity of the knee joint will reflect the movement of the swinging leg. At the same time, it also directly affects the quality of hurdle step technology.

It can be seen from Figure 6 that in the hurdle step technology, the angular velocity of the athlete's skeleton joint and the angular velocity of the knee joint cooperate with the angular velocity change. The results are as follows: in the landing stage of the starting leg, the swinging leg bends the knee and retracts the lower leg. Relevant studies believe that it is best to keep the folding leg folded before the starting leg leaves the ground as much as possible. From Figure 7, we can see that the peak value of the angular velocity of knee flexion appears before the valley value of the angular velocity of bone flexion, and the time difference between the two values is 4.5070. This phenomenon shows that the contraction angular velocity of the lower leg is greater than that of the thigh. The full folding of the lower leg will be conducive to the swing of the thigh. Because according to $I = \sum \Delta mr^2$ (I: moment of inertia, M: mass of swinging leg, R: radius of rotation of swinging leg), the shorter the radius of rotation of swinging leg, the smaller the moment of inertia of swinging leg. Greater rotational speed will be obtained with the same contraction force. Or the same rotational speed will require less contraction force.

From Table 2, we can also see that there is a good linear relationship between the angle of the knee joint and the angular velocity of the skeleton joint in the take-off stage of

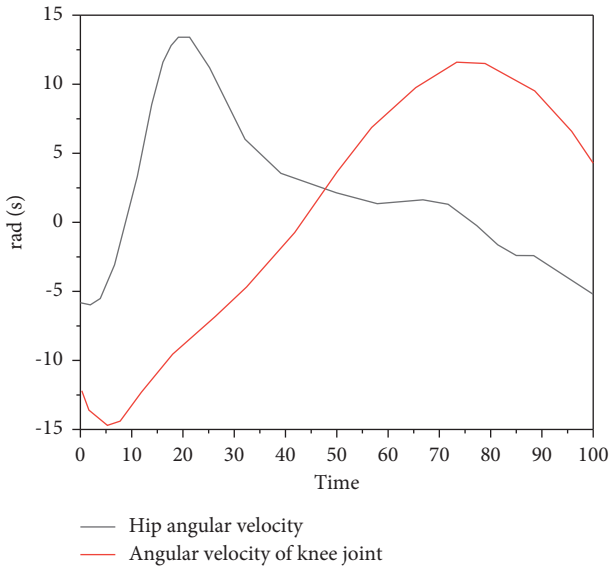


Figure 6: Change of knee joint angular velocity.

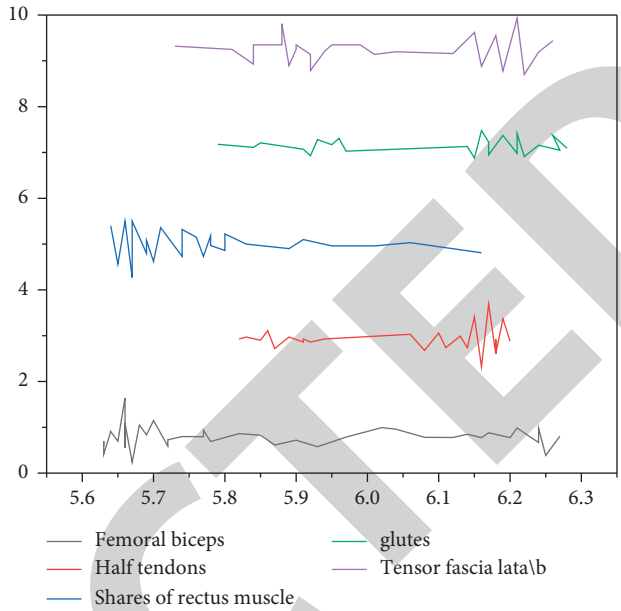


Figure 7: Original electromyography.

the swing leg, showing a significant negative correlation. This result also proves that the folding of the knee joint will affect the rotation speed of the skeleton joint. It conforms to the law of moment of inertia.

However, Figure 7 shows that the angular velocity curve of the knee joint of the swinging leg of the tested athlete is steep at this stage, indicating that the movement direction is changed immediately after the folding of the knee joint is completed, the knee joint is extended, and there is no sign of prolonging the folding of the swinging leg. Premature extension of the knee joint will not be conducive to the swing of the knee joint. Premature expansion of the knee joint will increase the swing inertia of the swing leg and increase the control difficulty of the swing leg. Excessive flexion of the swing leg joint will delay the pressing time [19].

In this paper, through the relationship between the distance of the center of gravity of the foot tip, the descent distance of the center of gravity in the depression stage, the rate of speed loss in the depression stage, the time of hurdle step, and the angular velocity of the skeleton joint, the results are as follows.

Through statistics, it is found that there is a negative correlation between the time of hurdle step, the rate of speed loss in the pressing stage of swinging leg, and the angular velocity of the skeleton joint. No correlation was found between other indicators.

In the past, relevant scholars have also obtained relevant results in the theoretical research of hurdle step technology. However, the relationship between relevant parameters is rarely proved by statistics. The main reason may be the limitation of experimental conditions and the accuracy of measured parameters is not high enough. Therefore, it is impossible to demonstrate the reasoning of hurdle step technology in the form of numerical value.

With the deepening of research, people gradually realize that the motion amplitude and speed of the skeleton joint are more important than those of the knee joint. In the process of pressing down the swinging leg, the movement of the swinging leg is driven by the skeleton joint. Therefore, the movement of the skeleton joint will determine the downward pressure of the swinging leg. From Tables 3 and 4, we can see that in the downward pressing stage of swinging leg, the greater the angular velocity of the skeleton joint, the less time required for the hurdle step and the smaller the rate of center of gravity speed loss. The relationship between skeletal joint movement and angular velocity proves that the change in the relative position of each limb can change the athlete's flying time in the flying stage. In hurdle events, the shortening of flying time is an important way to improve performance.

4.3.1. Surface Electromyography Processing Results. SEMG is the result of bioelectricity generated by nerve and muscle excitation. It is the source of electrical signal generating muscle force. It has different degrees of correlation with muscle activity and functional state, so it can reflect the activity of nerves and muscles to a certain extent. SEMG signal can be used to analyze the characteristics of muscle exertion, muscle activation sequence, exertion degree, and action coordination ability in sports. When the human body is moving, it is used to analyze the important joint angle, the relationship between torque and angle, and EMG. Therefore, it is widely used in the field of sports research. The measured images and data processing are as follows.

In order to observe the muscle action or phase change over a period, the rectified high-frequency signal existing in the EMG signal is usually removed, and the obtained curve is called an envelope. By observing the change of envelope, we can know the phase of muscle activity and understand the control and coordination of neuromuscular.

From Figures 8–11, we can see that in the hurdle step technology of five athletes, the overall trend of EMG activity

Table 2: Relationship between knee joint angle and skeletal joint angular velocity in the take-off stage of swing leg hurdle step technology.

Zhu XX	Hu XX	South XX	Zhang XX	Song XX	Average value	P value	Correlation coefficient
Knee angle (rad)	1.08 ± 0.17	1.00 ± 0.23	1.8 ± 0.34	1.34 ± 0.18	1.15 ± 0.25		
Hip angle						0.00	−0.911
Speed (rad/s)	12.04 ± 1.56	13.05 ± 3.85	10.32 ± 1.17	12.32 ± 0.17	13.32 ± 2.56		

Table 3: Relationship between the time of swinging leg hurdle step and the mean value of joint angular velocity in the next hurdle stage.

Zhu XX	Hu XX	South XX	Zhang XX	Song XX	Average value	P value	Correlation coefficient
Hurdle step time (S)	0.62 ± 0.01	0.66 ± 0.01	0.67 ± 0.01	0.63 ± 0.01	0.65 ± 0.02		
Hip angle						0.034	−0.567
Speed (rad/s)	12.08 ± 0.67	10.12 ± 0.35	10.81 ± 0.57	10.57 ± 1.13	10.99 ± 0.99		

Table 4: Relationship between velocity loss rate and mean angular velocity of skeleton joint in the pressing stage of swinging leg.

Zhu XX	Hu XX	South XX	Zhang XX	Song XX	Average value	P value	Correlation coefficient
Speed loss rate in pressing stage (%)	4.29 ± 0.86	6.78 ± 2.4	4.58 ± 0.54	5.87 ± 0.01	0.65 ± 0.02		
Hip angle						0.034	−0.567
Speed (rad/s)	12.08 ± 0.67	10.12 ± 0.35	10.81 ± 0.57	10.57 ± 1.13	10.99 ± 0.99		

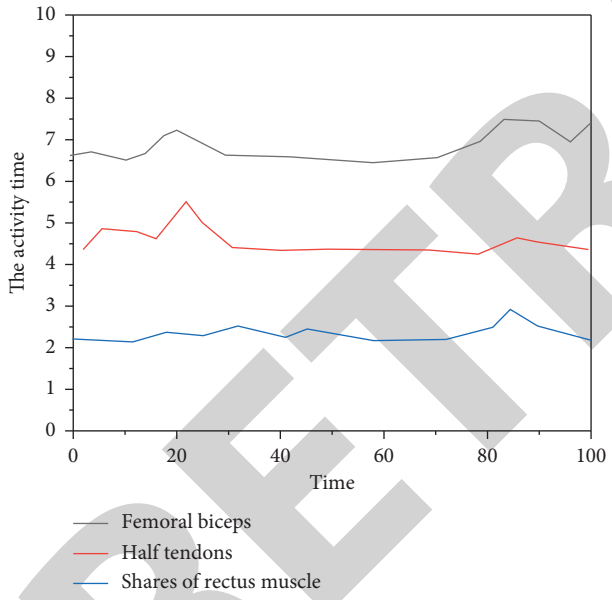


Figure 8: Time sequence of Hu XX muscle activity.

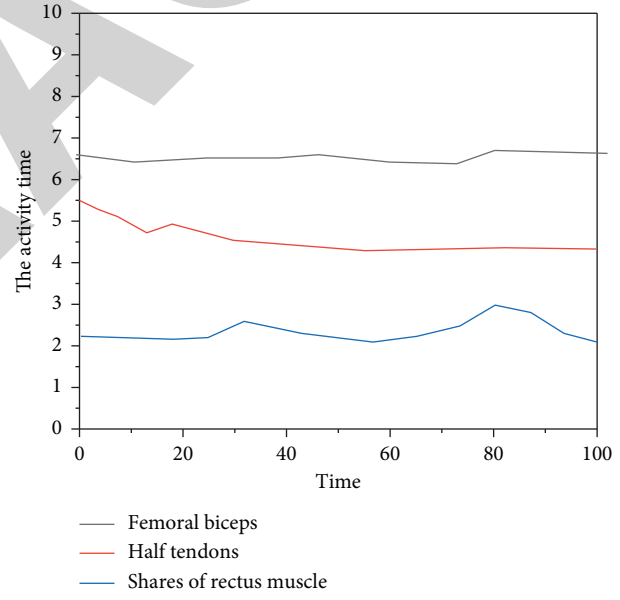


Figure 9: Sequence of muscle activity in South XX.

of swinging legs is relatively similar, while there are differences in EMG amplitude between athletes. The main reason for this phenomenon is that in the process of completing a specific technical action, the relevant muscles need to participate in the work according to their own functions to complete a specific joint movement. The difference in EMG amplitude between athletes is mainly due to the difference in cortical thickness of athletes' own skin. Cortical thickness is an important factor affecting surface electromyography acquisition. For example, in Zhu XX (the highest sports level among the five), in the whole hurdle step technology, the EMG amplitude of the swinging leg is smaller and more stable than that of other athletes. Through the observation of athletes, in addition to the influence of sebum, there should be other factors affecting Zhu XX's EMG amplitude which is small and stable. According to the neural control law, Zhu XX's EMG may be caused by Zhu XX's own training level [20]. EMG amplitude is small because athletes have a high degree of training. Smaller EMG activities can produce greater muscle strength, which is particularly obvious for beginners. As the EMG is relatively stable, the muscles measured by the swinging leg produce obvious EMG activity only in the take-off stage and support landing stage. It is due to the intermittent mechanism between muscles. Although the swinging leg has been moving throughout the hurdle step technology, no muscle in the

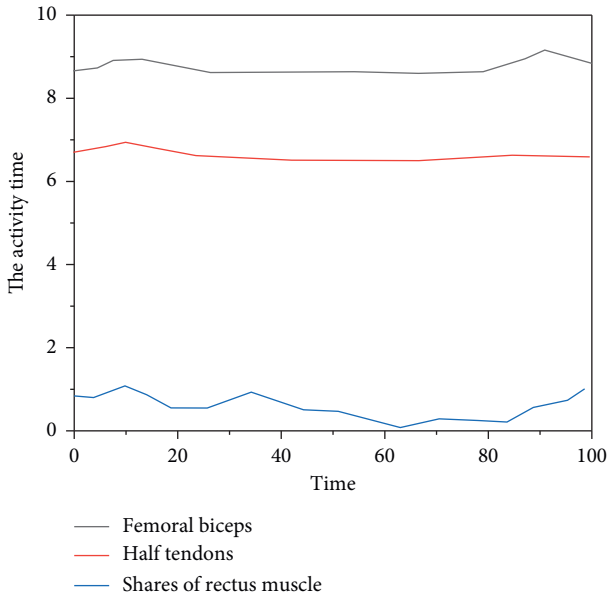


Figure 10: Timing of muscle activity.

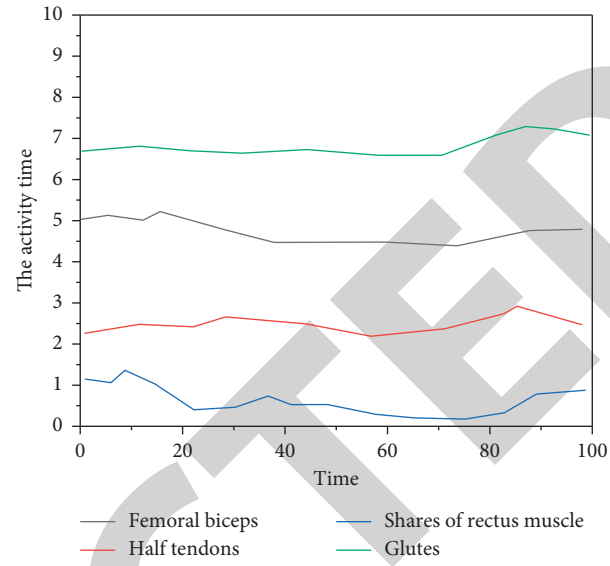


Figure 12: Envelope characteristics of swinging leg of hurdle step of tested athletes.

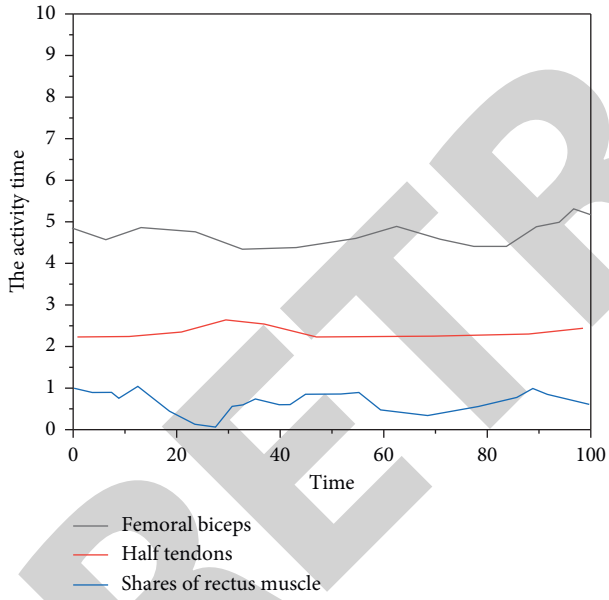


Figure 11: Timing of muscle activity.

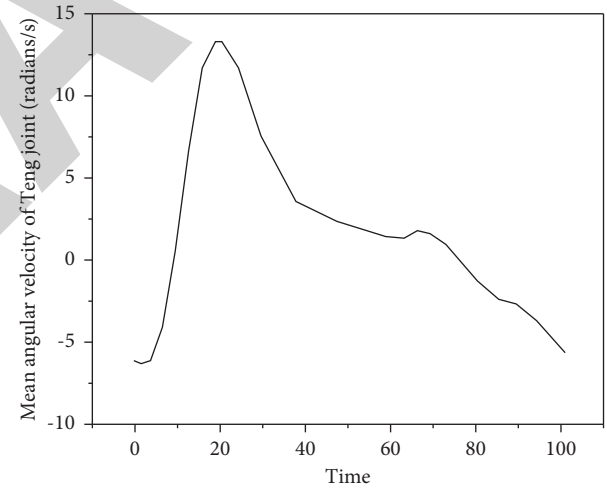


Figure 13: Changes in knee joint angular velocity.

measured muscles is involved in the whole process, but intermittently. This intermittent activity will be more conducive to the recovery of fast muscle fiber ability and the next stage of exertion. The stability of Zhu XX's EMG amplitude shows that the relaxation ability of the measured muscles is better than that of other subjects in the high-speed movement of skeleton joints. This phenomenon is closely related to the training level of athletes.

There are two main reasons for the obvious increase of muscle EMG amplitude measured by the swinging leg before landing. There is a delay in the generation of EMG between joint movements. There is a delay between EMG activity and the movement of lower limb joints. The delay between EMG and muscle strength generation is 10 milliseconds, and the delay between muscle strength generation and joint movement is 30 milliseconds. There is a phenomenon of preactivation in skeletal muscle. By observing the EMG activities of the long head and half key muscle of the biceps femoris, it is found that the EMG activities of the long head and half key muscle of the biceps femoris are similar. From the perspective of action anatomy, the biceps femoris starts from the upper part of the posterior part of the sciatic tubercle, ends at the fat bone, and partially ends at the collateral ligament on the outer side of the knee and the external stepping of the tibia. Its function is to bend the knee joint, rotate the tibia outward, and the function of the divine skeleton joint. The half key muscle starts from the inner upper part of the posterior part of the sciatic tubercle and ends above the inner side of the tibial shaft. Its function is to

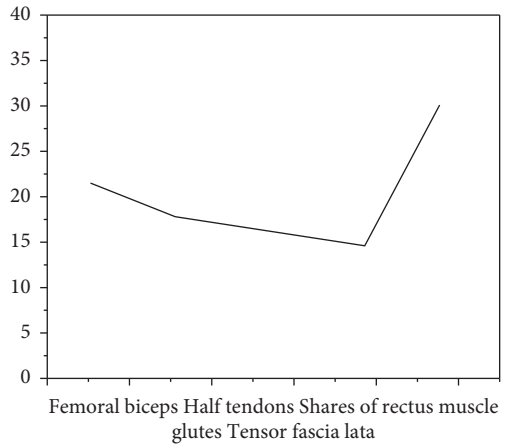


Figure 14: Average value and standard deviation of technical muscle contribution of swinging leg hurdle step (%).

extend the thigh, bend the knee joint, and rotate the tibia internally. From the perspective of anatomy, the functions of the biceps femoris and Hemi key muscle are similar. They are cross joint muscles, which have the functions of both bone flexion and knee flexion. Therefore, in the hurdle step technology, the EMG activities of the half key muscle of the swinging leg and the biceps femoris are similar and reasonable.

Through Figure 12, it can be found that there are three fluctuations in the EMG amplitude of the biceps femoris and biceps femoris in the hurdle step technology: the first appears in the support stage, in which the biceps femoris and biceps femoris bend their knees to retract the lower leg, reduce the swing radius of the swing leg, and increase the swing speed of the swing leg when the swing leg is swinging. The fluctuation of the second EMG amplitude occurred in the middle and late stages of the swing leg attacking the hurdle. Considering the disguised movement of the swing leg and the EMG action delay, it can be judged that the main function of this EMG activity is to extend the skeleton. However, we found that the amplitude of EMG in this stage is the smallest of the three fluctuations. Therefore, to some extent, it can be inferred that the hemidesmus and biceps femoris are not the main muscles of bone extension at this stage, and other muscles should undertake the main task of bone extension. In the third wave, the EMG amplitude began to increase significantly from the depression stage, reached the peak at the landing support stage, and remained at a high level throughout the support stage. The main reason for this is that the knee joint starts to bend the knee before landing, to prepare for the formation of strong ground picking action. As shown in Figure 13, actively bending the knee, and retracting the lower leg will play an important role in obtaining a favorable landing position when the swinging leg lands on the ground and completing the cross-run connection better. Because the active recovery of the lower leg before landing will help to form a "pick the ground" posture, reduce the force in the negative direction caused by the ground reaction, reduce the loss of speed, and help swing the leg, at the same time, it can avoid the injury of the rear muscle group caused by the load overload of the rear muscle group due to the unreasonable landing location. In the landing support stage, the EMG amplitude continued to increase until it reached the peak and began to decline steadily. At this stage, the biceps femoris and hemidesqualis are one of the main power sources of the horizontal backward direction of the center of gravity. In the first half of the landing support, it is also the time when the rear muscle group carries the maximum load, so athletes are often prone to injury at this stage. This is especially true when the landing place of the swinging leg is far from the center of gravity. Therefore, it can be concluded that accelerating the downward pressure of the swing leg is not only more conducive to the force of the swing leg when landing but also can effectively avoid the strain of the posterior femoral muscle group.

The technical muscle contribution of men's 110-meter hurdler's swinging leg hurdle step in Figure 14 is as follows.

The discrete degree of muscle contribution can explain the stability of a certain technique of the same athlete to a certain extent. The higher the dispersion of muscle contribution is, the more unstable the technology is. On the contrary, the lower the dispersion of muscle contribution is, the more stable the technology is. Through the observation of muscle contribution, we find that the dispersion of muscle contribution between the three tests of the same athlete is relatively small, indicating that the swing leg technology of the tested athletes is relatively stable in the hurdle step. However, the standard deviation of muscle contribution between different athletes is much larger than that between different tests of the same athlete. There are many reasons for this phenomenon, but the main reason may be the different habits of exerting a force between different athletes. Although the contribution degree of different athletes is relatively different, at the same time, we can also see that the contribution degree of individual muscles in the technical link of the hurdle step is much higher than that of other muscles, for example, tensor fascia lata. As a single joint muscle, tensor fascia lata mainly participates in the thigh retraction in the ground take-off stage and the upper leg lifting in the hurdle attack stage, and the strength and amplitude are relatively large. Therefore, excluding other factors, the contribution of tensor fascia lata in the measured muscles is large, which is also normal. From Figures 13 and 14, we can see that in the hurdle step technology, the measured muscle contribution of the swinging leg is as follows: the tensor fascia lata and biceps femoris participate in the activity obviously, followed by the half bond muscle, rectus femoris, and gluteus maximus.

5. Conclusion

Photogrammetry, camera measurement, isokinetic force measurement, 3D dynamic force measurement, and computer numerical simulation are the main test methods of track and field technical sports biomechanics. The kinematic analysis of track and field technology generally adopts high-speed photography or video recording. After analysis, the action details of fast movement can be obtained accurately,

Hindawi
Security and Communication Networks
Volume 2024, Article ID 9784640, 1 page
https://doi.org/10.1155/2024/9784640

Retraction

Retracted: Anonymization of Quasi-Sensitive Attribute Sets in Aggregated Dataset

Security and Communication Networks

Received 8 January 2024; Accepted 8 January 2024; Published 9 January 2024

This article has been retracted by Hindawi, as publisher, following an investigation undertaken by the publisher [1]. This investigation has uncovered evidence of systematic manipulation of the publication and peer-review process. We cannot, therefore, vouch for the reliability or integrity of this article.

Please note that this notice is intended solely to alert readers that the peer-review process of this article has been compromised.

Wiley and Hindawi regret that the usual quality checks did not identify these issues before publication and have since put additional measures in place to safeguard research integrity.

We wish to credit our Research Integrity and Research Publishing teams and anonymous and named external researchers and research integrity experts for contributing to this investigation.

The corresponding author, as the representative of all authors, has been given the opportunity to register their agreement or disagreement to this retraction. We have kept a record of any response received.

References

[1] Y. Li, S. Yuan, Y. Yuan, C. Chen, and J. Yu, "Anonymization of Quasi-Sensitive Attribute Sets in Aggregated Dataset," *Security and Communication Networks*, vol. 2022, Article ID 9721817, 16 pages, 2022.

Hindawi
Security and Communication Networks
Volume 2022, Article ID 9721817, 16 pages
https://doi.org/10.1155/2022/9721817

Research Article

Anonymization of Quasi-Sensitive Attribute Sets in Aggregated Dataset

Yafan Li,[1,2] **Shuguang Yuan**,[1,2] **Yulin Yuan**,[1,2] **Chi Chen**,[1,2] **and Jing Yu**[1,2]

[1]*State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China*
[2]*School of Cyber Security, University of Chinese Academy of Sciences, Beijing 101400, China*

Correspondence should be addressed to Jing Yu; yujing@iie.ac.cn

Received 17 January 2022; Revised 8 March 2022; Accepted 24 March 2022; Published 29 April 2022

Academic Editor: Zhiping Cai

The widespread use of Internet of Things (IoT) and Data Fusion technologies make privacy protection an urgent problem to be solved. The aggregated datasets generated in these two scenarios face extra privacy disclosure. We define attribute sets with different sources in an aggregated dataset as quasi-sensitive attribute sets (QS sets). The QS set itself is not sensitive, but internal linking attacks may occur when two QS sets in an aggregated dataset are linked. In this paper, we propose a new privacy model, namely, the QS k-anonymity model. The QS k-anonymity model is effective in preventing internal linking attacks. We provide two algorithms for the QS k-anonymity model, the Greedy QS k-anonymity algorithm and the Efficient QS k-anonymity algorithm. We evaluate our algorithms on real datasets. The experimental results show that the Greedy QS k-anonymity algorithm has good data utility, the Efficient QS k-anonymity algorithm shows better efficiency, and both algorithms are well scalable.

1. Introduction

In recent years, with the emergence and development of technologies such as data mining and information sharing, more and more organizations are releasing large amounts of data for use, analysis, and research [1]. Thus, how to prevent the disclosure of sensitive information has become a major research hotspot. As an important part of data mining and information sharing, privacy-preserving data publishing (PPDP) [2] has attracted many scholars to conduct research on it since it was proposed. Researchers often refer to an organization that holds, anonymizes, and publishes data as a "data publisher," and organizations that receive and use the data as "data analyzers."

Many studies have been proposed on anonymized data. Most of the current studies consider that the data publisher has a table in the form of explicit identifiers (EIs), quasi-identifiers (QIDs), sensitive attributes (SAs), and nonsensitive attributes (NSAs), where EIs are attributes that explicitly identify record owners (e.g. name and ID); QIDs are attributes that could be linked to external tables to identify the record owner [3]; SAs include sensitive information about individuals such as illness, salary, etc.; and NSAs contain all attributes except for the previous three types [4]. Most works assume that the four sets of attributes are disjoint. As the EIs are directly associated with the record owners with their sensitive information, they will be removed before the data are released for the privacy of the record owners. Even if the EIs are removed, the owner of the record can be re-identified by linking his or her QIDs to an external table. This attack is known as the linking attack [5]. To prevent linking attacks, the data publisher releases an anonymized table, including QIDs', SAs, and NSAs, among which QIDs are the results of QIDs being anonymized.

In the following paragraphs, we will give a brief introduction to k-anonymity and then describe the problems that will be discussed in this paper.

K-anonymity is one of the most widely used anonymous methods of privacy protection [6]. The model requires that each record in the anonymized dataset is indistinguishable from at least $k-1$ other records on the QIDs [7]. For example, Table 1 is an original table describing patient

Table 1: Patient table.

Name	Age	Sex	Zipcode	Disease
Alex	23	Female	17227	Flu
Beth	22	Male	17684	Hepatitis
Carl	25	Male	17657	Broken arm
Ellen	49	Female	19336	Hangnail
Glen	50	Male	18814	Bronchitis
Helen	44	Female	18835	Flu

Table 2: 3-Anonymity.

Age	Sex	Address	Disease
[22–25]	Person	[17227–17684]	Flu
[22–25]	Person	[17227–17684]	Hepatitis
[22–25]	Person	[17227–17684]	Broken arm
[44–50]	Person	[18814–19336]	Hangnail
[44–50]	Person	[18814–19336]	Bronchitis
[44–50]	Person	[18814–19336]	Flu

information, where Name is an EI; Age, Sex, and Zipcode are considered as QIDs; and Disease is considered as a SA. Table 2 shows the anonymized results obtained from Table 1 after 3-anonymity. Even if the data analyzers know Alex's QID values, it is difficult to tell which of the first three records he is.

However, multi-source data aggregation exists in IoT and Data Fusion scenarios. Considering the data aggregation process, the form of datasets in IoT and Data Fusion scenarios may be different from the form of datasets mentioned above. In this paper, we refer to the dataset formed by data aggregation in IoT and Data Fusion scenarios as an *Aggregate d* Dataset (*A D*). We discuss the simplest of these cases, where the aggregated dataset consists of data from two sources.

We find that the two attribute sets that constitute an aggregated dataset are insensitive before aggregation, but there may exist linkability between these two attribute sets after aggregation, leading to attacks based on linkability. We refer to this attack as internal linking attacks, and such attribute sets as quasi-sensitive attribute sets (QS sets). We will describe the aggregated dataset and the internal linking attacks in detail in Section 3.

We classify the existing privacy-preserving methods based on k-anonymity into two categories. One is the conventional k-anonymity methods, including many classical anonymization methods and optimization algorithms [12–18]. They are more concerned with optimizing for the efficiency and utility of the algorithms. However, the impact of specific scenarios on the anonymity method is not taken into account. The other type of anonymization methods is scenario-based anonymization methods. Shi et al. [19] introduce "quasi-sensitive attributes" that can indirectly lead to the disclosure of sensitive information. Terrovitis et al. [20] argue that in some scenarios, some attributes are both QIDs and SAs. Sei et al. in [3] propose to treat QIDs as SAs and introduce the concept of "sensitive quasi-identifiers," but this approach leads to reduced utility of the anonymized data. However, none of these methods takes into account the problem of internal linking attacks faced by aggregated datasets generated in IoT and Data Fusion scenarios.

Our main **contributions** are as follows:

(1) We identify a new privacy disclosure to aggregated datasets in IoT and Data Fusion scenarios. And, we propose internal linking attacks based on linkability faced by QS sets in aggregated datasets.

(2) We propose a new privacy model, namely, *QS k*-anonymity model, which can effectively defend against internal linking attacks faced by QS sets in aggregated datasets.

(3) We propose two simple and effective anonymization algorithms for the QS k-anonymity model.

The Greedy QS k-anonymity algorithm: The Greedy QS k-anonymity algorithm uses a greedy heuristic to find and compute the Cartesian product of records, while achieving higher data utility by comparing information loss.

The Efficient QS k-anonymity algorithm: The Efficient QS k-anonymity algorithm sorts the records in an aggregated dataset by the Hilbert transform, and then the algorithm traverses the dataset only once and calculates the Cartesian product of the records.

(4) We perform experiments on the Greedy QS k-anonymity algorithm and the Efficient QS k-anonymity algorithm in terms of data utility, efficiency, and scalability. Through a preliminary experimental evaluation, we demonstrate that our algorithms are practical and effective.

Our main contributions are as follows: We discuss the methods related to k-anonymity model and the data utility metrics in Section 2. We introduce the aggregated dataset and the internal linking attacks, while describing the motivation for our research in Section 3. Section 4 presents the novel privacy model and the design of our algorithms. Section 5 evaluates our approach based on experimental results. Finally, Section 6 concludes the paper and introduces the future work.

2. Related Works

2.1. k-Anonymity. Privacy is one of the most important issues in IoT and data fusion. In [21], a security and privacy algorithm for Unicode data is proposed in order to maintain privacy in the IoT ecosystem. In [22], the optimization of the generalization algorithm is achieved by generalizing quasi-identifiers with the same data type in the IoT data. In [23], Jiang, W. and Clifton, C. proposed a two-party framework that can generate k-anonymity data from two vertically split sources without disclosing the data from one site to the other. Or, in [24], k-anonymity for multi-source data is achieved by a semi-honest adversary model and a game-theoretic approach. Over the past decade, many approaches have been proposed to address privacy protection issues, and k-anonymity is one of the most prominent ways to protect privacy.

The *k*-anonymity model for privacy protection was first proposed by Samarati and Sweeney in 1998 [25], followed by Sweeney's publication in 2002 [7] which brought k-anonymity to widespread attention in the academic community. Over the years, *k*-anonymity algorithms have been implemented through generalization, suppression, clustering, and microaggregation, with algorithms varying depending on the application domain (e.g. data mining, data publishing) or privacy and data utility needs [8].

Among these algorithms, many methods achieve better anonymity through search strategies and optimization. For example, LeFevre et al. [12] achieved efficient full-domain k-anonymity algorithms through breadth-first search strategy and pruning strategy; they also proposed a multidimensional partitioning algorithm for k-anonymity in [13]. Liang and Samavi [14] proposed a k-anonymity optimization method. They proposed to express the k-anonymity optimization problem in a mathematical formulation and then found the equivalence class that minimized the information loss by an optimization solver. These methods do not rely on specific privacy-preserving scenarios and are generic anonymization algorithms that anonymize QIDs directly. Similar algorithms exist for [15–18].

Some methods redefine the relationship between QIDs and SAs in the context of specific privacy protection scenarios. Shi et al. [19] introduced new attributes concept called "quasi-sensitive attributes," which were not sensitive in themselves, but certain values or combinations of them might be associated with external knowledge, thus indirectly revealing sensitive information about individuals. Terrovitis et al. [20] proposed a k-anonymity algorithm based on a separation method that could be applied when some attributes were both QIDs and SAs. Sei et al. in [3] considered QIDs as SAs and proposed a new attribute named "sensitive quasi-identifiers," and then they achieved the protection of private data by anonymization and reconstruction algorithms. However, this method is suitable for usage scenarios with high privacy requirements, and the utility of the data is reduced after anonymization.

2.2. Utility Metrics. Many researchers use certain well-designed metric functions to measure the quality of anonymized data. A metric function tends to examine the quality of anonymized data from a certain perspective. According to previous literature, the most common measures include the discernibility metric (DM) [9], which sums the squares of the cardinality of the equivalence classes; the classification metric (CM) [10], which requires a class label to classify the tuples; the normalized certainty penalty (NCP) [11], defined by the sum of the ranges of QIDs in each equivalence class; and the global certainty penalty (GCP) [26], which is a normalization of the sum of the NCP of all equivalence classes. However, according to observations, while the equivalence classes with few records are feasible, DM does not reflect the distribution of records in a dataset [27]. Furthermore, the CM is more suitable when the purpose of anonymized data is to train a classifier. Therefore, we chose NCP and GCP as the information loss metric functions for the privacy model in the later section, which can reflect the cardinality and spatial extent of each equivalence class. For a single numeric attribute A_{num}, the NCP of an equivalence class E is defined as follows:

$$NCP_{A_{num}}(E) = |E| \frac{\max_{A_{num}} - \min_{A_{num}}}{\max_U - \min_L}, \tag{1}$$

where the numerator represents the range of the attribute A_{num} in the equivalence class E, and $\max_U$ and $\min_L$ are, respectively, the maximum and minimum allowed values for the attribute A_{num}. In addition, for a categorical attribute, which does not have natural order like numerical attributes, the NCP is defined through a taxonomy tree:

$$NCP_{A_{cat}}(E) = |E| \frac{|\text{level}(u)|}{|\text{level}(A_{cat})|}, \tag{2}$$

where $|\text{level}(u)|$ denotes the height of the lowest parent node u of the value of the categorical attribute A_{cat} in the equivalence class E and $|\text{level}(A_{cat})|$ denotes the height of the taxonomy tree of A_{cat}. Thus, the *NCP* of an equivalence class E is defined as:

$$NCP(E) = \sum_{i=1}^{d} NCP_{A_i}, \tag{3}$$

where d denotes the number of attributes in the equivalence class E, and A_i represents the i-th attribute either numerical or categorical. *NCP* denotes the information loss of an equivalence class, while the information loss of the entire anonymized dataset is measured by *GCP*, which is defined as

$$GCP(T) = \frac{\sum_{E \in T} NCP(E)}{d \cdot n}, \tag{4}$$

where n denotes the number of records in the original dataset. Obviously, a large *GCP* implies a high information loss of the anonymized dataset.

3. Challenges and Motivations

Aggregated datasets formed in IoT and Data Fusion scenarios may lead to new privacy disclosures. We first describe the formation of aggregated datasets.

IoT: The IoT refers to a network that connects any object to the Internet through information sensing devices (e.g. sensors, mobile phones, etc.) according to an agreed protocol for intelligent identification, monitoring, and management [28]. Typically, the data collected through different information sensing devices may be used directly or aggregated first and then used. The latter may result in the disclosure of sensitive information.

Data Fusion: Data Fusion is the process of cognition, synthesis, and judgment of multiple data. The data involved in fusion are often characterized by multiple sources, heterogeneity, and incompleteness. Data Fusion combines relevant information from multiple related databases to achieve higher accuracy and more

specific inferences than using individual data alone [29]. But similarly, the aggregation of data from multiple sources can easily lead to the disclosure of sensitive information.

We discuss the simplest case that exists in the above two scenarios, where the data in a dataset are sourced from two different information sensing devices or related databases. We classify the formation and publication of the aggregated dataset into three processes. In the data collection stage, two sets of data are collected from two different information sensing devices or related databases and stored in Dataset1 and Dataset2, respectively. In the data aggregation stage, the data in Dataset1 and the data in Dataset2 are aggregated to form the aggregated dataset which is to be published. In the data publishing stage, the aggregated dataset can be published directly or anonymized. We also describe the formation and publication of the aggregated dataset in Figure 1, and the anonymized dataset is indicated within the dotted line in the diagram.

We focus on the anonymization of aggregated datasets. In the next section, we will describe the new privacy disclosure faced by aggregated datasets.

3.1. Extra Privacy Disclosure. In addition to the three privacy disclosures of membership disclosure, attribute disclosure, and identity disclosure already considered [30], we find a new privacy disclosure in the aggregated dataset. Consider an example in Figure 2. Figure 2(a) shows a dataset containing *EI*, *QI D*, and *NSA*. The data in this dataset released with EI removed are able to provide vehicle information without causing privacy disclosure. Similarly, the data in Figure 2(b) released with EI removed are able to be used to count vehicle traffic information without causing privacy disclosure. Due to the need of statistics or analysis, sometimes the datasets need to be fused before use. Figure 2(c) shows the aggregated dataset after fusion by Dataset1 and Dataset2. The dataset is usually published with the EI removed, but even if the data publisher removes the license plate number when publishing the aggregated dataset, the data analyzer can still associate the vehicle information (registration date and color) from Dataset1 with the location information (latitude, longitude, and time) from Dataset2 to obtain additional sensitive information, such as inferring the specific license plate number, and thus leading to the disclosure of sensitive information.

The dataset in Figure 2(c) is considered as an aggregated dataset. The aggregated dataset may cause privacy disclosure when released. And, the aggregated dataset is formed by combining two datasets that do not result in privacy disclosure when released separately. For example, the attribute set containing Registration date and Color in Figure 2(c) is not sensitive itself and does not cause privacy disclosure, but linking to other attribute sets in aggregated dataset will cause privacy disclosure. We refer to this attribute set as a quasi-sensitive attribute set (QS set), and the attributes in it are called quasi-sensitive attribute (QS attribute). Therefore, we believe that a simple aggregated dataset may consist of EI, two QS sets (QS_1 and QS_2), and NSA.

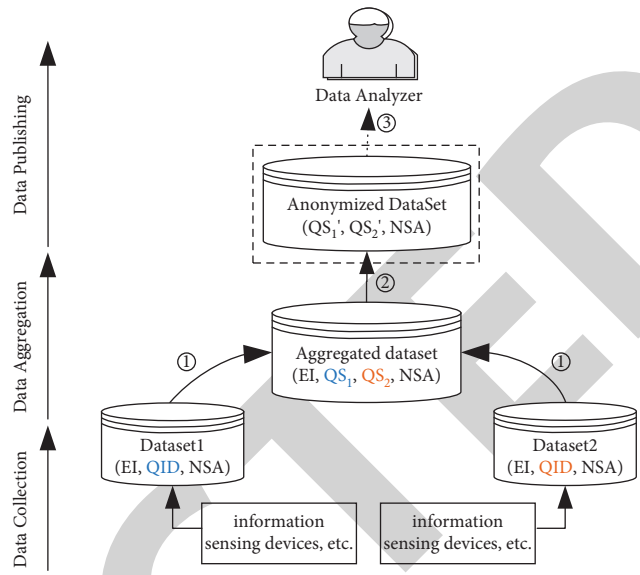


Figure 1: Formation and publication of aggregated dataset.

A privacy disclosure based on linkability [31] may exist in aggregated dataset. Linkability means that a data analyzer can successfully distinguish whether two IOI (items of interest) are linked and gain new knowledge by linking two IOI, even if he or she does not know the actual identity of the subject of the linkable IOI. The definition of linkability is based on Pfitzmann and Hansen's definition of unlinkability [32]. Linkability may lead to identification and inference. When a data analyzer links two IOI, the actual identity of the subject of the linkable IOI may be inferred from their links, leading to identification. In contrast to identification, inference is not limited to linking data belonging to the same person. Even if a data analyzer does not obtain the true identity corresponding to two IOI, he or she may infer relationships from certain related attributes (people with overlapping tracks, people who buy the same items, etc.) and try to generalize them, which may lead to privacy disclosure. The example in Figure 2 reflects the identification and inference that result from linkability. The attacks based on linkability are called internal linking attacks. Figure 3 illustrates the risk of privacy disclosure in aggregated dataset. Data analyzers are able to gain access to certain sensitive information by mining the information generated by the linkability of QS_1 and QS_2 in an aggregated dataset, posing new privacy disclosure.

3.2. Motivation. Based on the description of the aggregated dataset and its privacy disclosure in the above section, in this section we describe the motivation for our research. We first describe the additional knowledge available to the data analyzer: We assume that the data analyzer only can obtain some or all of the attribute values in QS_1 or QS_2 of a certain record in the aggregated dataset.

Through the analysis in the previous section, aggregated datasets can be subject to sensitive information disclosure if they are not processed by privacy-preserving technologies. As we mentioned above, k-anonymity is one of the most

EI	QID		NSA
license plate	Registration date	Color	Place of Origin
AJ1382	2013	White	America
AK3847	2018	Black	Germany
BQ3948	2015	Blue	Japan
DW5769	2019	Black	China

(a)

EI	QID		NSA
license plate	Location (°E/°N)	Time	Speed
AJ1382	118/22	21:00	65
AK3847	110/30	13:00	80
BQ3948	111/47	17:00	78
DW5769	110/30	13:00	85

(b)

EI	QS1		QS2		NSA	
license plate	Registration date	Color	Location (°E/°N)	Time	Speed	Place of Origin
AJ1382	2013	White	118/22	21:00	65	America
AK3847	2018	Black	110/30	13:00	80	Germany
BQ3948	2015	Blue	111/47	17:00	78	Japan
DW5769	2019	Black	110/30	13:00	85	China

(c)

QID'				NSA	
Registration date	Color	Location(°E/°N)	Time	Speed	Place of Origin
[2013,2015]	Color	[111,118]/[22,47]	[17:00,21:00]	65	America
[2018,2019]	Black	110/30	13:00	80	Germany
[2013,2015]	Color	[111,118]/[22,47]	[17:00,21:00]	78	Japan
[2018,2019]	Black	110/30	13:00	85	China

(d)

Figure 2: Vehicle dataset. (a) Dataset1. (b) Dataset2. (c) Aggregated dataset. (d) Anonymized dataset (2 anonymity).

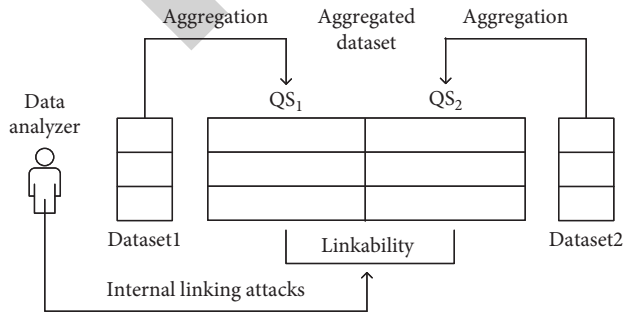


Figure 3: Disclosure risk of aggregated datasets.

widely used privacy-preserving methods in PPDP, but there are some limitations to the application of k-anonymity in aggregated datasets.

Limitation of use scenarios: As we said, the purpose of k-anonymity is to prevent privacy disclosure caused by linking attacks, so it handles QIDs that can be linked to external tables for privacy protection purposes. But for the aggregated datasets that may be generated in the IoT and Data Fusion scenarios, the data analyzer is concerned with the additional knowledge that can be gained through the linkage between the QS_1 and QS_2. However, k-anonymity does not take into account the

potential for internal linking attacks on aggregated datasets generated in IoT and Data Fusion scenarios.

Unable to defend against internal linking attacks: Internal linking attacks are caused by the linkage between QS_1 and QS_2 in the aggregated dataset. The attributes in the QS set are QIDs in a dataset before aggregation. If the aggregated dataset is anonymized using the k-anonymity method, all attributes in QS_1 and QS_2 will be anonymized to eliminate linkability between the QS sets in the aggregated dataset. However, we find that although k-anonymity hopes to achieve the goal of eliminating linkability by generalizing the values of attributes in QS_1 and QS_2, in some cases, it still cannot eliminate linkability between QS_1 and QS_2 and thus cannot resist internal linkage attacks. For example, Figure 2(d) shows the anonymized dataset after 2-anonymity, where the shaded parts represent two equivalence classes, respectively. A data analyzer who knows that the registration date is 2018 and the color is black, is able to easily combine the exact location and time information of the vehicle (since it is not anonymized) to infer sensitive information such as the license plate number of the vehicle. This is because k-anonymity may be achieved by generalizing only some of the QIDs.

In this case, we should consider how to eliminate the linkability between QS_1 and QS_2 in the aggregated dataset. Our proposed approach uses the QS k-anonymity to prevent data analyzer from mapping attribute values from one QS set to the other. Thereby, internal linkage attacks are effectively prevented.

In addition, the main relevant symbols and descriptions involved in this paper are shown in Table 3.

4. Models and Algorithms

To simplify our problem, we assume that there are only EIs and two QS sets (QS_1 and QS_2) in an aggregated dataset. In fact, in addition to the EIs and QS sets, the aggregated dataset also may contain NSAs.

Let QS be the set of attributes in the aggregated dataset and q be the number of these attributes (i.e. $q = |QS|$). Let QS_1 represent a QS set in the aggregated dataset and q_1 be the number of attributes in the QS set (i.e. $q_1 = |QS_1|$). Let QS_2 denote the other QS set in the aggregated dataset, and q_2 represent the number of attributes in this QS set (i.e. $q_2 = |QS_2|$). Then we can obtain the following relation that $QS_1 \cup QS_2 = QS$, $QS_1 \cap QS_2 = \varnothing$ and $q_1 + q_2 = q$.

Then, we define some basic concepts and present our privacy model.

4.1. Basic Definition

Definition 1 (Quasi-sensitive attribute set). An attribute set consisting of one or more attributes is a quasi-sensitive attribute set (QS set) if it is not sensitive itself but can be linked with other attribute sets to generate sensitive information. The attributes in the QS set are called quasi-sensitive attributes (QS attributes).

Definition 2 (Attack model). For a record r in an aggregated dataset, we assume that the data analyzer may only obtain some or all of its attribute values in QS_1 or QS_2.

Since the two datasets forming the aggregated dataset may have been partially published before aggregation, the data analyzer may obtain some or all of the attribute values in QS_1 or QS_2. But if the data analyzer obtains all the attribute values of a record at the same time, any anonymous method will be meaningless.

Definition 3 (Aggregated Dataset). An aggregated dataset (AD) may consist of explicit identifiers (EIs), two QS sets (QS_1 and QS_2), and nonsensitive attributes (NSAs).

Figure 1① shows the data aggregation process. The QS_1 and QS_2 in the aggregated dataset are derived from the QIDs in Dataset 1 and Dataset 2, respectively. As we mentioned in the previous section, the attributes in Dataset 1 and Dataset 2 do not cause privacy disclosure when they are published with EI removed. However, when they are aggregated to form an aggregate dataset, the aggregated dataset may face privacy disclosure risk even if the EI is removed.

Definition 4 (Linkability). Linkability occurs when QS_1 and QS_2 in a dataset AD are linked and some extra knowledge is generated. Based on the linkability, a data analyzer is able to gain extra knowledge by linking QS_1 and QS_2 in AD, which may contain some sensitive information with privacy implications. We refer to attacks based on linkability as internal linking attacks.

Definition 5 (Anonymized Dataset). An anonymized dataset (AD^*) may consist of QS_1', QS_2' and nonsensitive attributes (NSAs).

Figure 1② shows the formation process of the anonymized dataset. The data publisher removes the EI before publishing the aggregated dataset, while anonymizing the QS sets to break the linkability between QS_1' and QS_2'. Then the anonymized dataset is released for use by the data analyzer, as shown in process ③.

Our goal is to prevent internal linking attacks that may result in the disclosure of sensitive information, while making an effort to improve the utility of the anonymized dataset. Under this attack, according to our assumptions above, the data analyzer does not have access to the value of the attributes in both QS_1 and QS_2 for a record in AD at the same time. Next, we will construct our privacy model based on this attack hypothesis.

4.2. Proposed Privacy Models. According to the property of the aggregated dataset we described, the internal linkage attack can occur with higher probability only when the data analyzer obtains the accurate values of all the attributes in the QS_1 and QS_2. Therefore, it follows that we define a new privacy model QS k-anonymity to defend against internal linking attacks.

Table 3: Symbol and description.

Symbol	Description
$A\ D$	Aggregated dataset
AD^*	Anonymized dataset
k	Anonymity requirement
r	Records in the dataset
QS_i	QS sets in an aggregated dataset, $i \in \{1, 2\}$
q, q_1, q_2	Number of attributes in the attribute sets
$QS_{i,j}$	The j-th attribute in the QS_i
$R_{i,j}$	The set of the j-th attribute values in the QS_i of the records
$Cp_{i,R}$	Cartesian product of $R_{i,j}$
$\lvert Cp_{i,R}\rvert$	The size of the Cartesian product
A_k, B_k, C_k, D_k	Attribute values
n, N	Number of records and records set in $A\ D$
γ, C	Clusters
$\mathfrak{R}$, Clusters	Set of clusters
$D(x, y)$	The distance between records x and y
best_r	Best record
best_C	Best cluster
Hilbert	Hilbert transform function
NCP, GCP	Information loss metric function

Definition 6 (Equivalence Class). We define a set of records that contain all the same QS attribute values as an equivalence class.

For example, there are 2 equivalence classes in Figure 2(d), where the records 1 and 3 form one equivalence class, the records 2 and 4 form the other equivalence class.

Definition 7 (QS k-anonymity). The anonymized dataset AD^* satisfies QS k-anonymity if and only if for each record in AD^*, the probability of mapping QS attribute values from QS_1 to QS_2 while obtaining the exact value of all QS attributes in QS_2 is less than $1/k$, and the probability of mapping QS attribute values from QS_2 to QS_1 while obtaining the exact value of all QS attributes in QS_1 is also less than $1/k$.

Example 1. We still use the vehicle dataset mentioned above as an example. Figure 4 represents an example of the QS 4-anonymity of Figure 2(c). In Figure 4, bold face indicates the original values. Note that this is for clarity only. Our proposed approach is to represent the anonymized dataset with the combined values of the attributes in the QS sets in order to satisfy QS 4 anonymity. In Figure 4, if a data analyzer knows that the registration date and color are 2013 and white, respectively, there are four possible combinations of location and time that he or she can know, which are {110/30, 13: 00}, {110/30, 21: 00}, {118/22, 13: 00}, and {118/22, 21: 00}. The probability that the data analyzer obtains the exact combination of location and time values is 1/4, as is the probability of being able to correctly infer from the attribute values in the QS_1 and QS_2.

We provide two specific implementation algorithms for the QS k-anonymity model, the Greedy QS k-anonymity algorithm and the Efficient QS k-anonymity algorithm. The Greedy QS k-anonymity algorithm is able to provide good data utility through greedy search, and the Efficient QS k-anonymity algorithm provides efficient algorithmic efficiency through Hilbert transform. We will describe the specific implementation algorithms in detail in the next section.

Registration date	Color	Location(°E/°N)	Time
{2013,2018}	{Black,White}	{110/30,118/22}	{13:00,21:00}
{2013,2018}	{Black,White}	{110/30,118/22}	{13:00,21:00}
{2015,2019}	{Black,Blue}	{110/30,111/47}	{13:00,17:00}
{2015,2019}	{Black,Blue}	{110/30,111/47}	{13:00,17:00}

Figure 4: The QS 4-anonymity of Figure 2(c).

4.3. Algorithms. First, we describe the core method of the proposed algorithms. Then, two specific implementation algorithms are proposed to achieve QS k-anonymity while improving the utility of anonymized data as much as possible.

Let $QS_{i,j}$ denote the j-th attribute in the QS_i ($i \in \{1, 2\}$). For $QS_{i,j}$ in record r, the data publisher extracts $x - 1$ records from records other than r and creates the set $R_{i,j}$ containing the extracted records and the original record r (If the same attribute value exists in the records, the value is only recorded once in $R_{i,j}$). Then, the data publisher calculates the Cartesian products $Cp_{i,R}$ of $R_{i,1}, \ldots, R_{i,q_i}$, respectively, and inserts each element of the $R_{i,j}$ into the anonymized dataset. The value of x is taken such that $\lvert Cp_{i,R}\rvert$ is greater than or equal to the anonymity requirement k.

Example 2. Figure 5(a) shows the original dataset containing QS_1 and QS_2, where each QS set contains two attributes with attribute values denoted by A_k, B_k, C_k, D_k, respectively. We assume that the values in A_k, B_k, C_k, and D_k are not the same. Figure 5(b) shows the anonymized dataset, assuming that anonymity requirement $k = 4$. We

r_k	$QS_{1,1}$	$QS_{1,2}$	$QS_{2,1}$	$QS_{2,2}$
r_1	A_1	B_1	C_1	D_1
r_2	A_2	B_2	C_2	D_2
r_3	A_3	B_3	C_3	D_3
r_4	A_4	B_4	C_4	D_4
r_5	A_5	B_5	C_5	D_5
r_6	A_6	B_6	C_6	D_6
r_7	A_7	B_7	C_7	D_7
r_8	A_8	B_8	C_8	D_8

(a)

r_k	$QS_{1,1}$	$QS_{1,2}$	$QS_{2,1}$	$QS_{2,2}$
r_1	$\{A_1,A_5\}$	$\{B_1,B_5\}$	$\{C_1,C_5\}$	$\{D_1,D_5\}$
r_5	$\{A_1,A_5\}$	$\{B_1,B_5\}$	$\{C_1,C_5\}$	$\{D_1,D_5\}$
r_2	$\{A_2,A_7\}$	$\{B_2,B_7\}$	$\{C_2,C_7\}$	$\{D_2,D_7\}$
r_7	$\{A_2,A_7\}$	$\{B_2,B_7\}$	$\{C_2,C_7\}$	$\{D_2,D_7\}$
r_3	$\{A_3,A_8\}$	$\{B_3,B_8\}$	$\{C_3,C_8\}$	$\{D_3,D_8\}$
r_8	$\{A_3,A_8\}$	$\{B_3,B_8\}$	$\{C_3,C_8\}$	$\{D_3,D_8\}$
r_4	$\{A_4,A_6\}$	$\{B_4,B_6\}$	$\{C_4,C_6\}$	$\{D_4,D_6\}$
r_6	$\{A_4,A_6\}$	$\{B_4,B_6\}$	$\{C_4,C_6\}$	$\{D_4,D_6\}$

$QS_{2,1}$	$QS_{2,2}$
C_1	D_1
C_1	D_5
C_5	D_1
C_5	D_5

$QS_{1,1}$	$QS_{1,2}$
A_3	B_3
A_3	B_8
A_8	B_3
A_8	B_8

(b)

Figure 5: QS 4-anonymity by our proposed method. (a) Original dataset. (b) QS 4 anonymity.

select record r_1 as the original record and select record r_5 among the remaining records, and then generate $R_{1,1} = \{A_1, A_5\}$, $R_{1,2} = \{B_1, B_5\}$, $R_{2,1} = \{C_1, C_5\}$, and $R_{2,2} = \{D_1, D_5\}$ according to the anonymization algorithm. Therefore, for the attributes in QS_1 and QS_2, their Cartesian products are $Cp_{1,R} = \{(A_1, B_1), (A_1, B_5), (A_5, B_1), (A_5, B_5)\}$ and $Cp_{2,R} = \{(C_1, D_1), (C_1, D_5), (C_5, D_1), (C_5, D_5)\}$, respectively, of size $|Cp_{1,R}| = |Cp_{2,R}| = 4$. Even if the data analyzer knows all the attribute values in one QS set QS_1 or QS_2 in r_1, the data analyzer cannot specify the exact combination of attribute values in the other QS set with a probability greater than 1/4. Therefore the probability of the data analyzer making an accurate inference based on the QS_1 and QS_2 is also less than 1/4. For example, as shown in Figure 5(b), assuming that the data analyzer has access to the attribute values C_8 and D_8 in QS_2. The data analyzer does not know which of (A_3, B_3), (A_3, B_8), (A_8, B_3), (A_8, B_8) is the corresponding combination of attribute values in QS_1.

Because the size of the Cartesian product can be very large, the data publisher may generate an anonymized record in the "aggregated expression." Figure 5(b) shows the anonymized record in an aggregated expression. And, the shaded part represents the equivalence class. Next, we will give two specific algorithms for the implementation of QS k-anonymity.

4.3.1. Greedy Algorithm. We use a greedy algorithm to implement QS k-anonymity. We consider QS k-anonymity as a clustering problem. Thus, QS k-anonymity can be defined as follows:

Definition 8 (QS k-Anonymity Clustering). The QS k-anonymity clustering problem finds a set of clusters from the given n records according to the QS_1 and QS_2 such that the size of the Cartesian product of the attribute values in each QS set in each cluster is at least k $(k \le n)$, and all clusters are formed in such a way that the current information loss is minimized.

Let N represent the set of n records in $A\ D$. Let $Cp_{i,a}$ denote the Cartesian product of attribute values in QS_i in cluster a. Then, QS k-anonymity clustering $\Re = \{\gamma_1, \ldots, \gamma_m\}$ is denoted as:

(1) $\cup_{a=1,\ldots,m}\gamma_a = N$;
(2) $\forall a, b \in \{1, \ldots, m\}(a \neq b), \gamma_a \cap \gamma_b = \varnothing$;
(3) $\forall i \in \{1, 2\}, a \in \{1, \ldots, m\}, |Cp_{i,a}| \ge k$;
(4) $\sum_{\ell=1,\ldots,m}|\gamma_\ell| \cdot MAX_{a,b=1,\ldots,|\gamma_\ell|}D(r(\ell, a), r(\ell, b))$ is minimized.

Here $|\gamma|$ represents the size of cluster γ, $r(\ell, a)$ denotes the a-th record in cluster γ_ℓ, and $D(x, y)$ denotes the distance between records x and y.

Definition 9 (Distance between two records). Let m and n represent the number of numerical and categorical attributes in the dataset, and $r_a[A]$ represent the value of attribute A of record r_a. We define the distance between two records r_1 and r_2 in the dataset as

$$D(r_1, r_2) = \sum_{i=1,\ldots,m} \frac{|r_1[A_i] - r_2[A_i]|}{|D_i|} + \sum_{j=1,\ldots,n} \frac{|\text{level}(u_j)|}{|\text{level}(A_{j\text{cat}})|}, \tag{5}$$

where $|D_i|$ represents the value domain of the attribute A_i, $|\text{level}(u_j)|$ represents the height of the lowest parent node u_j of the categorical attribute $A_{j\text{cat}}$ in r_1 and r_2, and $|\text{level}(A_{j\text{cat}})|$ represents the height of the taxonomy tree of the categorical attribute $A_{j\text{cat}}$.

Several studies [33, 34] have shown that the optimal k-anonymity problem is an NP-hard problem. Therefore, to create a locally optimal solution for QS k-anonymity that is as close to the global optimal solution as possible, we employ a greedy approach. Figure 6 shows the main implementation of the Greedy QS k-anonymity algorithm, which is able to show the implementation of our algorithm in a more comprehensive way. The input to the algorithm is the original aggregated dataset $A\ D$ and the anonymity requirement k. First, record r is randomly selected from $A\ D$, and then entered in the loop until $A\ D = \varnothing$. Finally, Clusters is output, which contains all clusters that satisfy the anonymity requirement k. The loop process achieves finding the optimal clusters that satisfy the anonymity requirement k. And the detailed loop process will be described in the next paragraph.

The main algorithm is shown in Algorithm 1. Given a dataset $A\ D$ and anonymity requirement k, we first judge whether $A\ D$ satisfies the condition for starting anonymity (lines 2–4). We select a record r at random, then select the record farthest from r to add to cluster C (lines 7–8) and remove that record from dataset $A\ D$ (line 9). Then, we traverse the dataset $A\ D$ and select the record best_r that makes the smallest information loss to add to cluster C. Repeat this process (lines 10–14) until the size of Cartesian product of attribute values in the QS_1 and QS_2 in cluster C is greater than or equal to k. Then, we add cluster C to cluster Clusters. Repeat lines 7–15 until the size of the Cartesian product of attribute values in QS_1 or QS_2 for the remaining records is less than k. Then, we iterate over these remaining records, inserting each record into the cluster with the least incremental information loss (lines 16–23). We use NCP to compare the information loss of each cluster. The time complexity of the greedy $QS\,k$-anonymity algorithm is $O(n^2)$.

Due to the higher time complexity of the greedy $QS\,k$-anonymity algorithm, in practice, we can partition the original dataset $A\ D$. Dividing $A\ D$ into multiple small datasets to be anonymized separately can effectively improve the efficiency of the algorithm. And, for the choice of the partitioning method, in order to minimize the information loss caused by partitioning, the clustering method can be used for partitioning. Firstly, the similar records in the original dataset are clustered and divided into smaller datasets, which are then anonymized using the greedy $QS\,k$-anonymity algorithm.

4.3.2. Efficient Algorithm. The Greedy QS k-anonymity algorithm has a higher time complexity and lower algorithm efficiency because it needs to continuously traverse the whole dataset. In this section, we implement an anonymization algorithm based on Hilbert curve, which can improve the efficiency of the algorithm effectively and try to guarantee the utility of the anonymized dataset at the same time.

The Hilbert curve [35] is a well-known spatial mapping technique, and it is a continuous fractal capable of mapping every region in space to an integer. If two points are close in a multidimensional space, they will also be close in the Hilbert transform with high probability [27]. For example, Figure 7(a) shows the transformation of data from 2-D to 1-D. The dataset is completely ordered with respect to the 1-D Hilbert values.

In order to perform data mapping, a number must be assigned to each attribute value so that the attribute value can be sorted. For numerical attributes, we can use the attribute values directly due to their natural orderliness. For categorical attributes, each attribute value is assigned to a different integer based on the taxonomy tree. Figure 7(b) shows a taxonomy tree. We consider that the information loss between child nodes with the same parent is low. For example, the $NCP(\text{India}, \text{Japan}) = 1/2$, and their common parent is Europe. The $NCP(\text{Cambodia}, \text{England}) = 1$, and their common parent is Country. Therefore, when sorting the categorical attributes, we believe that the distance between attributes with the same parent node should be closer, as shown in Figure 7(b).

To efficiently implement the QS k-anonymity method, we propose our anonymization algorithm based on Hilbert curves. Figure 8 shows the main implementation process of the Efficient QS k-anonymity algorithm. The algorithm takes the original aggregated dataset $A\ D$ and the anonymity requirement k as input. First, a Hilbert transform is performed on $A\ D$ to obtain the ordered dataset D. Then, the loop is entered until $D = \varnothing$. The final output Clusters, contains all clusters that satisfy the anonymity requirement k. The purpose of the loop process is to find the optimal clusters that satisfy the anonymity requirement k. We will describe the detailed loop process in the following:

The main algorithm is shown in Algorithm 2. We first judge whether $A\ D$ satisfies the condition for starting anonymity (lines 2–4). And then we implement the mapping from d-D to 1-D by Hilbert transform. As we mentioned before, two close points in the multidimensional space are also close in the Hilbert transform with high probability. Therefore, by the Hilbert transform process, we achieve the sorting of the records with d-D attributes in the dataset $A\ D$ (line 5). Then, we iterate through the sorted dataset D and take the record r_i from dataset D to cluster C (line 10) until the size of the Cartesian product of the attribute values in the QS_1 and

Input: $A\ D$, k
Output: a set of clusters in each of which the size of Cartesian product of attributes in QS_1 and QS_2 is greater than or equal to k

(1) Clusters = ∅, $C = \emptyset$
(2) **if** $(|Cp_{1,A\ D}| < k \,\|\, |Cp_{2,A\ D}| < k)$ **then**
(3) **return** $A\ D$
(4) **end if**
(5) r is a randomly selected record in $A\ D$
(6) **while** $|A\ D| \neq \emptyset$ **do**
(7) r = the furthest record from r
(8) $C = \{r\}$
(9) $A\ D = A\ D - \{r\}$
(10) **while** $|Cp_{1,C}| < k \,\|\, |Cp_{2,C}| < k$ **do**
(11) $\text{best}_r \leftarrow \text{best\_record}(A\ D, C)$
(12) $C = C \cup \{\text{best}_r\}$
(13) $A\ D = A\ D - \{\text{best}_r\}$
(14) **end while**
(15) Clusters = Clusters $\cup\, C$
(16) **if** $(|Cp_{1,A\ D}| < k \,\|\, |Cp_{2,A\ D}| < k)$ **then**
(17) **while** $(|A\ D| \neq \emptyset)$ **do**
(18) r = *a* random tuple in $A\ D$
(19) $A\ D = A\ D - (r)$
(20) $\text{best}_C = \text{best\_cluster}(\text{Clusters}, r)$
(21) $\text{best}_C = \text{best}_C \cup \{r\}$
(22) **end while**
(23) **end if**
(24) **end while**
(25) **return** Clusters

Algorithm 1: The Greedy QS k-anonymity Algorithm.

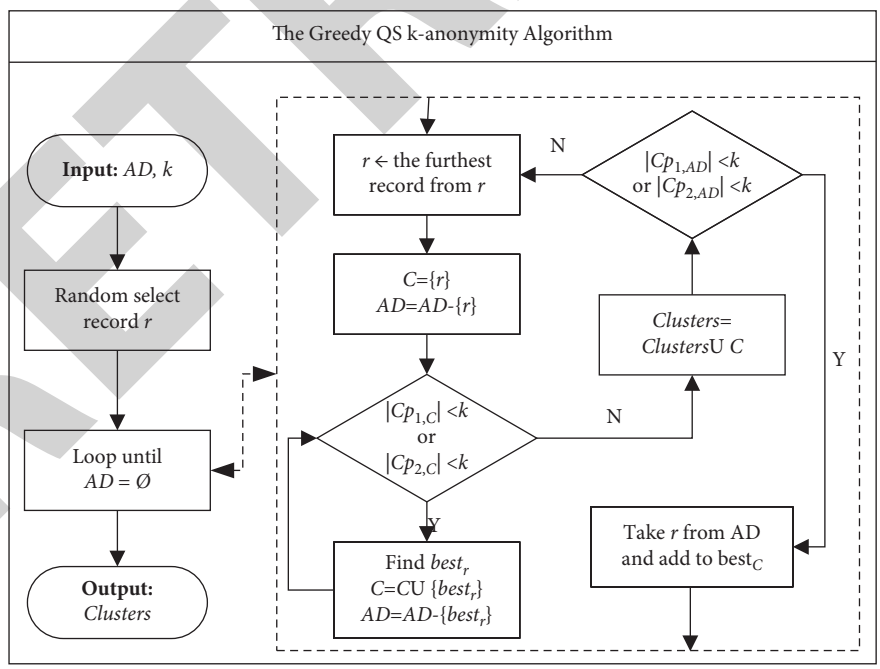


Figure 6: The main implementation process of the Greedy QS k-anonymity algorithm.

QS_1 in cluster C is greater than or equal to k (lines 9–11). Then, we add cluster C to the cluster Clusters. Repeat lines 7–14 until the size of the Cartesian product of the attribute values in the QS_1 or QS_2 of the remaining records in D is less than k. Then, we iterate through these remaining records, inserting each record into the cluster with the least incremental information loss (lines 16–21). We still use *NCP* tso compare the information loss of each

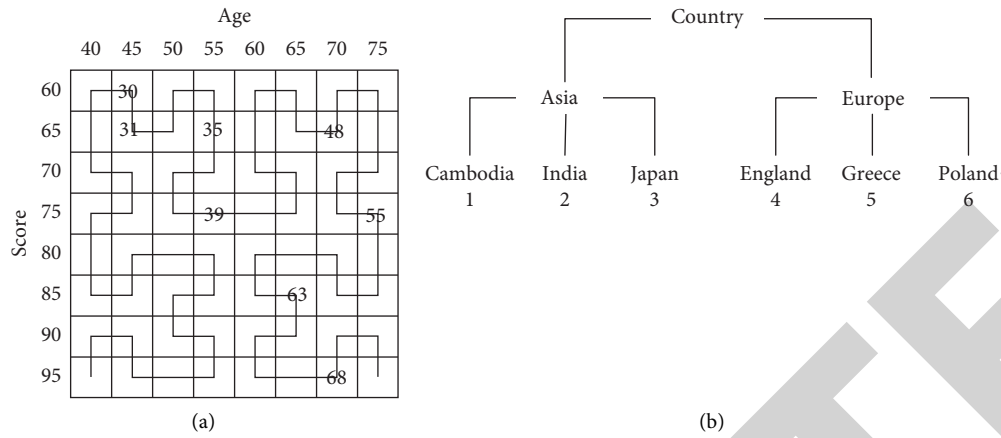


Figure 7: Multi-dimensional to 1-D mappings. (a) Hilbert curve. (b) Categorical attribute mapping.

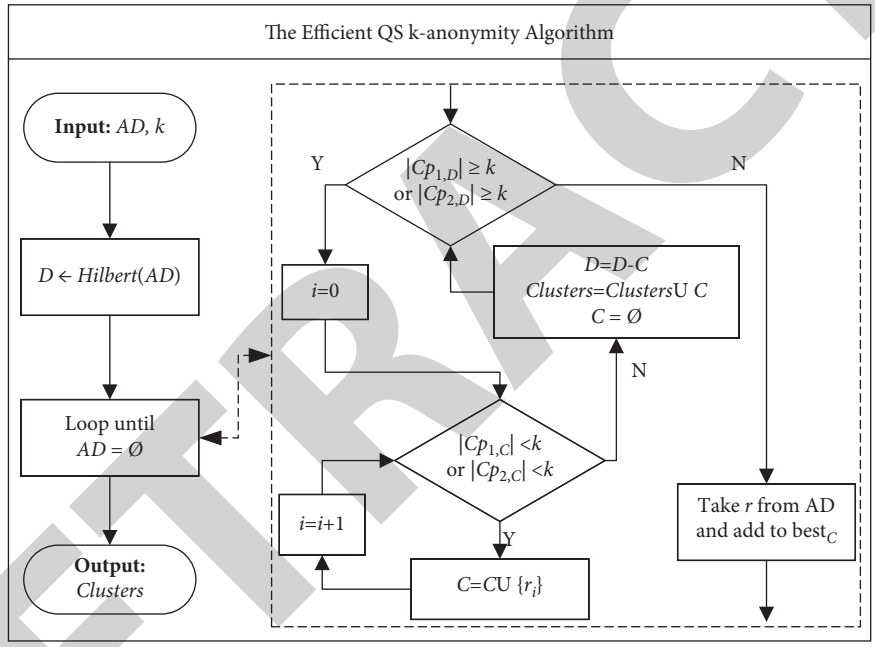


Figure 8: The main implementation process of the Efficient QS k-anonymity algorithm.

equivalence class. Finally, when representing the anonymized dataset, we sort the values of the attributes in each equivalence class in the Clusters in dictionary order, as shown in Figure 4.

The time complexity of the Hilbert transform is $O(d)$ for each record, so the algorithm is very efficient. Since the input dataset D is ordered after the Hilbert transform, our method only needs to scan the data once. Therefore, the I/O cost is linear.

5. Experimental Evaluation

In this section, we present the experimental evaluation of our practical algorithms in terms of data utility, efficiency, and scalability. In Section 5.1, we describe the dataset used for the experiments and the experimental environment setup. In Section 5.2, we provide the experimental results of our algorithms in terms of data utility and efficiency. In Section 5.3, we perform experiments on the scalability of our algorithms.

5.1. Experimental Setup

5.1.1. Dataset. We evaluated our proposed two algorithms in the publicly available dataset. For our experiments, we used the Adult dataset from the UC Irvine Machine Learning Repository [36]. The dataset includes 32561 records and 14 attributes. And 8 attributes in the Adult dataset were used in our experiment.

For QS k-anonymity, we considered {age, workclass, occupation, race} as attribute set QS_1 and {education-num, marital-status, gender, native-country} as attribute set QS_2. We considered age and education-num as numerical

Input: $A\ D$, k
Output: a set of clusters in each of which the size of Cartesian product of attributes in QS_1 and QS_2 is greater than or equal to k
(1) Clusters = $C = \varnothing$
(2) **if** $(|Cp_{1,A\ D}| < k \,\|\, |Cp_{2,A\ D}| < k)$ **then**
(3) **return** $A\ D$
(4) **end if**
(5) $D \leftarrow$ Hilbert $(A\ D)$
(6) **while** $|D| \neq \varnothing$ **do**
(7) **if** $(|Cp_{1,D}| \geq k \,\&\, |Cp_{2,D}| \geq k)$ **then**
(8) $i = 0$
(9) **while** $(|Cp_{1,C}| < k \,\|\, |Cp_{2,C}| < k)$ **do**
(10) $C = C \cup \{r_i\}$, $i = i + 1$
(11) **end while**
(12) $D = D - C$
(13) Clusters = Clusters $\cup\, C$
(14) $C = \varnothing$
(15) **else**
(16) **while** $(|D| \neq \varnothing)$ **do**
(17) $r = a$ random tuple in D
(18) $D = D - \{r\}$
(19) best_C = best_cluster (Clusters, r)
(20) $\text{best}_C = \text{best}_C \cup \{r\}$
(21) **end while**
(22) **end if**
(23) **end while**
(24) **return** Clusters

Algorithm 2: The Efficient QS k-anonymity Algorithm.

attributes, while the other six attributes were considered as categorical attributes.

5.1.2. Experimental Environment. The experiments were conducted on a machine equipped with a 2.30 GHz Intel(R) Core(TM) i7 processor with 16 GB RAM. The operating system on the machine was Microsoft Windows 10, and the implementation was built and run on IntelliJ IDEA 2021.2. The programming language we used is Java and the JDK version is 8.

5.2. Data Utility and Efficiency. In this section, we report the experimental results of the Greedy QS k-anonymity algorithm and the Efficient QS k-anonymity algorithm in terms of data utility and execution efficiency.

Figure 9(a) shows the variation of information loss with increasing k values for the two algorithms (The Greedy QS k-anonymity and The Efficient QS k-anonymity). We use the *GCP* to measure the information loss of the anonymized dataset. The higher the *GCP*, the greater the information loss. As shown in the figure, for all k values, the Greedy QS k-anonymity algorithm results in the lowest *GCP*. Meanwhile, the information loss of the two algorithms increases with the increase of the k values. The reason that the Greedy QS k-anonymity algorithm outperforms the Efficient QS k-anonymity algorithm in terms of data utility is that the Greedy QS k-anonymity algorithm traverses the dataset to find the optimal record based on the *NCP*.

We also measured the execution time of the Greedy QS k-anonymity algorithm and the Efficient QS k-anonymity algorithm under different k values. The results are shown in Figure 9(b). The execution time of the Greedy QS k-anonymity algorithm is higher than that of the Efficient QS k-anonymity algorithm, but we believe that the QS k-anonymity algorithm is still acceptable in practice because the anonymization process is usually considered as an offline process. Moreover, we can see that the execution time of the Efficient QS k-anonymity algorithm gradually decreases as the value of k increases. This is because the increase in the value of k leads to a decrease in the number of equivalence classes, and thus saves the time to compute the information loss of the equivalent classes. For the Greedy QS k-anonymity algorithm, the increase in the value of k leads to the increase in the size of the equivalence class, thus increasing the time to calculate the information loss of the equivalence class in each round.

5.3. Scalability. In this section, we examine the scalability of the algorithms. We discuss the data utility and execution time of the Greedy QS k-anonymity algorithm and the Efficient QS k-anonymity algorithm under different number of attributes and different number of records.

We first measure the impact of changes in the attribute sets QS_1 and QS_2 on the Greedy QS k-anonymity algorithm and the Efficient QS k-anonymity algorithm in terms of data utility and execution time when $k = 4$. Figure 10 shows the attributes in QS_1 and QS_2 at the time of measurement.

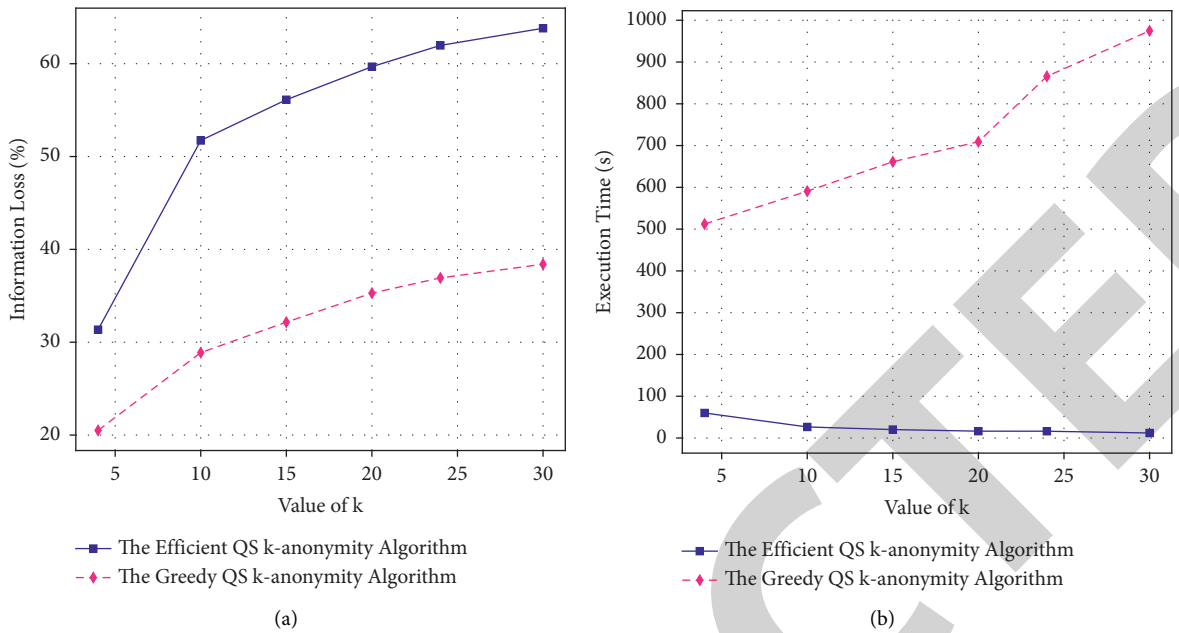


Figure 9: Variation of information loss and execution time with the value of k. (a) Information loss. (b) Execution time.

QS set	Attributes=2	Attributes=3	Attributes=4	Attributes =5	Attributes=6	Attributes=8
QS_1	\age	\age \workclass	\age \workclass	\age \workclass \occupation	\age \workclass \occupation	\age \workclass \occupation \race
QS_2	\education-num	\education-num	\education-num \marital-status	\education-num \marital-status	\education-num \marital-status \gender	\education-num \marital-status \gender \native-country

Figure 10: The attributes in QS_1 and QS_2.

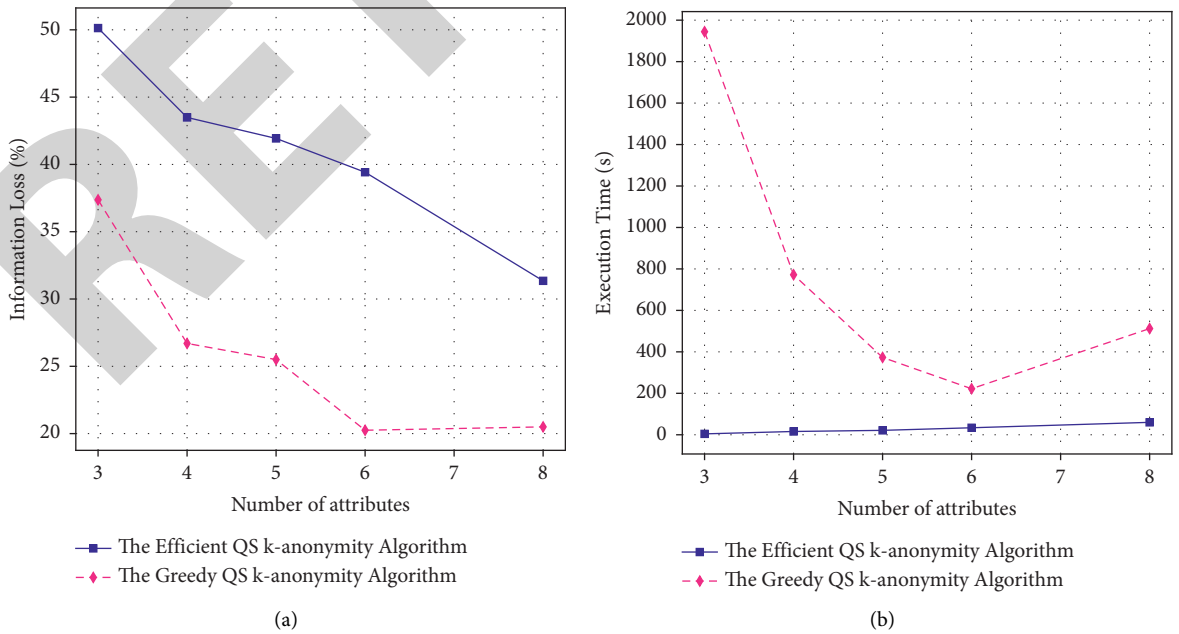


Figure 11: Variation of information loss and execution time with the number of attributes. (a) Information loss ($k = 4$). (b) Execution time ($k = 4$).

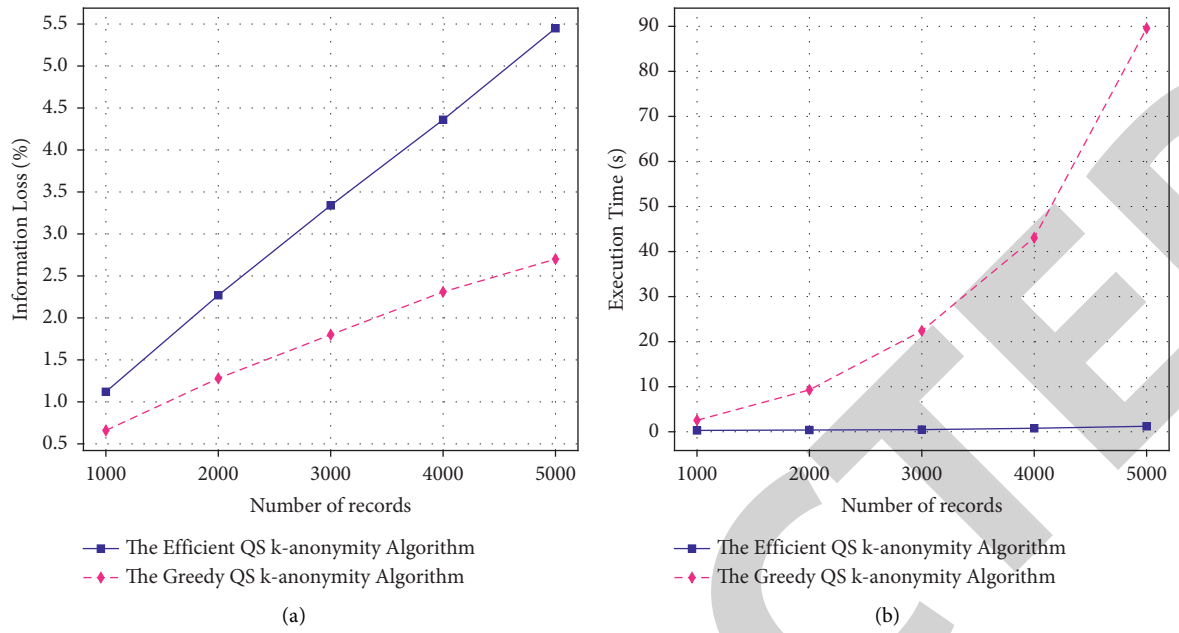


FIGURE 12: Variation of information loss and execution time with the number of records. (a) Information loss ($k = 4$). (b) Execution time ($k = 4$).

Figure 11 shows the results of our experiments. Again, the Greedy QS k-anonymity algorithm consistently outperforms the Efficient QS k-anonymity algorithm in terms of data utility, but the Efficient QS k-anonymity algorithm has the advantage of short execution time. We also find that for both the Greedy QS k-anonymity algorithm and the Efficient QS k-anonymity algorithm, the information loss in the anonymized dataset tends to decrease with increasing attribute values. This is because the k value constrains the size of the Cartesian product of the attributes in QS_1 and QS_2. Thus, for QS k-anonymity, the more attributes in QS_1 and QS_2, the easier it is to satisfy the constraint k on the size of the Cartesian product when anonymized, and the smaller the average equivalence class size formed, the lower the information loss after anonymization. Furthermore, in Figure 11(b), we can see that for the Greedy QS k-anonymity algorithm, the execution time of the algorithm tends to decrease with the increase in the number of attributes. This is because the increase in attributes enables the clusters to satisfy the anonymity requirement k faster and thus reduces the time to compute the information lost per round. For the Efficient QS k-anonymity algorithm, the execution time of the algorithm increases with the number of attributes. This is because the increase in the number of attributes increases the time for the algorithm to compute the information loss.

In addition, different attributes in the QS sets have different effects on the data utility and execution time of the algorithms. Therefore, for the experiments on the number of attributes, we obtain only a trend, but there may be fluctuations in the data utility and execution time of the algorithms in the change of the number of attributes.

Figure 12 shows the data utility and execution time behaviors of the Greedy QS k-anonymity algorithm and the Efficient QS k-anonymity algorithm for various dataset cardinalities (for $k = 4$). For this experiment, we use the subsets of Adult dataset with different sizes. As shown in the figure, the information loss of both algorithms increases almost linearly with the size of the datasets. The greedy QS k-anonymity algorithm introduces the lowest information loss for any size of dataset. Although the Greedy QS k-anonymity algorithm is slower than the Efficient QS k-anonymity algorithm, we believe that the time overhead is still acceptable in most cases, considering that it provides better data utility.

6. Conclusion and Future Work

The k-anonymity model has been extensively studied for privacy protection. The aggregated datasets formed in IoT and Data Fusion scenarios are exposed to a new attack, the internal linking attack. And, the k-anonymity model cannot defend against the internal linking attacks. We assume that there are two QS sets in an aggregated dataset which do not cause privacy disclosure when published separately but may cause privacy problems when linked to each other. We propose a new privacy model, namely, QS k-anonymity, and anonymization algorithms that can handle QS sets to prevent internal linking attacks. Through experiments on the real dataset, we demonstrate that our proposed approach is effective.

Our study focuses on aggregated datasets in the IoT and Data Fusion scenarios. In the current existing work, we assume that the data in the aggregated dataset comes from two information sensing devices or related databases, respectively. And, we discuss the internal linking attacks faced by the aggregated dataset under this assumption. However, in many situations, the data in an aggregated dataset may be from multiple sources due to the complexity of the application

scenario. Our proposed QS k-anonymity model and implementation algorithms are able to prevent internal linking attacks on the aggregated dataset, which is formed by data from two sources. However, the aggregated dataset from multiple sources has not been discussed in this paper yet.

In our future work, we plan to analyze the internal linking attacks on the aggregated dataset, which consists of data from multiple sources, while optimizing our QS k-anonymity model and algorithms to prevent internal linking attacks on aggregated datasets from multiple sources.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was supported by National Science and Technology Major Project (No.2016ZX05047003).

References

[1] C. Wang, K. Wu, T. Zhou, G. Yu, and Z. Cai, "Tsagen: Synthetic Time Series Generation for Kpi Anomaly Detection," *IEEE Transactions on Network and Service Management*, vol. 19, no. 1, 2021.

[2] B. C. Fung, K. Wang, A. W.-C. Fu, and S. Y. Philip, *Introduction to Privacy-Preserving Data Publishing: Concepts and Techniques*, CRC Press, Florida, FL, USA, 2010.

[3] Y. Sei, H. Okumura, T. Takenouchi, and A. Ohsuga, "Anonymization of sensitive quasi-identifiers for l-diversity and t-closeness," *IEEE Transactions on Dependable and Secure Computing*, vol. 16, no. 4, pp. 580–593, 2017.

[4] B. C. Fung, K. Wang, R. Chen, and P. S. Yu, "Privacy-preserving data publishing: a survey of recent developments," *ACM Computing Surveys*, vol. 42, no. 4, pp. 1–53, 2010.

[5] L. Sweeney, "Achieving k-anonymity privacy protection using generalization and suppression," *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, vol. 10, no. 05, pp. 571–588, 2002.

[6] P. Samarati, "Protecting respondents identities in microdata release," *IEEE Transactions on Knowledge and Data Engineering*, vol. 13, no. 6, pp. 1010–1027, 2001.

[7] L. Sweeney, "k-ANONYMITY: a model for protecting privacy," *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, vol. 10, no. 05, pp. 557–570, 2002.

[8] V. Ayala-Rivera, P. McDonagh, T. Cerqueus, and L. Murphy, "A systematic comparison and evaluation of k-anonymization algorithms for practitioners," *Transactions on data privacy*, vol. 7, no. 3, pp. 337–370, 2014.

[9] R. J. Bayardo and R. Agrawal, "Data privacy through optimal k-anonymization," in *Proceedings of the 21st International Conference on Data Engineering (ICDE'05)*, pp. 217–228, IEEE, Tokyo, Japan, April 2005.

[10] V. S. Iyengar, "Transforming data to satisfy privacy constraints," in *Proceedings of the Eighth ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, pp. 279–288, New York, NY, USA, July 2002.

[11] J. Xu, W. Wang, J. Pei, X. Wang, B. Shi, and A. W.-C. Fu, "Utility-based anonymization using local recoding," in *Proceedings of the 12th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, pp. 785–790, Philadelphia, PA, USA, August 2006.

[12] K. LeFevre, D. J. DeWitt, and R. Ramakrishnan, "Incognito: efficient full-domain k-anonymity," in *Proceedings of the 2005 ACM SIGMOD International Conference on Management of Data*, pp. 49–60, Baltimore, Maryland, June 2005.

[13] K. LeFevre, D. J. DeWitt, and R. Ramakrishnan, "Mondrian multidimensional k-anonymity," in *Proceedings of the 22nd International Conference on Data Engineering (ICDE'06)*, April 2006.

[14] Y. Liang and R. Samavi, "Optimization-based k-anonymity algorithms," *Computers & Security*, vol. 93, p. 101753, 2020.

[15] B. C. Fung, K. Wang, and P. S. Yu, "Top-down specialization for information and privacy preservation," in *Proceedings of the 21st International Conference on Data Engineering (ICDE'05)*, pp. 205–216, IEEE, Tokyo, Japan, April 2005.

[16] J.-W. Byun, A. Kamra, E. Bertino, and N. Li, "Efficient k-anonymization using clustering techniques, Advances in Databases: Concepts, Systems and Applications," *in International Conference on Database Systems for Advanced Applications*, Springer, New York, pp. 188–200, 2007.

[17] M. R. Sarrafi Aghdam and N. Sonehara, "Achieving high data utility k-anonymization using similarity-based clustering model," *IEICE - Transactions on Info and Systems*, vol. E99.D, no. 8, pp. 2069–2078, 2016.

[18] W. K. Wong, N. Mamoulis, and D. W. L. Cheung, "Non-homogeneous generalization in privacy preserving data publishing," in *Proceedings of the 2010 ACM SIGMOD International Conference on Management of Data*, pp. 747–758, Indianapolis, Indiana, USA, June 2010.

[19] P. Shi, L. Xiong, and B. C. Fung, "Anonymizing data with quasi-sensitive attribute values," in *Proceedings of the 19th ACM International Conference on Information and Knowledge Management*, pp. 1389–1392, Toronto, ON, Canada, October 2010.

[20] M. Terrovitis, N. Mamoulis, J. Liagouris, and S. Skiadopoulos, "Privacy preservation by disassociation," *Proceedings of the Vldb Endowment*, vol. 5, no. 10, pp. 944–955, 2012.

[21] B. Maram, J. M. Gnanasekar, G. Manogaran, and M. Balaanand, "Intelligent Security Algorithm for Unicode Data Privacy and Security in Iot," *Service Oriented Computing and Applications*, vol. 13, 2018.

[22] W. Mahanan, W. A. Chaovalitwongse, and J. Natwichai, "Data anonymization: a novel optimal k-anonymity algorithm for identical generalization hierarchy data in iot," *Service Oriented Computing and Applications*, vol. 14, no. 2, pp. 89–100, 2020.

[23] W. Jiang and C. Clifton, "A secure distributed framework for achieving k-anonymity," *The VLDB Journal*, vol. 15, no. 4, pp. 316–333, 2006.

[24] M. Noman, C. Benjamin, M. FungMourad, and Debbabi, "Anonymity meets game theory: secure data integration with malicious participants," *The VLDB Journal*, vol. 20, 2011.

[25] *Protecting Privacy when Disclosing Information: K-Anonymity and its Enforcement through Generalization and Suppression*, Cambridge, 1998.

[26] G. Ghinita, P. Karras, P. Kalnis, and N. Mamoulis, "Fast data anonymization with low information loss," in *Proceedings of the 33rd International Conference on Very Large Data Bases*, pp. 758–769, Vienna, Austria, September 2007.

Hindawi
Security and Communication Networks
Volume 2024, Article ID 9780872, 1 page
https://doi.org/10.1155/2024/9780872

Retraction

Retracted: A K-Means Clustering Algorithm for Early Warning of Financial Risks in Agricultural Industry

Security and Communication Networks

Received 8 January 2024; Accepted 8 January 2024; Published 9 January 2024

This article has been retracted by Hindawi following an investigation undertaken by the publisher [1]. This investigation has uncovered evidence of one or more of the following indicators of systematic manipulation of the publication process:

(1) Discrepancies in scope

(2) Discrepancies in the description of the research reported

(3) Discrepancies between the availability of data and the research described

(4) Inappropriate citations

(5) Incoherent, meaningless and/or irrelevant content included in the article

(6) Manipulated or compromised peer review

The presence of these indicators undermines our confidence in the integrity of the article's content and we cannot, therefore, vouch for its reliability. Please note that this notice is intended solely to alert readers that the content of this article is unreliable. We have not investigated whether authors were aware of or involved in the systematic manipulation of the publication process.

In addition, our investigation has also shown that one or more of the following human-subject reporting requirements has not been met in this article: ethical approval by an Institutional Review Board (IRB) committee or equivalent, patient/participant consent to participate, and/or agreement to publish patient/participant details (where relevant).

Wiley and Hindawi regrets that the usual quality checks did not identify these issues before publication and have since put additional measures in place to safeguard research integrity.

We wish to credit our own Research Integrity and Research Publishing teams and anonymous and named external researchers and research integrity experts for contributing to this investigation.

The corresponding author, as the representative of all authors, has been given the opportunity to register their agreement or disagreement to this retraction. We have kept a record of any response received.

References

[1] X.-T. Li and X.-H. Duan, "A K-Means Clustering Algorithm for Early Warning of Financial Risks in Agricultural Industry," *Security and Communication Networks*, vol. 2022, Article ID 3751539, 9 pages, 2022.

Hindawi
Security and Communication Networks
Volume 2022, Article ID 3751539, 9 pages
https://doi.org/10.1155/2022/3751539

Research Article

A K-Means Clustering Algorithm for Early Warning of Financial Risks in Agricultural Industry

Xue-Tong Li[1] and Xiao-Hua Duan[2]

[1]*College of Economics and Management, Xi'an Kedagaoxin University, Xi'an 710109, China*
[2]*School of Finance, Xi'an Eurasia University, Xi'an 710065, China*

Correspondence should be addressed to Xiao-Hua Duan; duanxiaohua@eurasia.edu.cn

Received 6 March 2022; Revised 24 March 2022; Accepted 4 April 2022; Published 28 April 2022

Academic Editor: Fang Liu

As the primary industry, agricultural industry is the basis of guaranteeing people's basic life and national economic development. Agricultural industrial finance/financial is a weak link in the financial system, which seriously hinders the emergence of agricultural scale effect and the improvement in agricultural production efficiency. In order to find the financial risk of agricultural industry in time, this article proposes an agricultural industry financial risk early warning system based on improved K-means clustering algorithm. Because the traditional K-means algorithm is easy to fall into local optimization in the clustering process, the clustering effect is not reliable. In this article, the idea of immune cloning and particle swarm optimization location update is added to the grey wolf optimization algorithm. Grey wolf optimization algorithm and K-means algorithm are combined to solve the problem that K-means algorithm is easy to fall into local optimization. In the experimental part, through comparative verification, it can be found that the prediction performance of this system is superior to other models. Its practical application value is higher. Therefore, choosing this system for early warning of agricultural industry finance can effectively improve the accuracy of early warning and provide guarantee for the economic development of agricultural industry.

1. Introduction

Agricultural industry finance is a relatively weak link in China's financial system. The financial demand in rural areas mainly includes the demand for productive loans, including planting, breeding, animal husbandry, deep processing of agricultural products, etc. It has long cycle and low income and is greatly affected by natural factors. Agriculture-related loans have instability risk and high service cost. The supply of rural formal finance is insufficient, and the structural contradiction is more prominent. Its financial ecology is fragile and the risk of guarantee chain is large. At the same time, the insufficient supply of rural formal finance provides space for the development of underground finance. Some individuals are engaged in insurance and deposit business under the guise of Internet finance and farmer cooperatives, so that illegal fundraising problems often occur. Therefore, the study of rural financial risk has very important practical significance.

There are four main causes of rural financial risk in China [1]. First, the uncertainty of agricultural economy. At present, there are some problems in China's agricultural economy, such as scattered scale, ineffective formation of production chain, low level of agricultural science and technology, and unpredictable natural disasters. Therefore, farmers' production and income are reduced, their ability to repay loans is weakened, and the risk of small agricultural loans is formed. Second, the resource allocation of agricultural financial institutions is unreasonable. The cost and income of financial service supply are upside down. Some state-owned commercial banks are shrinking in rural areas, and the service object and scope of policy banks are relatively single. The governance mechanism of rural credit cooperatives has not been fundamentally solved. The level of

internal control management is relatively low, the electronization of rural banks and the construction of core business system are backward, and the quality of employees needs to be improved. Third, the rural credit environment is imperfect and lacks an effective punishment mechanism for dishonesty. Intermediary services are not standardized, providing false credit certificates. Meanwhile, fraudulent loans and malicious evasion of debts occur from time to time. Fourth, the construction of risk early warning system and prevention mechanism of rural financial institutions is not in place, so it is difficult to find and warn rural financial risks in time.

In order to predict the agricultural industry finance, domestic and overseas scholars at home and abroad have made positive contributions [2]. As for the risk of accounts receivable financing, some scholars have proposed that most of the customers of global accounts receivable financing are small and medium-sized enterprises, and there are hidden risks in the international accounts receivable factoring business [3]. The longer the maturity time of accounts receivable, the higher the risk. The provider of accounts receivable financing funds should also pay attention to the risk of changes in the value of suppliers' accounts receivable [4]. Meanwhile, there are some problems in accounts receivable financing, such as legal supervision, bank enterprise information asymmetry, etc [5]. The smooth implementation of accounts receivable financing of commercial banks needs to reduce the moral hazard of core enterprises and carry out dynamic risk monitoring of financing enterprises [6]. Because China is a large agricultural country, the development of agricultural industry is largely limited by the supply chain transportation industry. Therefore, the development of supply chain finance business affects agricultural finance business. As for the research on risk assessment with supply chain financial business as a whole, scholars choose the assessment indicators of supply chain financial risk from the aspects of core enterprises, financing enterprises, financing projects, and supply chain operation [7]. At the same time, the methods of supply chain financial risk assessment mainly include objective methods, support vector machine (SVM), fuzzy comprehensive evaluation method, game model, entropy weight TOPSIS model [8–11]. Due to the different methods, indicators and samples used by scholars in the research of supply chain financial risk, there are some differences in the composition and evaluation results of supply chain financial risk. However, it is generally believed that it is necessary to pay attention to the possible risks in the supply chain financial business and take corresponding preventive measures. Under different supply chain financial models, the focus of risk evaluation indicators may be different. Therefore, this article takes agricultural listed enterprises of small and medium-sized enterprises as an example and establishes a risk evaluation index system of accounts receivable financing of small and medium-sized enterprises based on fully considering the characteristics of accounts receivable financing mode. In this way, the credit risk of accounts receivable financing of small and medium-sized enterprises can be truly reflected and the decision-making basis can be provided for the practice of accounts receivable financing of small and medium-sized enterprises.

In order to improve the early warning ability of agricultural financial risk, this article improves the problem that K-means clustering algorithm is easy to local optimal solution and proposes an agricultural financial risk early warning system based on improved K-means clustering. The innovations and contributions of this article are listed below:

(1) The elite individuals in the iterative process of grey wolf optimization algorithm are deeply mined to improve the in-depth exploration ability of grey wolf optimization algorithm and avoid the premature convergence of grey wolf optimization algorithm.

(2) In order to expand the scope of prey search in the field of elite individuals and give full play to the residual value of elite individuals, the idea of monomer position update of particle swarm optimization algorithm is combined with the original grey wolf position update. The improved grey wolf optimization algorithm is combined with the classical K-means algorithm to solve the problem that K-means algorithm is easy to fall into local optimization.

(3) The financial risk early warning experiment of agricultural industry is carried out to verify the effectiveness of this system.

The rest of the article is organized as follows: Section 2 details the financial risk prediction model of agricultural industry based on K-means clustering algorithm, Section 3 illustrates the system design, Section 4 is about experimental simulation and analysis, and Section 5 is the final concluding section of the article.

2. Financial Risk Prediction Model of Agricultural Industry Based on K-Means Clustering Algorithm

2.1. Grey Wolf Optimization Algorithm (GWO). GWO algorithm is a mathematical expression of social hierarchy and predation behaviour in grey wolf population. The hierarchy of GWO algorithm is divided into four, namely α, β, δ, and ω Wolf. Let the grey wolf population with population size n be: $I = \{i_1, i_2, \ldots, i_T\}$. The best value of the candidate solution in the grey wolf population is taken as α Wolf, second best value as β Wolf, the third best value as δ Wolf, the remaining candidate solutions are set to ω Wolf. In GWO algorithm, by α, β, and δ as a leader, the wolf searches for the optimal solution within the specified range, and ω under the leadership of the three wolves, the wolves updated their positions. The mathematical model of GWO algorithm is as follows:

In the process of grey wolf searching prey, the distance between each wolf and prey can be expressed by the following formula:

$$D = \left| C \cdot I_u(n) - I(n) \right|, \tag{1}$$

$$I(n+1) = I_u(n) - G \cdot D, \tag{2}$$

where $I_u(n)$ represents the position vector of prey, $I(n)$ represents the position vector of grey wolf, D represents the distance vector between grey wolf and prey, and N represents the number of iterations. The calculation formulas of coefficients G and C are as follows:

$$G = 2g \cdot r_1 - g, \tag{3}$$

$$C = 2 \cdot r_2. \tag{4}$$

In the process of encirclement, the value of g linearly from 2 to 0, and r_1 and r_2 are random vectors in [0, 1].

Grey wolves have the ability to judge the location of prey and surround prey. Preservation α, β, and δ wolves are the first three best solutions obtained in the population. And force other search agents (ω (Wolf) according to α, β, δ the wolf's position updates its position. Other search agents and α, β, δ the wolf distance can be expressed by the following formula:

$$\begin{cases} D_\alpha = \left|C_1 \cdot I_\alpha - I\right|, \\ D_\beta = \left|C_2 \cdot I_\beta - I\right|, \\ D_\delta = \left|C_3 \cdot I_\delta - I\right|. \end{cases} \tag{5}$$

After the distance of each wolf is obtained, the individual position of grey wolf is updated through the following formulas:

$$\begin{cases} I_1 = I_\alpha - G_1 \cdot (D_\alpha), \\ I_2 = I_\beta - G_2 \cdot (D_\beta), \\ I_3 = I_\delta - G_3 \cdot (D_\delta), \end{cases} \tag{6}$$

$$I(n+1) = \frac{I_1 + I_2 + I_3}{3}. \tag{7}$$

Although GWO algorithm has strong search ability, the population diversity is decreasing with the increase of iteration times. The difference between individuals is getting smaller and smaller, and the optimal value cannot be found in the search space. Premature convergence may occur, which will affect the performance of GWO algorithm. Therefore, GWO algorithm is improved based on immune cloning theory and particle swarm optimization position update idea. Immune cloning selects elite individuals from the population and performs cloning and mutation operation on them to increase the diversity of the population and avoid premature convergence of the algorithm. Then, the position change idea of a single grey wolf is introduced to increase a certain mutation ability to the change of grey wolf position, so as to improve the global search ability of the algorithm.

2.2. Immune Clone Selection Operation. The essence of immune clonal selection is to select elite individuals from the population according to individual fitness value, and clone and mutate the elite individuals to form a new species group. Then elite individuals are selected from the new population to enter the next iteration until the maximum iteration number of immune clone selection is reached. Applying it to the grey wolf optimization algorithm is a more in-depth exploration of the elite individuals in the original grey wolf population, so as to expand the search scope and improve the population diversity. The detailed steps of clone selection are as follows:

Step 1: select m individuals with good fitness from the grey wolf population according to the fitness function value to form an elite population (set the m value to 1/4 of the number of grey wolf individuals).

Step 2: clone all grey wolf individuals in the elite population. The clone size is directly proportional to the number m of the selected elite population to form a temporary population T with the size of NC. The calculation of NC is as follows:

$$T_c = \sum_{x=1}^{w} \text{round}\left(\frac{\lambda w}{x} + h\right). \tag{8}$$

The round () function is a rounding function. λ is a random number between [0, 1]. H is an integer constant and $h \geq 1$. Compared with the original population t, the size of T_c is positively correlated with the value of h, which can ensure that each individual in the elite population has a certain number of clones.

In step 3, high-frequency mutation is implemented for each individual in the population to obtain better candidate solutions near elite individuals. The variation operation is shown in the following formulas:

$$n_x^{\text{new}} = n_x + u \cdot \eta \cdot n_x \cdot r_4 - u \cdot \eta \cdot n_x \cdot r_5, \tag{9}$$

$$u = \begin{cases} 1, & r_6 \leqslant 0.5, \\ 0, & \text{other}, \end{cases} \tag{10}$$

$$\eta = 1 - (1/(exp(1) - 1)) \times (exp(x/(x_{\max} - 1)) - 1), \tag{11}$$

where n_x is the individual of the xth iteration of population n; n_x^{new} is a new individual produced by n_x after mutation operation; r_4, r_5, r_6 are random numbers between [0, 1]; X stands for iteration x; $x_{\max}$ represents the maximum number of iterations of immune cloning operation; and η is a clonal variation parameter. It can be seen from formula (11) that the number of iterations is negatively correlated with the clone variation parameter η. η is close to 1 at the beginning, with a wide range of variation. At this point, a global range search is performed to ensure population diversity. As the number of iterations increases, the value of η gets closer and closer to 0, indicating that local searches are performed within a small range to increase fine-tuning capability and ensure the accuracy of the search.

Step 4: select w better individuals from N as the elite individual population for the next iteration until the maximum number of iterations of immune cloning operation is reached.

2.3. Particle Swarm Location Update Idea. In the grey wolf optimization algorithm, it can be seen from formula (5) that the position change of grey wolf is mainly to explore the prey position according to the position of three wolves. Then, three wolves (α, β, and δ) led the position update. Because we are now facing the elite population, the information contained in the prey search results of each elite individual may have an impact on the search results of the final location of the prey. Therefore, it is necessary to consider the location information of a single elite individual, so as to maximize the utilization rate of elite individuals and expand the search range of prey around elite individuals.

This article is inspired by the idea of location update of particle swarm optimization algorithm. It introduces the position change idea of a single grey wolf into the grey wolf position update to avoid premature convergence of the algorithm. Adjust the update strategy of formula (7) accordingly as follows.

$$I(n+1) = \frac{I_1 + I_2 + I_3}{3} + q(n), \tag{12}$$

where the position change $q(n)$ of a single grey wolf is expressed as the following formula:

$$\begin{aligned} q(n+1) = m\big(&q(n) + C_1 \cdot r_7\big(I_1 - I(n)\big) \\ &+ C_2 \cdot r_8\big(I_2 - I(n)\big) + C_3 \cdot r_9\big(I_3 - I(n)\big)\big), \end{aligned} \tag{13}$$

where m is the random number between [0, 1]. After many simulation experiments, when the value of m is between [0.6, 1], the algorithm has better search performance and more accurate optimization results. When m is large, it has better global search ability. When w is small, the local search ability is strong, which can effectively avoid premature convergence. r_6, r_7, r_8 are random numbers between [0, 1]. C_1, C_2, C_3 are obtained from formula (4). I_1, I_2, I_3 are obtained from formula (6). $I(n)$ represents the current position of the grey wolf.

2.4. Clustering Algorithm Based on GWO and K-Means. Because the input data of agricultural financial risk is usually in the format of text document, and the text document belongs to unstructured data, this article needs to preprocess the text document before text clustering. Convert text data type to data that can be input by GWO K-means algorithm. The basic steps of text preprocessing are text word segmentation, removal of stop words, text feature selection, and text vectorization.

This article uses Jieba word segmentation in Python to segment text documents and remove stop words. Commonly used text representation models mainly include Boolean space model (BM) [12], suffix tree model (STM) [13], vector space model (VSM) [14], and probabilistic retrieval model (PM) [15]. In this article, the most classical text vector model (VSM) is used for text vectorization. For document D, it is represented by $(nf - xdf_1, nf - xdf_2, \ldots, nf - xdf_t)$. The calculation formula of $nf - xdf$ is as follows:

$$nf - xdf(n, D) = \frac{lh(nf(n, D) + 0.1) \times lh(T/t_x)}{\sqrt{\sum_{x=1}^{t} \left[lh(nf(n, D) + 0.1) \times lh(T/t_x)\right]^2}}, \tag{14}$$

where t_x is the number of documents containing the word n_x, T is the total number of documents, and $nf(n, d)$ indicates the number of times the word n_x appears in document D.

In this article, GWO and K-means algorithm are used for text clustering analysis. Specifically, GWO algorithm is used to find a group of optimal clustering centres to minimize the distance from all texts in each category to the group of clustering centres, that is, the similarity of each document is the largest. In GWO algorithm, the fitness function is the goal of grey wolf to find the optimal solution. In K-means algorithm, the sum of intraclass distances is an important index to measure the advantages and disadvantages of clustering algorithm. The smaller the value, the better the clustering performance. The purpose of the combination of GWO and K-means algorithm is to use the powerful optimization ability of GWO algorithm to accurately find the optimal clustering centre. Text documents are classified by the clustering centre. This article selects the sum of the intraclass distances between text documents as the fitness evaluation function of GWO algorithm. As shown in formula:

$$Y = \sum_{y=1}^{Z} \sum_{\forall s_x \in c_y} d\left(s_x, c_y\right)^2, \tag{15}$$

where z stands for clustering category.

3. System Design of This Article

The structure of agricultural industry financial risk early warning system should be considered from three aspects. It includes acquisition system, which is used for data acquisition and input. It specifically includes macro financial data, risk event data, etc. There is also a database system for inductive analysis of data. And the most critical early warning system for risk prediction and monitoring (as shown in Figure 1).

In the process of information collection, it is necessary to adopt the means of data mining, assisted by manual intervention to collect and sort out the data. The direction of data mining can include crawler technology and scanning monitoring technology, such as risk event crawler and scanning monitoring of risk indicators. The architecture of the acquisition system is shown in Figure 2.

The amount of data collected is huge and comes from a wide range of sources, which cannot be measured by a unified standard. Therefore, further induction and analysis are needed, and the rationality and function of the database system are highlighted. By means of improved K-means clustering algorithm, the early warning model is trained through a large number of data to improve the early warning of agricultural financial risk early warning system. The system architecture is shown in Figure 3.

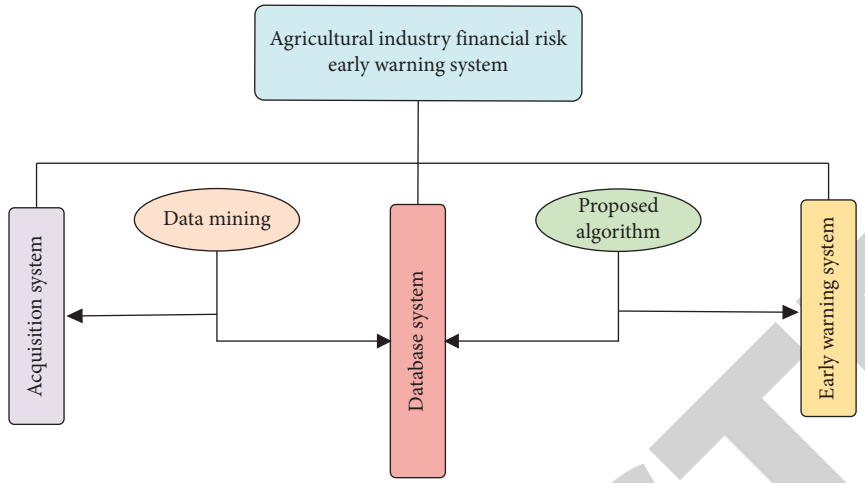


Figure 1: The structure diagram of agricultural industry financial risk early warning system.

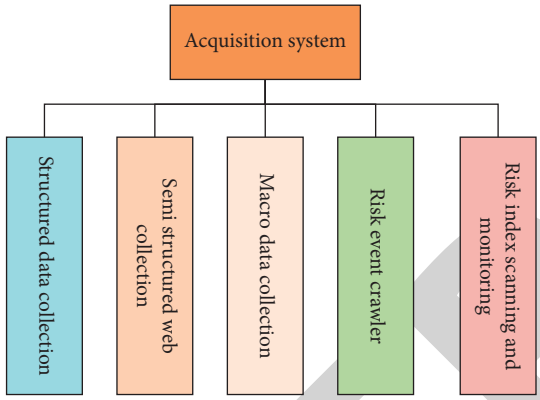


Figure 2: Acquisition system architecture diagram.

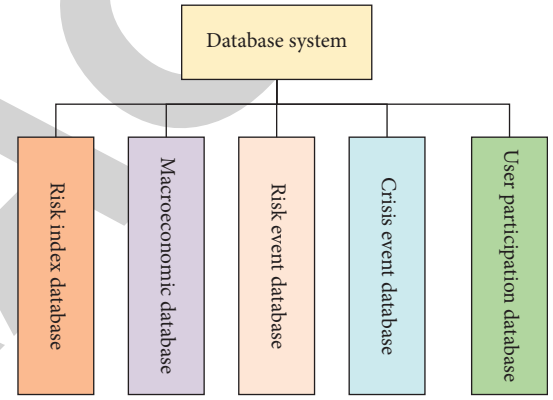


Figure 3: The database system architecture.

Early warning system is the explicit output part of the whole agricultural industry financial risk early warning system. Its coverage include risk analysis, prediction analysis, and early warning tracking. Considering that there may be some deviation between the predicted results and the actual results, it is necessary to introduce technical means such as improved K-means clustering algorithm in this article. The predicted results and the actual results are constantly compared and analyzed, and the results are constantly optimized through a large amount of data training. Finally, the prediction results are constantly improved, and the scientificity and accuracy of the results are also improved. Considering that there are many sudden risk factors in financial activities, it is necessary to rely on human intervention. Moreover, the changes of financial activities are very fast and are constantly updated and iterated. Therefore, the early warning system should also be accompanied by a correction algorithm. Continuously iterate and upgrade to optimize the system. The architecture of the early warning system is shown in Figure 4. In the training stage, the model is implemented by human participation. In the experimental testing stage, it is learned and corrected by the model itself.

4. Experiment and Analysis

4.1. Data Collection and Sorting. A total of 3,812 enterprise data sets of listed companies from 2,000 to 2,020 were extracted from Cathay Pacific and other databases. After data cleaning, enterprise data sets are divided according to whether they are in ST (special treatment) state, and 472 ST enterprise data sets and 3,167 normal enterprise data sets are obtained. In addition, according to the company information recorded in the data set, we sorted out the high-dimensional feature collection based on the financial characteristics of agricultural industry and nonagricultural industry. This study divides the characteristics of enterprises by agricultural industrial financial indicators and nonagricultural industrial financial indicators. The training set and test set are obtained by multilevel division based on business ability, profitability, growth ability, and management structure.

4.2. Characteristic Causal Analysis. In the ST enterprise data set, if the company is repeatedly in ST within the time range studied in this article, the timeline of being in ST for the first

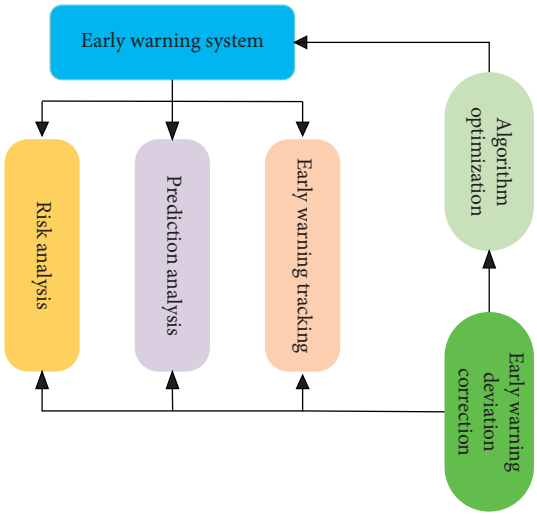


Figure 4: Architecture of early warning system.

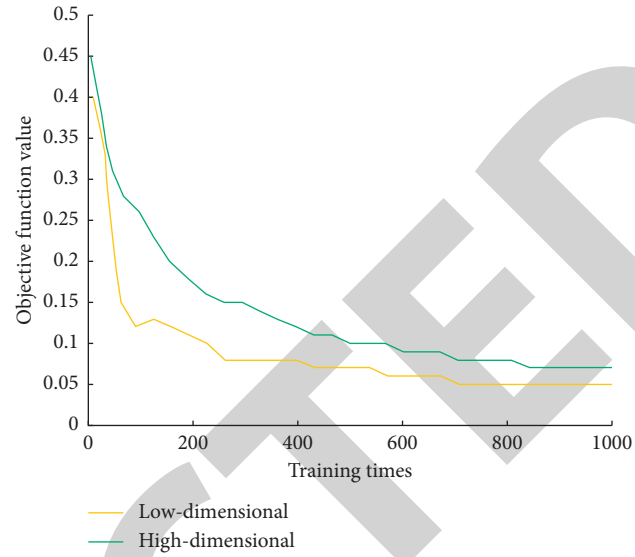


Figure 5: Training of high-dimensional and low-dimensional integrated classifier.

time shall prevail. According to the timeline of ST for the first time or the timeline recorded in the normal data set, the stability of ST data set and normal data set is tested. After the stationarity test is completed, the code is constructed according to the dimensionality reduction steps of the model in this study, and the low-dimensional feature collection corresponding to the high-dimensional feature table is obtained through iterative training.

4.3. Integrated Classifier Training. As shown in Figure 2, the low-dimensional feature collection (including nonagricultural industrial financial low-dimensional feature collection and agricultural industry financial low-dimensional feature collection) is used as the first training data set to train the integrated classifier. By monitoring the function value object^K of the objective function, the curve between the function value and the training times is constructed. At the same time, in order to compare the excellence of low-dimensional feature collection with high-dimensional feature collection in the training process of integrated classifier, high-dimensional feature collection (including nonagricultural industrial finance high-dimensional feature collection and agricultural industrial finance high-dimensional feature collection) is taken as the second training data set. The integrated classifier is trained to get the training comparison diagram of low-dimensional feature collection and high-dimensional feature collection in the integrated classifier (see Figure 5).

According to Figure 3, when using low-dimensional feature collection to train the integrated classifier, the training times reach 700, the change range of the target value tends to be stable. The average value of the target value is 0.0519, and the training of the integrated classifier is completed. When using high-dimensional feature collection to train the integrated classifier, the change range of the target value tends to be stable after 900 times of training. And the average value of the target value is 0.0636. It can be seen that the low-dimensional feature collection obtained by using the feature causal analysis in this model is more conducive to the training of integrated classifiers in terms of training times, target value, and stability.

Literature [16] and literature [17] are relatively typical models with feature analysis and financial early warning function of agricultural industry. In order to explore the comparative results of this model with literature [16] and [17] model, data enrichment was performed on the second training data set above to obtain the third training data set. Proposed model, literature [16] model, and literature [17] model were successively trained to obtain the comparison figure (see Figure 6).

According to Figure 6, in the training cycle, the model cycle in this study is the longest, and the objective function value needs to reach about 1,500 times before it tends to be stable. Literature [17] takes the second place, and it takes about 1,000 training times for the value of the objective function to stabilize. Literature [16] is at least 1,000 times. In terms of objective function value, when the training of each model is completed, the objective function value of the model in this study is the smallest, with an average value of 0.055. In literature [17], the mean value of objective function is 0.081 and in literature [16] it is 0.067. The model in this study has the best adaptability to the third training data set and the highest early warning accuracy.

4.4. Comparative Analysis of Financial Risk Models. After the model training is completed, this study selects the comparison model based on machine learning and deep learning. Among them, the machine learning model selects the literature [18] model with simple model structure and fast training speed and adds the literature [16] model with stationarity test to improve the robustness of the model. The literature [17] model of dimension reduction operation is added under the low-dimensional feature set. Literature [19] model with excellent performance is added under high-dimensional feature collection. For the in-depth learning

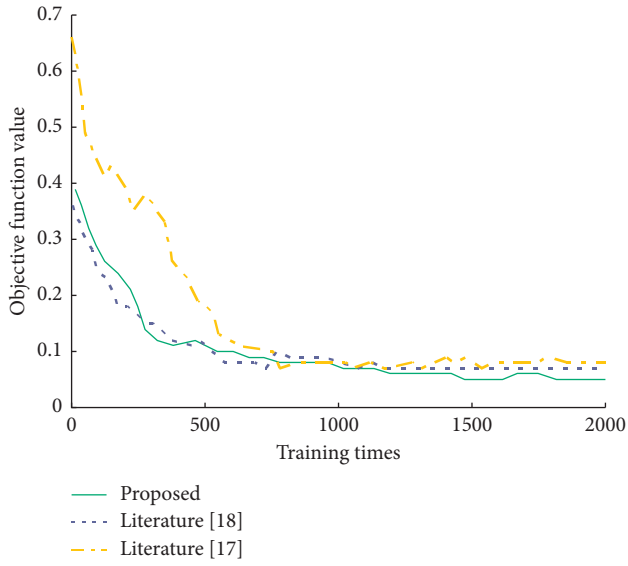


Figure 6: Training comparison of proposed model.

model, the typical literature [20] model is selected. Through comparison, the actual early warning performance of this model is further evaluated.

First, the test data set including 83 dimensions is divided into three groups, and the accuracy of each group is tested by each model (as shown in Table 1).

Combined with the performance of each model in Table 2, we can see the difference between machine learning and deep learning. Compared with machine learning, deep learning has obvious advantages in image and natural language [39, 40]. However, in the direction of corporate agricultural industry financial early warning, the early warning performance of the early warning model based on machine learning is not necessarily worse than that of the deep learning model. For example, in literature [17], its training accuracy and test accuracy are obviously superior to literature [20]. The early warning model constructed by a single improved K-means clustering algorithm generally does not have the function of feature screening, such as literature [18]. However, the shortcomings of not having feature screening can be overcome by combining models, such as literature [16], literature [17], etc. Moreover, the early warning performance of the combined model can generally be further improved.

Combined with (1) and (2), in terms of corporate agricultural industry financial early warning, compared with the deep learning model, the clustering algorithm proposed in this article has a better early warning performance. This further verifies the feasibility of combining the grey Wolf optimization algorithm with K-means algorithm for cluster analysis.

From the perspective of the specific performance of each model, the six groups of models can realize the role of agricultural industry financial early warning. However, compared with the other five groups of models, the accuracy of this model is higher. On the premise that each group of models is trained 2000 times, the training accuracy of this model reaches the highest 96.59%, which is superior to the second best performance literature [17]. In addition, this model also has better feature screening ability. Compared with other models that also have feature screening, such as literature [20], literature [17], literature [16], etc., the model test accuracy of this study is ahead of other groups of models, reaching 86.77%. Therefore, generally speaking, proposed model has strong feature screening ability and effectively improve the accuracy of the company's agricultural industry financial early warning.

The impact of changes in feature dimensions on the early warning performance of the model in the enterprise dataset will be further explored. Based on the principle of removing features in proportion, 83 groups of features in the above test data set are removed. If 25%, 50%, and 75% features in the test data set are removed in turn, 25%, 50%, and 75% test data sets are obtained respectively. The corresponding original test data set is abbreviated as 0% test data set, indicating that feature removal is not performed. Thereafter, four groups of test data sets of 0%, 25%, 50%, and 75% were used successively. The early warning performance of the above six groups of models is evaluated and shown in Table 2.

With the continuous reduction of feature dimensions in the test data set, the accuracy of different models also varies greatly. Among them, the change of feature dimension has the least impact on the test accuracy of literature [17] and literature [16], and the change range is no more than 2.5%. The change of feature dimension has the greatest impact on the accuracy of proposed model and literature [20]. With the decreasing of feature dimension, the accuracy of convolution neural network and long-term and short-term memory network decreases.

In order to further explore the impact of the change of feature dimension on the early warning performance of the model, this study adopts the method of reducing each group of test data sets by 5%. Then, a total of 18 test data sets can be obtained, namely 0%, 5%, 10%, . . ., 80%, 85%. Among them, 0% of the test data sets still represent the features not removed and 85% of the test data sets represent the data sets after 85% of the features have been removed.

The accuracy of each model in the above 18 groups of test data sets is summarized, and a dotted line diagram of the accuracy and feature removal ratio is constructed (see Figures 7 and 8).

Further, the fourth-order polynomial is used to fit each point line in Figure 7 to obtain the fitting curve of accuracy and feature removal ratio (see Figure 8).

As can be seen from the overall performance of each fitting curve in Figure 8, the accuracy of proposed model and machine learning models such as literature [18] and literature [17] will fluctuate in a small range and tend to decline gently as the enterprise feature dimension decreases. The accuracy of literature [20] represented by deep learning will drop sharply without fluctuation. Therefore, the model and machine model in this study have stronger model stability and robustness than literature [20].

Importantly, each set of models corresponds to the feature optimal dimension. That is, compared with the performance of the model in the nonoptimal dimension, the

Table 1: The accuracy of each model.

Model	Training accuracy (%)	Test accuracy (%)			Average accuracy (%)
		Group 1	Group 2	Group 3	
Literature [18]	80.02	71.28	70.28	69.35	70.30
Literature [16]	87.02	77.44	78.94	80.14	78.84
Literature [19]	91.92	81.27	80.67	83.57	81.84
Literature [20]	89.21	79.95	81.02	81.45	80.81
Literature [17]	94.71	84.2	85.2	85.52	84.97
Proposed	96.59	86.38	86.64	87.29	86.77

Table 2: Test accuracy of each model under ratio removal characteristics.

Model	0% test accuracy	25% test accuracy	50% test accuracy	75% test accuracy	Range of accuracy change
Literature [18]	70.12	72.15	73.4	73.2	3.96
Literature [16]	78.66	79.08	78.37	76.91	2.85
Literature [19]	81.66	83.64	83.12	79.85	4.47
Literature [20]	80.63	78.04	72.74	71.72	9.59
Literature [17]	84.79	86.87	85.95	82.94	2.76
Proposed	86.59	87.96	83.99	80.95	7.69

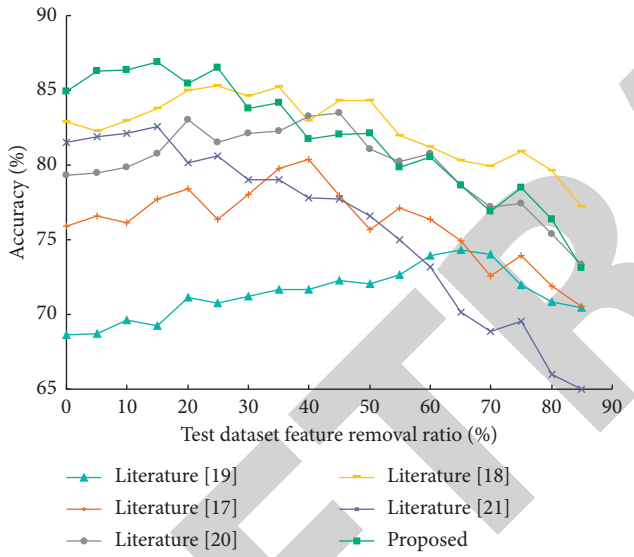


Figure 7: Point line relationship between test accuracy of each model and feature removal ratio.

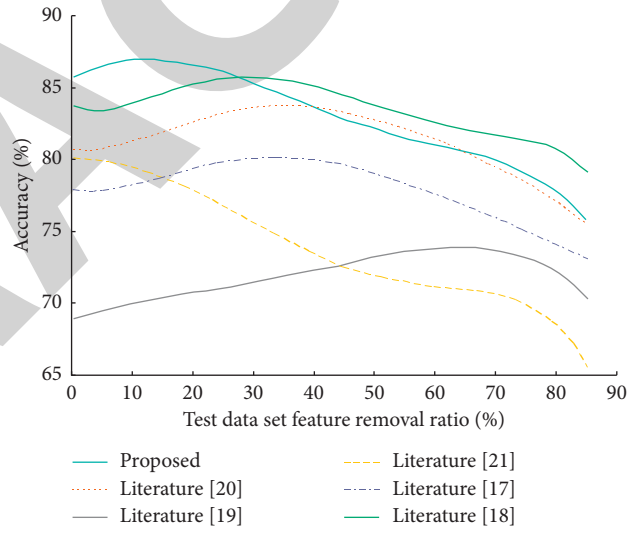


Figure 8: Fitting curve of test accuracy and feature removal ratio of each model.

early warning performance under the optimal dimension is often the best. Among them, the feature optimal dimension of the model in this study is about [63, 82] (corresponding to the x-axis [0, 23] in Figure 8). At this point, the test accuracy is as high as 87.26%, which is obviously better than other models. When the feature number removal ratio is greater than 23%, the early warning performance of this model gradually declines. In the interval [47, 63] (corresponding to the x-axis [23, 42] in Figure 8), the early warning performance of the model in this study is reversed by literature [17], that is [47, 63] becomes the feature optimal dimension of literature [17]. In other words, compared with other models, the model in this study has a larger feature optimal dimension (e.g., the test data set given in this study, the optimal dimension of agricultural industry financial features is [63, 82]). Then, it is concluded that the model in this study has the same performance for agricultural industry financial early warning with low-dimensional features. But it has obvious advantages in high-dimensional features, and the accuracy of early warning is much higher than that of other models.

5. Conclusion

Agricultural industry finance is a weak link in China's financial system. In order to improve the risk warning ability of agricultural industry, this article proposes an agricultural industry financial risk warning system based on improved K-means clustering algorithm. In order to solve the problem that K-means algorithm cannot jump out of the local optimal solution in the clustering process, this study combines the grey Wolf optimization algorithm with K-means algorithm for clustering analysis. In the iterative process of grey Wolf optimization algorithm, the elite individuals in grey