Hindawi
Security and Communication Networks
Volume 2023, Article ID 9894738, 1 page
https://doi.org/10.1155/2023/9894738

Retraction

Retracted: Application of Face Recognition in E-commerce Security Authentication in the Era of Big Data

Security and Communication Networks

Received 5 December 2023; Accepted 5 December 2023; Published 6 December 2023

This article has been retracted by Hindawi, as publisher, following an investigation undertaken by the publisher [1].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] S. Chang and Y. Duan, "Application of Face Recognition in E-commerce Security Authentication in the Era of Big Data," *Security and Communication Networks*, vol. 2022, Article ID 4246750, 11 pages, 2022.

Hindawi
Security and Communication Networks
Volume 2022, Article ID 4246750, 11 pages
https://doi.org/10.1155/2022/4246750

Research Article

Application of Face Recognition in E-commerce Security Authentication in the Era of Big Data

Shu Chang[1] and Youtao Duan[2]

[1]*School of Management, Northwest University of Political Science and Law, Xi'an 710122, China*
[2]*School of Humanity, Shanghai University of Finance and Economics, Shanghai 200433, China*

Correspondence should be addressed to Youtao Duan; ne001@163.sufe.edu.cn

Received 28 June 2022; Revised 26 September 2022; Accepted 6 October 2022; Published 12 October 2022

Academic Editor: C. Venkatesan

Although Internet technology brings invaluable benefits to all walks of life, the security of network and information is becoming more and more prominent. The leakage of personnel information caused by Internet security incidents causes irreparable harm and loss to individuals or enterprises. E-commerce is a virtual transaction mode based on Internet technology. Its security requirements for transactions are more stringent than those for traditional transaction modes. Traditional identity authentication technology can no longer meet its security needs. People urgently need a reliable identity authentication system, meaning to ensure the security of e-commerce. According to the actual application scenarios of the algorithm in e-commerce, this paper, based on the research on face recognition technology, focuses on the in-depth research on face detection technology under the background of big data in order to introduce face recognition technology in this paper. This paper proposes a feature-based face matching algorithm. The face image is preprocessed to improve the accuracy of real-time face detection and reduce the false detection rate. Based on the research of traditional facial feature extraction technology, a virtual sample set that can effectively support a traditional facial feature extraction algorithm is constructed to solve the problem of insufficient training samples in practical applications. The experimental results showed that the accuracy of the method in this paper can reach up to 79.5% and that the minimum time consumption is only 0.142 s. Compared with the traditional method, the accuracy rate is higher and the time consumption is shorter.

1. Introduction

In order to successfully conduct electronic transactions on an open platform such as e-commerce, the security of the transaction network platform and the confirmation of the identities of both parties must be solved. Traditional authentication technologies include password-based authentication, smart card-based authentication, and password-based authentication. These identity authentication technologies have many disadvantages, such as being easy to lose, easy to forget, and inconvenient to carry. In addition, these authentication methods are particularly weak against emerging cyber fraud and attack techniques. The traditional authentication method can only guarantee the identity reliability between the microcomputers but cannot solve the natural isolation of the identity authentication between the user and the microcomputer. In order to solve this problem, people have turned their attention to technologies that utilize human biometrics for identification. Facial recognition is considered to be one of the best biometrics available for identity authentication due to its unique advantages.

Regarding e-commerce security certification, relevant scientists have conducted the following research studies. Kabanda and Brown attempted to identify structural practices related to SME e-commerce. Using structuring theory and following an interpretive stance, the findings suggest that SMEs develop three main e-commerce structuring practices: (1) through the use of the website for marketing and image building, (2) through the extensive use of mobile technology for transactions, and (3) through the establishment of partnerships to solve technical problems. The results showed that SMEs' use of the website is limited because their understanding of the website is incompatible with the cultural bargaining system, which is characterized by cash transactions and face-to-face bargaining [1]. Boyd et al. provided the first systematic analysis of key exchange security involving authentication systems. A family of security models is defined that, in addition to allowing different standard key exchange adversary query sets, it allows adversaries to register arbitrary bit strings as keys. For this family of models, general results are demonstrated, enabling designed and verified protocols to achieve security even if some keys are maliciously generated, and the method is applicable to a wide range of models and protocols [2]. Anisetti et al. showed how to handle security attribute validation of composite services through test-based security authentication and establish effective and efficient validation in dynamic composition scenarios. This approach builds on the existing security authentication scheme of a single service and extends it to service composition. It starts with the certificate granted to the component service, which virtually authenticates the composite service. The proposed industrial evaluation demonstrated the utility and generality of the proposed method by showing how the certification results can be used as a basis for establishing compliance with payment card industry data security standards [3]. Tsvilii studied conformity assessment systems and programs for operational technology cyber security, as a set of rules and procedures that describe what is certified, identify specific requirements, and provide methods of certification. The main hypothesis of the study is that the quality of cyber security can be improved by moving towards a common approach based on agreed international standards and international best certification practices. A layered model of cyber security certification system evaluation criteria and a layered model of the cyber security certificate mutual recognition protocol have been developed, which will allow the creation of operational technology cyber security certification systems and programs in a systematic manner [4]. The main problem of these studies is that the accuracy of security authentication is not high, so this paper introduces face recognition technology.

At present, there are the following research results for face recognition. Min et al. proposed the first publicly available sensor-based face database. The database includes different data patterns and multiple facial variations. Standard face recognition methods benchmark the proposed database and demonstrate performance gains when integrating depth data with data via fractional-level fusion. 3D images are also compared with traditional high-quality 3D scans for face biometrics, which reveal the urgent need for the proposed database in face recognition research [5]. Lu et al. proposed a new joint feature learning method to automatically learn feature representations from raw pixels for face recognition. An unsupervised feature learning method is proposed to learn hierarchical feature representations. Since different face regions have different physical features, it is suggested to use different feature dictionaries to represent them and simultaneously learn multiple related feature projection matrices for these regions. After learning these feature projections for different face regions, face patches within each region are spatially pooled to improve the representation of the learned features [6]. Meng et al. proposed a new joint regularization nearest point algorithm. On the joint-regularized near point, the nearest point of the query set is generated by synthesizing the entire gallery set of all classes. Joint regularization of the closest points minimizes the distance between the query set and the single-category set. On this basis, a greedy and adaptive-based method is presented and classified. Experiments showed that this method has good application prospects in face recognition [7]. This paper introduces face recognition technology to improve the accuracy of security authentication.

The four methods are simulated and analyzed, respectively, to verify the effectiveness of the fitted face detection algorithm. The correct rate, misclassification rate, and detection time of the method in this paper are 96.7%, 8.4%, and 0.171 s, respectively, which can achieve the goal of reducing missed detection and false detection. The accuracy rates of face recognition in the single-sample case of this method are 14.8%, 15%, 15.2%, and 17.3%, respectively, and the face recognition accuracy rates in the virtual sample case are 72.5%, 71.3%, 73.5%, and 78.6%, respectively.

2. E-Commerce Security Authentication Methods

The security authentication technology in e-commerce can ensure the identity and normal operation of both parties involved in transactions. When two people do not know each other, authentication technology is the best way to confirm each other's identity [8]. In e-commerce, how to realize safe access control, how to ensure safe and reliable transmission, and how to carry out effective identity authentication for transaction parties are all issues that need to be considered and solved. To successfully carry out e-commerce transactions, it is necessary to have authentication technology. The essence of identity verification is a kind of information, whether it is confidential, private, or specific biometric information. Only the authenticated party can prove their identity. According to the degree of confidentiality that the authenticated party relies on, it can be divided into two types: one is identity authentication based on confidential information and the other is identity authentication based on physical security [9]. An e-commerce security system is shown in Figure 1.

A firewall is composed of a series of components, and these components are located in different networks, such as a trusted corporate intranet and an untrusted public network or a network security field. The system is the only information input channel between each network or network security field, which can control (allow, deny, and monitor) the information entering and exiting the network according to the company's security policy. In addition, it has a good ability to resist attacks.

Authentication technology is an effective means to prevent information from being tampered, deleted, replayed, and forged. It allows the recipient to authenticate and attest

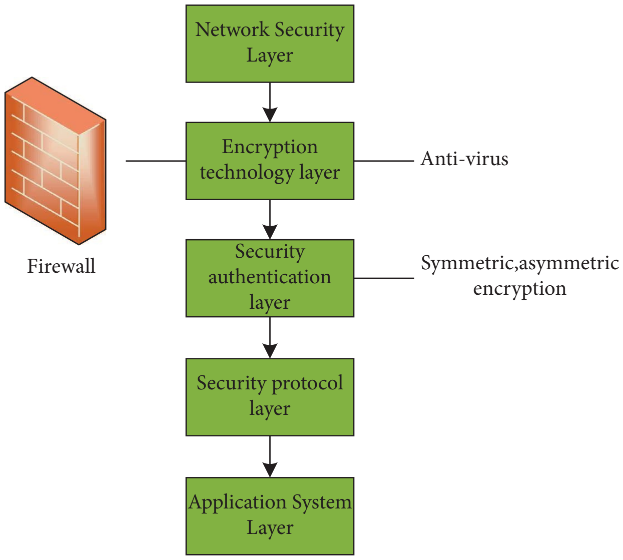
Network Security Layer
Encryption technology layer
Anti-virus
Firewall
Security authentication layer
Symmetric,asymmetric encryption
Security protocol layer
Application System Layer

Figure 1: E-commerce security system.

to the origin and authenticity of information. This method of the static password is the most frequently used authentication method in real life; that is, the method indicates someone's identity by means of the identity and password. As long as the user whose ID and password are both correct is judged by the computer to be a legitimate user, he can log in and perform operations. This is an authentication method based on information held by the user. Once the password of this authentication method is stolen, the user's identity is stolen [10].

An SMS password means that the service provider sends a number of passwords to the user in the form of SMS, which generally includes a valid time limit. The user logs in to the service provider with the dynamic password, thereby ensuring the security of system identity authentication [11]. This method has many advantages. The first is excellent security. Because the user and the mobile phone usually appear on the same occasion and the generation of the SMS password has nothing to do with the specific application scenario, the password is not easy to be intercepted. The second is high popularity and low learning cost. In view of the basic popularity of mobile phones, it is enough to send and receive text messages. In addition, SMS password authentication also has the advantages of easy charging and easy maintenance [12].

The dynamic password authentication method requires the user to hold a special terminal, and the terminal can dynamically generate a password at certain time intervals. Terminals can be divided into hard terminals and soft terminals. A hard terminal is a kind of hardware device, which is obtained by users through certain channels, such as onboarding. The soft terminal is often just a piece of software running on the mobile phone operating system. This authentication method has the highest security factor and is widely used in e-commerce [13].

At present, iris, fingerprint, face, etc. are the biometrics that are used for more research studies in authentication technology. Iris recognition is similar to face recognition and generally requires three steps: image capture, feature extraction, and pattern matching. Difficulty lies in the image capture process. The acquisition of iris images requires expensive professional camera equipment because ordinary shooting equipment cannot obtain a complete iris image of a person [14]. The iris image acquisition must have strong light, especially for the black eyes of Chinese people. However, strong light causes great damage to the human eye. Therefore, although iris recognition has been deeply researched in theory, the feasibility in reality is not high.

People have all seen in movies that police officers collect fingerprints at crime scenes and then compare them with the fingerprints of suspects. Fingerprint recognition is actually an identity authentication method that uses the uniqueness of human fingerprints to collect and compare fingerprints. As the most traditional and most studied recognition technology, fingerprint recognition has a series of significant advantages, such as high accuracy and good reliability. The schematic diagram of fingerprint recognition is shown in Figure 2.

However, this method is applied in the identity authentication of e-commerce, and fingerprint recognition has obvious defects. Hence, professional fingerprint collection equipment is required. It seems impossible to require every user who uses e-commerce to buy a fingerprint capture device, and very few computers are equipped with fingerprint readers [15].

In the authentication mechanism based on a smart card, the authenticator requires the smart card to have hardware encryption function and high security. The authentication method based on smart cards is a two-factor authentication method (PIN + smart card). Even if the PIN or smart card is stolen, the user will still not be impersonated. Smart cards provide hardware protection measures and encryption algorithms that can be used to enhance security.

The most common and easiest way to identify a user is password verification. The system will set a user/password pair for each legal user. When logging in or using a specific function, the user will be prompted to enter the username and password. The system will check that the user's username/password matches the username/password pairs of legitimate users already in the system (these are stored encrypted in the system). If it matches a specific username/password pair, then the user's identification is verified [16]. The disadvantage of this method is that it is only based on the secrecy of the user's password, and the user's password is usually short and easy to be guessed, so the scheme cannot resist the attack of password guessing. In addition, the attacker can also listen to the communication channel or perform network peeping, and the clear text transmission of the password can allow the attacker to obtain the user password when transmitting the password, thereby destroying the password [17]. The security of this protocol is very low due to the lack of civilization, especially in the network environment. The workaround is to encrypt and send the password. At this time, shortcomings can partially be solved, but the attacker can still take offline methods to perform dictionary attacks on passwords. Another difficulty

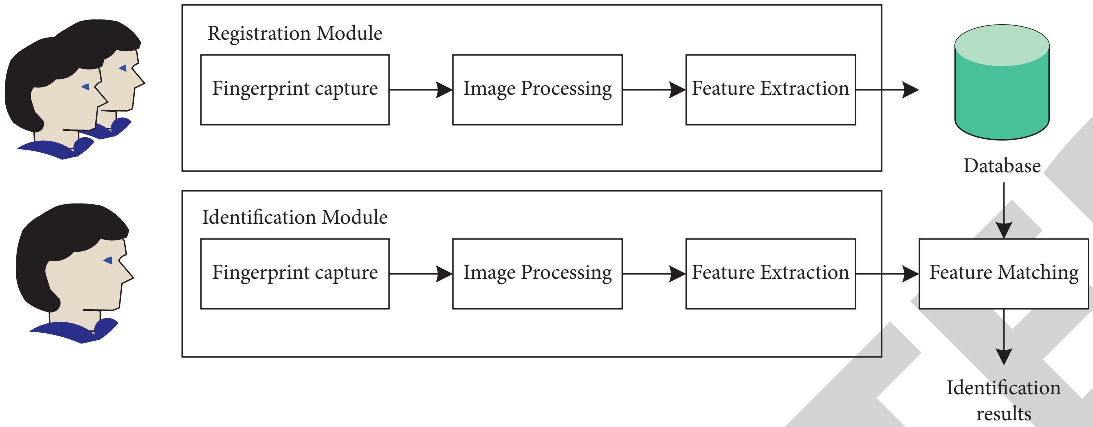

Figure 2: A schematic diagram of fingerprint recognition.

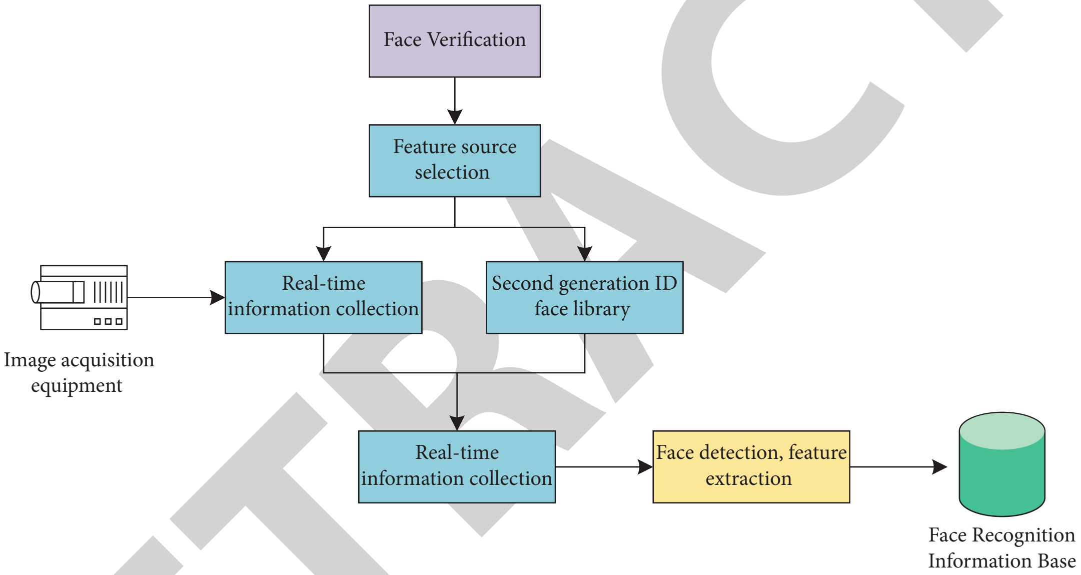
Face Verification
Feature source selection
Image acquisition equipment
Real-time information collection
Second generation ID face library
Real-time information collection
Face detection, feature extraction
Face Recognition Information Base

Figure 3: Face recognition identity registration model.

in password transmission lies in the exchange of passwords. To solve these problems, this paper introduces face recognition technology [18]. Face recognition refers to the technology of identity search or identity authentication through facial features. Its three main components are face detection, feature value extraction, and face recognition.

Face identity authentication is a verification method that uses the currently captured face image or video to extract face features and compares it with the existing face features in the database to find and judge the specific identity of the face [19]. Face recognition is a popular and extensive research topic at present, and the application of face recognition in e-commerce identity authentication is the focus of many researchers. This is because identity authentication technology based on face recognition has incomparable advantages of characteristic authentication technology. The most important of which is that it can easily collect faces. At present, almost all microcomputers have their own shooting equipment. Although quality is uneven, the image as face recognition has fully met the requirements. In addition, face recognition is noninvasive to users, and users are easy to accept. However, the identity authentication method based on face recognition also faces many problems, such as the adverse effects of posture, illumination, expression, and complex background on face recognition. The face recognition identity registration model is shown in Figure 3.

In this model, users are not allowed to collect identity information by uploading static pictures. There are currently two solutions: one is to call the second-generation ID card face database as a face feature extraction source. The operation is relatively simple as long as the user's ID card is collected and associated with the relevant data in the second-generation ID card face database. A face image is sufficient. The second is to input a picture containing the user's avatar collected by the user's current hardware device as a face feature source. Comparing these two methods, the first method is simple to operate due to the standardization of the second-generation ID card avatar when shooting. It recognizes the face more clearly, requires a single background, generally has no facial decoration (such as glasses, etc.), and

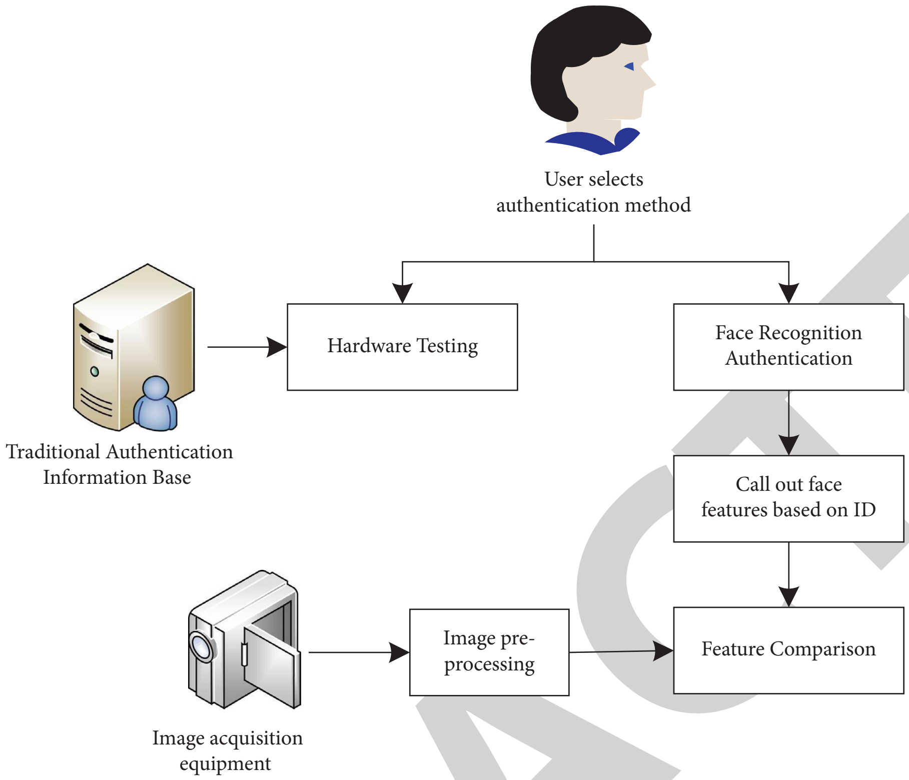
User selects
authentication method
Hardware Testing
Face Recognition Authentication
Traditional Authentication Information Base
Call out face features based on ID
Image pre-processing
Feature Comparison
Image acquisition equipment

Figure 4: Authentication model.

is basically not affected by light. However, this method first needs to obtain the face database of the second-generation ID card and then cannot serve users who have not applied for the second-generation ID card. The advantage of the second method is that it can provide any user with an identity authentication service based on face recognition, which is very flexible. However, disadvantages are also obvious. The images containing the user's face collected in real time are irregular. For example, the clarity will vary with the quality of the user's hardware and may contain complex backgrounds, strong lighting, and facial posture. As well as the influence of expression factors, additional processing of the image is required to extract and store the user's facial features. During the identity registration stage, the user will be asked whether there are twin brothers or sisters, considering that the facial features of people are sometimes extremely similar, such as twin brothers and sisters. If so, it is recommended that the user use traditional identity authentication or add several-digit feature codes to identity authentication based on face recognition. Face detection is the first stage of the face recognition system. Almost all face recognition systems need to obtain the position, size, shape, posture, and other information of the face from the input image or video information.

The identity authentication module is relatively simple. Considering different usage habits and hardware conditions of users, the system will provide two authentication methods, the traditional authentication method and the authentication method based on face recognition. The premise of using the traditional authentication method is that the user is in the registration stage. The account password and other related information have been registered. After reading the image input by the user, the system will automatically analyze, compare, and verify the user's identity to complete the identity authentication process. The authentication model is shown in Figure 4.

The identity authentication system should create at least three databases to store second-generation ID card data, face feature data, and traditional authentication information data, respectively. If the image in the second-generation ID card is used as the face feature extraction source, the second-generation ID card database should be obtained first. In reality, as an individual, it is temporarily impossible to obtain image information in the second-generation ID card database. Only information such as name, date of birth, and registered address can be obtained. Therefore, ID card information of some experimental individuals is temporarily collected as a simulation of the second-generation ID card database. At the same time, database information is simplified and only contains the ID number and avatar information.

No matter how the extracted face is an extremely complex mathematical representation, how to store these mathematical representations is also a problem that the system needs to solve. There are two processing methods here. The first method is to store the source image used for feature extraction during identity registration, collect the authentication image during face authentication, then perform the same feature extraction on the two images, and finally compare the two. The similarity of the facial features of the image determines whether authentication is passed. The second method is to not only store the source image for feature extraction during identity registration but also perform feature extraction on it and store the extracted features in the database in binary form. Then, during identity authentication, eigenvalues extracted in real time are compared with the eigenvalues stored in the database, and the final certification conclusion is drawn. The advantage of the first method is that it does not need to consider the storage implementation of complex mathematical features, but the disadvantage is that the time spent in the authentication process is doubled compared to the second method. Although the second method increases the complexity of the program, it relatively saves the user's waiting time.

In this system, the traditional authentication information library has the following two functions: recording the traditional authentication information of users, including ID, password, and password questions and the carrier of user statistical information; that is, the library should contain all users. If the user authentication method is not the traditional authentication method, the password can be left blank, that is, the password question and other related fields. The system simulates a minimal model of a traditional authentication information base containing three fields: user ID, user ID number, and password.

In environmental detection, the user's external device will be tested to see if it has the basic conditions for face recognition authentication, and it will also investigate whether the user has twin brothers or sisters and the user's acceptance of face recognition. The authentication method selection is based on the results of environmental testing to determine which authentication method the user uses. The priority order is that the user's willingness is superior to the hardware detection conclusion, and the hardware detection conclusion is superior to the existence of twin brothers or sisters. A random verification code will be sent to the user during the verification of the mobile phone or e-mail address. The user must fill in the verification code correctly to proceed to the final registration step. After completing the registration stage, the user will get a prompt message of successful or failed registration, and the program will perform related work such as feature extraction and data storage. According to the authentication method, an identity authentication module can be divided into a traditional identity authentication method and an identity authentication method based on face recognition. The identity authentication technology based on face recognition needs to collect face images in real time as access evidence, preprocess the collected images and face detection, and then performs feature extraction, and match and authenticate the extracted feature values with the face recognition information. The characteristics stored in the library when the user identity is registered are compared for similarity. If similarity satisfies a certain threshold, the user is considered to be a legitimate user.

In the practical application of the e-commerce identity authentication system based on face recognition, only a front-facing image is required as registration information, or the face image in the face database of the second-generation ID card is directly used. At this time, the user can be asked for a single image in the background, which is provided as authentication information for registration. When conducting transactions, users are often required to take real-time images for identity authentication. Due to some inherent defects of the image acquisition system, external factors are inevitably introduced when collecting images, such as lighting, posture, and complex backgrounds. In addition, the images collected by the collection system are also restricted by human expression factors. It is impossible to ask the collected user to maintain expression posture. Generally speaking, these interference factors are less controllable, but the problem faced in the application is that the identification task can be completed in any situation. Therefore, it is necessary to preprocess the image.

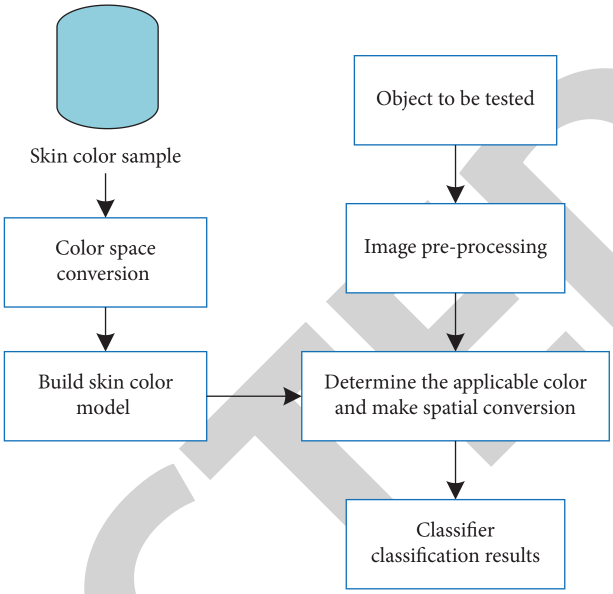

Figure 5: Face detection methods.

Video-based fast face detection and localization and local feature-based face detection and recognition are detection and recognition methods with face edge information as the main observation feature. In the case of strong light influence, the shadow on the face will blur its edge information, which leads to the inaccuracy of the detection and recognition method based on facial contour features. The skin color of the face has a large color difference with the surrounding environment and has good aggregation in some color spaces. The face detection algorithm based on this is a convenient, fast, and accurate face detection method. However, it is impossible to combine the brightness and color of the human face through certain color spaces. Therefore, it is impossible to quickly detect and locate faces according to skin color. The face detection method is shown in Figure 5.

In image processing, histogram equalization is a method of adjusting the contrast of the histogram applied to an image. This method is generally used to enhance the local contrast of the image, especially when the effective data contrast is very close. After this process, the brightness information of the image can be better distributed in the histogram and the local contrast can be improved without affecting the overall contrast. The following is the relevant formula of image preprocessing, and the algorithm is used to preprocess the face image:

$$\begin{aligned} U(m,n) &= R(m,n)\times P(m,n),\\ h(m) &= i\times \log m,\\ h(m) &= i^{m}, \end{aligned} \tag{1}$$

where U is the reflected light, R is the reflection property of objects on light, and P is the incident light.

$$f(u,v) = \max(R(u,v), H(u,v), J(u,v)), \tag{2}$$

where $f(u,v)$ is the grayscale value.

Binarized images play an important role in the extraction of facial features, which can effectively avoid the "dimension disaster" in feature extraction:

$$N_{u,v} = \mathrm{Me}\left[M_{u+a};\,(a,b)\right], \tag{3}$$

where $N_{u,v}$ the two-dimensional median filter.

$$G(m,n) = \frac{1}{A}\sum_{u=-b}^{b} f(m+u, n+v), \tag{4}$$

where $G(m,n)$ is the mean of pixel values.

$$u(m,n) = \sum U(m', n'), \tag{5}$$

where $U(m\prime, n\prime)$ is the pixel value of the image.

In order to reduce repeated calculation and save calculation time, the integral map of the image can be derived by the following formula:

$$\begin{aligned} d(m,n) &= d(m,n-1) + u(m,n),\\ u(m,n) &= u(m-1,n) + d(m,n). \end{aligned} \tag{6}$$

We normalize the sample weights as follows:

$$l_{t,u} = \frac{q_{t,u}}{\sum_{v=b}^{B} q_{t,u}}, \tag{7}$$

where $q_{1,u}$ initializes the weights of the samples.

$$\begin{aligned} g_v(m) &= \begin{cases} 1, & l_v\times\theta_{lo},\\ 0, & \text{otherwise,}\end{cases}\\ \mu_t &= \sum_{u=1}^{B} q_{t,u}\times\left|g_t(m_u - n_u)\right|, \end{aligned} \tag{8}$$

where $g_v(m)$ is the feature construction weak classifier and μ_t is the optimal weak classifier.

$$\begin{aligned} R &= \max(f_v, f_k),\\ q_{t+1,u} &= q_{t,u}\times \varepsilon_t^{\left|g_t(m_u)-n_u\right|}, \end{aligned} \tag{9}$$

where R is the feature correlation and $q_{t+1,u}$ is the weight adjustment.

Table 1: Experimental results of face detection methods.

Methods	Number of samples	Correct rate (%)	Wrong score rate	Time consumption (s)
DC	400	94	28.5	0.405
Ad	500	81.5	17.3%	0.342
DA	300	91.2	12%	0.212
This article	400	96.7	8.4%	0.171

Table 2: Basic user information.

Field meaning	Field name	Type	Size
User identification	UD	va	20
Name	UN	va	20
Gender	SE	bt	5
Date of birth	BI	smt	10

Table 3: User bank account information.

Field meaning	Field name	Type	Size
User identification	UD	va	20
Account number	UN	va	15
Face templates	SE	bt	3
Account balance	BI	smt	8

$$\phi = \frac{1}{B}\sum_{u=1}^{B} q_{t,u}\times\left|g_t(m_u) - n_u\right|, \tag{10}$$

where ϕ is the average degree of the error of the sample.

$$L\left(C_j, C_r\right) = \exp\left[(m-a)^{T} C^{-1}(m-a)\right], \tag{11}$$

where L is the skin color similarity.

$$g(m,n) = \mathrm{fum}\{|U(m,n)|\}, \tag{12}$$

where $g(m,n)$ is truncate integer operation U.

$$D_N = \sum_{k=0}^{1} q_k\left[x_k - x\right], \tag{13}$$

where D_N is the interclass dispersion matrix.

3. E-Commerce Security Authentication Experiment

In order to verify the effectiveness of image preprocessing to fit the face detection algorithm, the four methods are simulated and analyzed, respectively, and their efficiency and accuracy are compared. Table 1 shows the experimental results of the face detection method.

It can be seen that the correct rate of the method in this paper has reached 96.7%, the misclassification rate is only 8.4%, and the required time is 0.171 s. On the basis of ensuring classification accuracy and classification efficiency, the goal of reducing missed detection and false detection has been achieved.

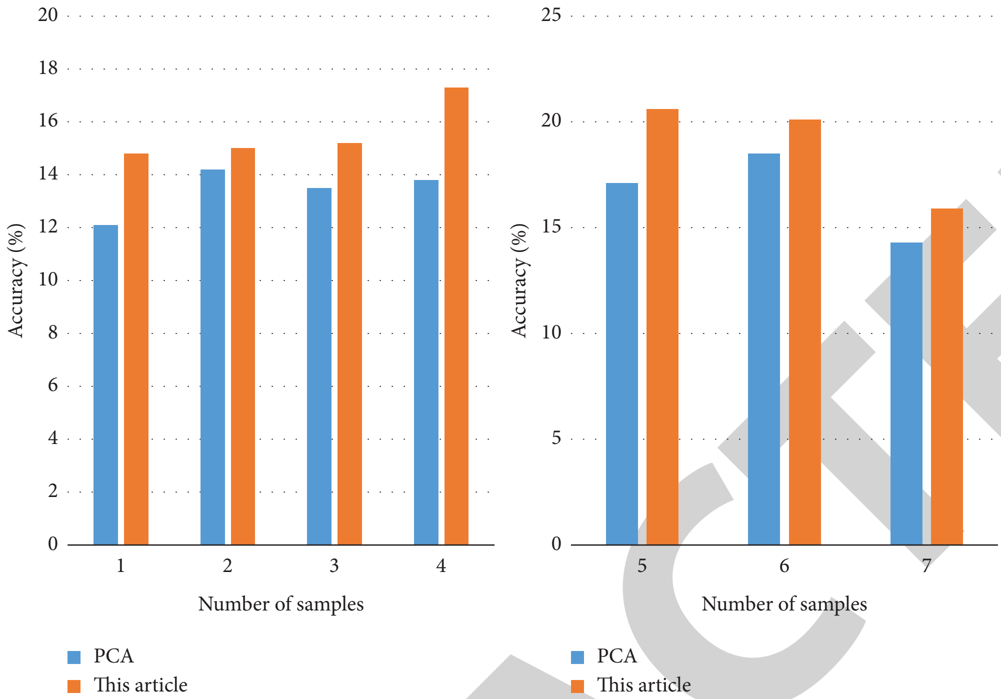

FIGURE 6: Face recognition accuracy in the single sample case.

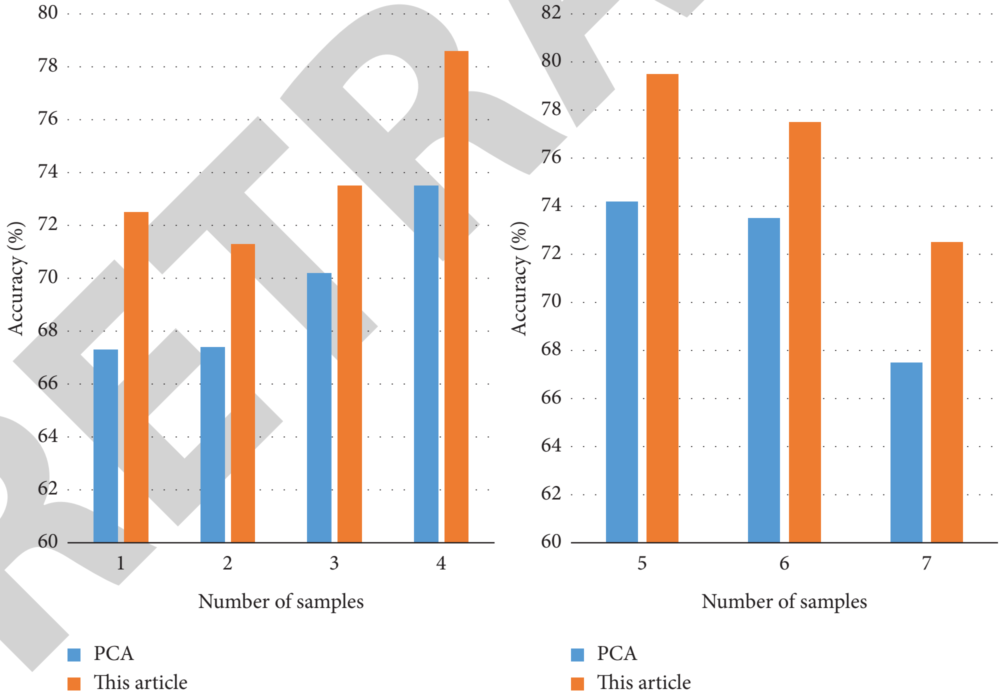

FIGURE 7: Face recognition accuracy in the case of virtual samples.

Reasonable database design can not only reduce data redundancy but also improve the efficiency of database operations. The standardization of data table design can improve database performance. As shown in Tables 2 and 3, the basic information of the user and the information of the user's bank account are shown. It can be seen that the corresponding modules of the user ID and the account number are the largest, reaching 20.

The principal component analysis (PCA) method, also known as the eigenface method, is based on the K-L transform. This method is a dimensionality reduction statistical method, by means of an orthogonal transformation.

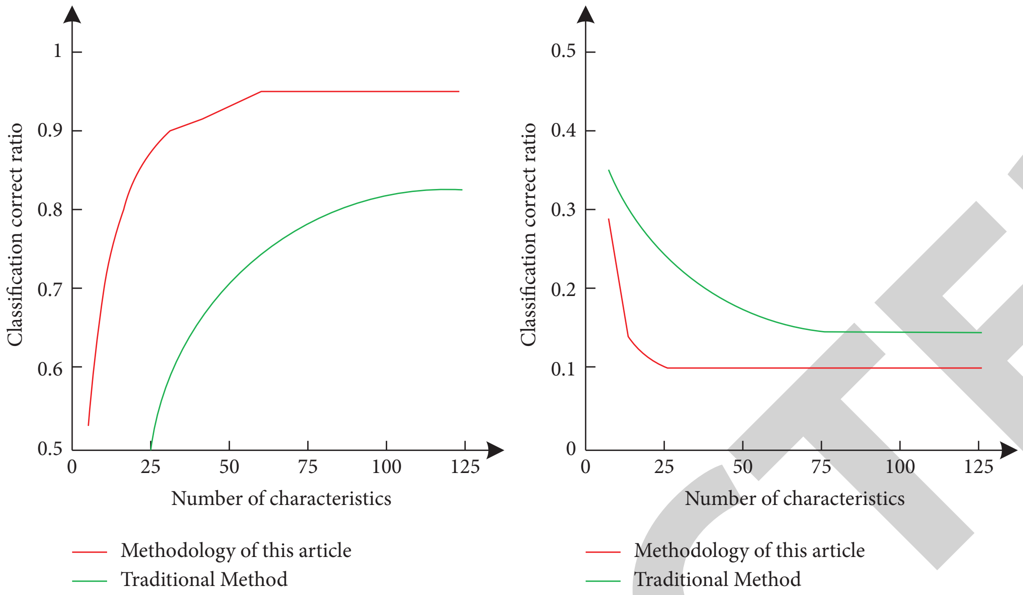

FIGURE 8: Correct and incorrect classified data.

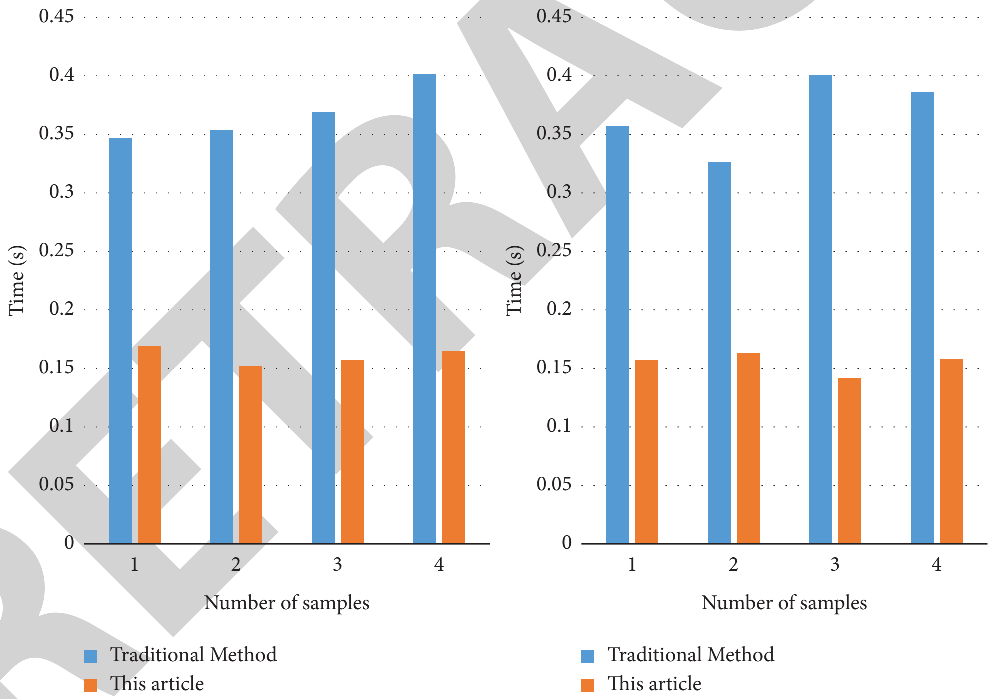

FIGURE 9: Time consumption comparison results.

The original random vector with related components is converted into a random vector with uncorrelated components. The recognition accuracy of the algorithm in this paper and the PCA feature extraction algorithm was tested in the case of a single sample; then, a virtual sample for each sample was created; the corresponding virtual sample was used to train the feature extraction algorithm, and its recognition accuracy was tested. Finally, the two methods were compared. Figures 6 and 7 show the accuracy of face recognition in the case of the single sample and the virtual sample.

According to the experimental results, it can be found that compared with a single sample, the method of constructing a virtual sample set for the sample can effectively improve the accuracy of the recognition algorithm, and the accuracy rate has reached 79.5% and 78.6%.

According to the improvement of the traditional algorithm, it is expected that the improved algorithm will take less time than the traditional algorithm and should use fewer features based on expected classification accuracy. The specific performance is that the detection accuracy will converge faster with the number of features. The two algorithms were simulated, and the experimental data were recorded, as shown in Figure 8 for correct and incorrect classification data. From the experimental results, it can be clearly observed that the accuracy of the method in this paper converges faster with the number of features than that of the traditional algorithm, and the number of features required to reach the limit accuracy is far less than those required by the traditional algorithm.

The time-consuming detection of the method in this paper and the traditional method is shown in Figure 9 for the time-consuming comparison results. It can be seen that the method in this paper takes less time than the traditional method and that the shortest time is 0.142 s, which has higher efficiency.

4. Conclusion

With the increasing development of e-commerce today, its requirements for security authentication technology are also getting higher and higher. Not only between microcomputers, but also the identity authentication between individual users and microcomputers is becoming more and more important. Traditional identity authentication technology cannot solve the problem of natural isolation between the user and the computer, so this paper introduced face recognition technology. Two kinds of problems that may arise in the application of face recognition to the e-commerce identity authentication system were analyzed: face detection problems in complex backgrounds and single-sample feature extraction problems. A fitting face detection method was proposed to improve the accuracy of face detection in complex backgrounds and reduce missed detections and false detections. A method of adding virtual samples was proposed to expand a single sample and construct a system that is sufficient to support the traditional method. The virtual sample set of the feature extraction method effectively improved the accuracy and efficiency of security authentication technology. In this paper, the preliminary prediction research study is carried out. In view of the limited data sources and academic level, there are inevitably some limitations in the research. In the current situation analysis stage, the analysis is not thorough enough, only showing the changes of relevant indicators and lacking internal judgment analysis. In the theoretical research stage, the grasp of theory is not deep enough. Future research should address strategies in face information collection.

Data Availability

The datasets used and/or analyzed during the current study are available from the corresponding author on reasonable request.

Conflicts of Interest

The authors declare that there are no conflicts of interest.

References

[1] S. Kabanda and I. Brown, "A structuration analysis of Small and Medium Enterprise (SME) adoption of E-Commerce: the case of Tanzania," *Telematics and Informatics*, vol. 34, no. 4, pp. 118–132, 2017.

[2] C. Boyd, C. Cremers, M. Feltz, K. G. Paterson, B. Poettering, and D. Stebila, "ASICS: authenticated key exchange security incorporating certification systems," *International Journal of Information Security*, vol. 16, no. 2, pp. 151–171, 2017.

[3] M. Anisetti, C. Ardagna, E. Damiani, and G. Polegri, "Test-based security certification of composite services," *ACM Transactions on the Web*, vol. 13, no. 1, pp. 1–43, 2019.

[4] O. Tsvilii, "Cybersecurity regulation: cybersecurity certification of operational technologies," *Technology Audit and Production Reserves*, vol. 1, no. 57, pp. 54–60, 2021.

[5] R. Min, N. Kose, and J. L. Dugelay, "KinectFaceDB: a kinect database for face recognition," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 44, no. 11, pp. 1534–1548, 2014.

[6] J. Lu, V. E. Liong, G. Wang, and P. Moulin, "Joint feature learning for face recognition," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 7, pp. 1371–1383, 2015.

[7] M. Yang, X. Wang, W. Liu, and L. Shen, "Joint regularized nearest points for image set based face recognition," *Image and Vision Computing*, vol. 58, no. C, pp. 47–60, 2017.

[8] J. L. Hernandez-Ramos, S. N. Matheu, and A. Skarmeta, "The challenges of software cyber security certification," *IEEE Security and Privacy Magazine*, vol. 19, no. 1, pp. 99–102, 2021.

[9] S. N. Matheu, J. L. Hernandez-Ramos, and A. F. Skarmeta, "Toward a cyber security certification framework for the Internet of things," *IEEE Security & Privacy*, vol. 17, no. 3, pp. 66–76, 2019.

[10] L. P. Xu, "Application of virtual network technology in computer network security," *Software*, vol. 43, no. 4, pp. 171–173, 2022.

[11] Y. Q. Liu and X. Y. Li, "Mobile secure payment scheme using identity-based cryptographic Algorithm+SMS verification code," *Computer Science*, vol. 47, no. 1, pp. 293–301, 2020.

[12] K. B. Fang, Z. W. Qin, C. Y. Yang, and C. K. Wang, "Password lock SMS dynamic password public verification simulation in mobile terminal," *Computer Simulation*, vol. 36, no. 4, pp. 115–119, 2019.

[13] D. K. Kipker, "EU cyber security act and certification schemes: an up-to-date progress report," *Datenschutz und Datensicherheit - DuD*, vol. 44, no. 6, pp. 390–392, 2020.

[14] C. Zhou and M. H. Li, "Iris system based on multi-channel convolutional neural network," *Journal of Jiujiang University (Natural Science Edition)*, vol. 36, no. 2, pp. 65–67, 2021.

[15] Z. Liu, "Development and application of fingerprint verification system based on LabVIEW," *Computer Knowledge and Technology*, vol. 17, no. 10, pp. 246–248, 2021.

[16] J. Doubleday, "DOD: "Security is an allowable cost" in shift toward new cyber certification," *The Pentagon*, vol. 35, no. 25, pp. 9-10, 2019.

[17] E. Lachaud, "The General Data Protection Regulation and the rise of certification as a regulatory instrument," *Computer Law & Security Report*, vol. 34, no. 2, pp. 244–256, 2018.

[18] A. L. Ma, H. X. Peng, Y. Zhang, Y. Zhang, and S. He, "Analysis and research on commercial cryptography application strategy of information system," *Telecom Engineering Technics and Standardization*, vol. 23, no. 18, pp. 124-125, 2021.

[19] Q. C. Wang and Z. G. Wu, "A survey on security and privacy problems in application systems of face recognition," *The Journal of New Industrialization*, vol. 9, no. 5, pp. 47–50, 2019.