Hindawi
Wireless Communications and Mobile Computing
Volume 2022, Article ID 1761154, 11 pages
https://doi.org/10.1155/2022/1761154

Research Article

Trend and Identification Analysis of Anti-investigation Behavior in Crime by Machine Learning Fusion Algorithm

Junshan Zhang and Yang Lei

Investigation Department, Fujian Police College, Fuzhou, 350007 Fujian, China

Correspondence should be addressed to Junshan Zhang; zjs@fjpsc.edu.cn

Received 24 March 2022; Revised 19 April 2022; Accepted 28 April 2022; Published 19 May 2022

Academic Editor: Chia-Huei Wu

In recent years, people's living standards have gradually improved, and informatization has brought convenience, but it has also led to many criminal cases. Because the criminals' criminal methods are diverse and constantly renovated, this feature is very prominent, and the illegal activities on the Internet are becoming more and more intense. Therefore, it is necessary to strengthen the research on the trend and identification of anti-investigation behavior in crime. The purpose of this paper is to study how to use machine learning fusion algorithms in the trend and identification of anti-investigation behavior in crime. This paper proposes a machine learning fusion algorithm and the basic conceptual knowledge of anti-investigation behavior in crime. The experimental results of this paper show that with the increasing number of criminal incidents, criminals' means of committing crimes have also been improved. The anti-investigation capabilities of criminals have also become more sophisticated, which makes the work of law enforcement officers more difficult. The anti-investigation behavior of criminals in crime has many characteristics, among which the concealment reaches 54%-68%, and the virtuality reaches 68%-79%. It can be seen that the characteristics of criminals' anti-investigation behavior provide a wider space for criminals to commit crimes. The advantage of the machine fusion algorithm is that the classification rules generated are easy to understand and have high accuracy, so it is very suitable for the classification and identification of anti-investigation behaviors in crimes. Therefore, it is urgent to use machine fusion algorithms to identify them.

1. Introduction

With the development of Internet technology, the impact of cybercrime on people's production and life cannot be underestimated. Therefore, the legislation, law enforcement, and judicial system of cybercrime should be adjusted quickly. Since the development trend of cybercrime usually coincides with the development of network technology, the understanding and handling of cybercrime should also be in line with the technological development trend. The most direct harmful consequence of illegal crime is the victim, whether it is a property crime, or a violent crime that violates the right to life and health. Most of the victims are people or the victim's property.

In the era of network information sharing, cybercrime help can be seen everywhere in the network. This allows the practitioner and the helper to participate in the crime without the need for contact. And in most cases, the purpose and motive of practicing people and helping people are not the same. At the same time, there is no temporal consistency between the two in terms of crime implementation. That is, the helper may have already published "criminal technology" in the network, which has a certain degree of independence. The practitioner is looking for "technical support" on the Internet after having a criminal motive, which has a certain randomness.

The innovations of this paper are as follows: (1) It introduces the theoretical knowledge of machine learning fusion algorithm and anti-investigation behavior in crime. It also uses machine learning fusion algorithm to analyze the trend and importance of machine learning fusion algorithm in anti-investigation behavior in crime. (2) It expounds the machine learning fusion algorithm and antireconnaissance behavior. Through experiments, it is found that the

identification of intelligent anti-investigation behavior based on machine learning fusion algorithm is conducive to the smooth progress of law enforcement work.

2. Related Work

With the development of science and technology in recent years, the development of the Internet of Things is also getting faster and faster. Coley et al. found that computer-aided synthesis design has been around for over 40 years. But reverse integrated planning software has struggled to achieve widespread adoption. A key challenge in developing high quality is that it is difficult to achieve in the laboratory. They proposed a model framework for predicting reaction outcomes. The framework combines the traditional use of reactive templates with the flexibility of pattern recognition provided by neural networks. Although they scholar found that it is difficult to achieve high-quality development in real life, and also proposed a solution model framework, they did not experiment with the framework [1]. Voyant et al. found that predicting the output power of a solar system is necessary for the good operation of the grid. Before predicting the output of the solar system, the forecast must focus on solar irradiance. Global solar radiation forecasts can be made through a variety of methods, such as cloud images combined with physical models and machine learning models. In this context, their aim is to outline methods for predicting solar radiation using machine learning methods. Although the scholars found that the combination of machine learning and cloud images is more beneficial to the operation of the power grid, they did not specify how the method works [2]. Zhou et al. find that machine learning (ML) continues to unleash its power in a wide range of applications. It has been pushed to the forefront in recent years, in part due to the advent of big data. Big data enables machine learning algorithms to spot finer patterns and make more timely and accurate predictions than ever before. They introduced the big data machine learning framework to face the opportunities and challenges. But the scholars did not specify what the challenges and opportunities are [3]. Kavakiotis et al. found that remarkable advances in biotechnology and health sciences have led to the generation of massive amounts of data, such as high-speed genetic data and clinical information generated from large electronic health records. For this reason, the application of machine learning and data mining methods in biological sciences is now more important and indispensable than ever. It intelligently transforms all available information into valuable knowledge. Although the scholars found the advantages of big data, there is no concrete example to prove its advantages [4]. Liu et al. discovered interactive model analysis, the process of understanding, diagnosing, and refining machine learning models with the help of interactive visualizations. It is very important for users to effectively solve real-world artificial intelligence and data mining problems. The huge advances in big data analytics have led to the emergence of a wide variety of interactive model analysis tasks. They provide a comprehensive analysis and explanation of this rapidly developing field. But the scholars did not introduce in detail how they analyzed and explained the rapid development of this field [5]. Kolouri et al. found that transmission techniques for signal and data analysis have received increasing attention recently. Given their ability to provide accurate generative models for signal strength and other data distributions, they have been used in a variety of fields. It includes content-based retrieval, cancer detection, image superresolution, and statistical machine learning, among others, and they have been shown to produce state-of-the-art results. They provide a practical overview of the mathematical underpinnings of methods related to mass transport, including numerical implementation, as well as a review and demonstration of several applications. But the scholars did not elaborate on the review and demonstration [6]. Brynjolfsson and Mitchell found that thanks to recent advances in machine learning, it is now at the beginning of a larger and faster transformation that can accelerate the pace of automation itself. However, while it is clear that ML is a "general purpose technology," there is no broad consensus on what tasks ML systems are good at. Although the scholar realizes that there is no broad consensus on ML systems, no specific solutions have been proposed [7]. Thrall et al. found that interest in artificial intelligence (AI) applications, including imaging, is high and growing rapidly, driven by the availability of large datasets, significant advances in computing power, and new deep learning algorithms. In addition to developing new AI approaches, there are also many opportunities and challenges. Artificial intelligence programs can be used to extract "radioactive" information from images that cannot be discerned by visual inspection. This in turn may increase the diagnostic and prognostic value derived from image datasets. Radiologists are more likely to beneficially incorporate AI approaches into their practice. However, the scholars have no specific data to illustrate that artificial intelligence can be integrated into medicine [8].

3. Support Vector Machine Classification and Recognition Method Based on Machine Learning Fusion Algorithm

The current society is undergoing tremendous changes in terms of economy, politics, science, and technology, and various illegal and criminal acts often appear around us [9]. These high-tech, gang-based, and intelligent criminal behaviors seriously affect people's normal life order. This paper analyzes the development trend of cybercrime from 2010 to 2020, as shown in Figure 1.

As shown in Figure 1, the development of cybercrime increased by 10% in 2010, and the development of cybercrime in 2020 increased by 43%, which is a 33% increase from 2010. At present, China's network security legislation is still in its infancy, and it is difficult to keep up with the pace of network technology development. No matter in criminal investigation or network operation security, there is no normative and systematic legal system [10–12]. Under the high-risk situation of cybercrime, the traditional investigation cooperation mode is difficult to deal with the challenges brought by cybercrime. The current investigation

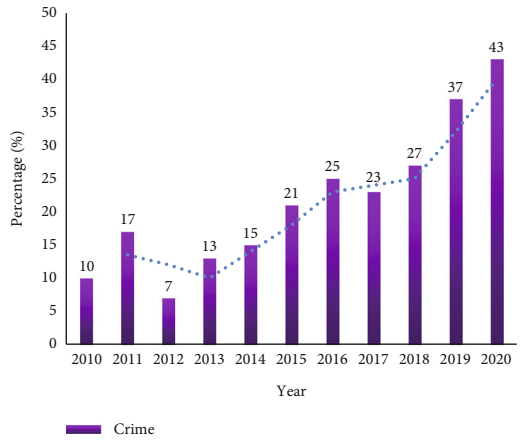


Figure 1: The development trend of cybercrime from 2010 to 2020.

cooperation and the technical means of investigators need to be completely updated and upgraded [13].

Investigation is a very important step in the process of handling a criminal case. It refers to special investigations carried out by procuratorial, public security and other organs in criminal procedures, as well as relevant compulsory measures to discover criminal facts, resolve cases, and arrest criminal suspects [14]. Anti-investigation simply means that the perpetrators are more familiar with the investigators' investigation methods. However, when committing a crime, the practice is more clever and will not leave some clues to the investigators at the scene that are conducive to the investigation of the case. The schematic diagram of the investigation is shown in Figure 2.

As shown in Figure 2, informatization surveys mainly rely on scientific and technical means for collecting, managing, and using information. It connects the latest information technology, network technology, and computer technology with investigative work. It infiltrates information and intelligence into the whole investigation activity with intelligence and forms a new investigation mode and case processing that combines crime prevention and countermeasures [15].

With the popularity of online shopping and online banking payment services, there are more and more attack methods, such as network eavesdropping and fraud, threatening the property and privacy of network users [16]. A higher degree of attention should be paid to network traffic related to finance, payment, real-time stock fluctuations, etc., to protect the property safety of network users. This article analyzes the number and growth percentage of online shopping from 2011 to 2020, as shown in Tables 1 and 2.

As shown in Tables 1 and 2, today's network scale continues to expand, network traffic grows explosively, and network threats also grow simultaneously. Identifying network traffic can solve the problem to a certain extent [17, 18]. Network traffic identification can distinguish normal traffic from threats to defend against attacks. However, network traffic identification not only needs to analyze massive data but also realize real-time monitoring without affecting network performance, which requires high computing time and computing space [19–21].

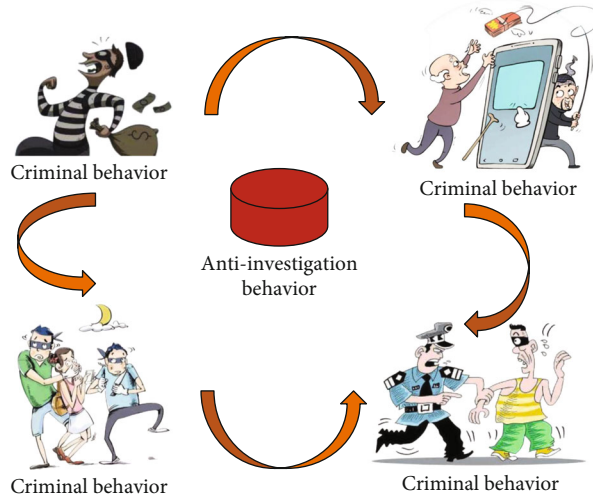


Figure 2: Schematic diagram of reconnaissance.

Table 1: Quantity and percentage growth of online shopping, 2011-2015.

Years	Quantity(ten thousand)	Percentage%	Growth rate
2011	1563.87	5.6	2.1%
2012	3764.60	7.8	2.2%
2013	6730.42	12.7	4.9%
2014	9072.65	18.4	5.7%
2015	12749.09	31.7	13.3%

Table 2: Quantity and growth percentage of online shopping 2016-2020.

Years	Quantity(ten thousand)	Percentage%	Growth rate
2016	38940.42	39.0	8.3%
2017	53630.09	56.5	17.5%
2018	89050.42	65.7	9.2%
2019	125314.79	78.3	12.6%
2020	156789.69	89.9	9.2%

3.1. Hidden Potential Forms of Cybercrime

3.1.1. Ransomware. Ransomware is developed based on Trojan horses, and its essence is a Trojan horse with specific functions. After experiencing ransomware attacks and kidnapping user files, infected computer users cannot use the computer normally and cannot display important data [22]. The process of ransomware is shown in Figure 3.

As shown in Figure 3, ransomware has appeared frequently in the past year. Ransomware is a form of spreading through emails, web pages, removable media, etc. It also encrypts the files on the victim's computer and demands a certain ransom after the victim executes it. User data includes documents, emails, databases, source codes, images, compressed files, and other files [23].

3.1.2. Botnet. A botnet is a complex network of computers infected with malicious code. The so-called botnet is

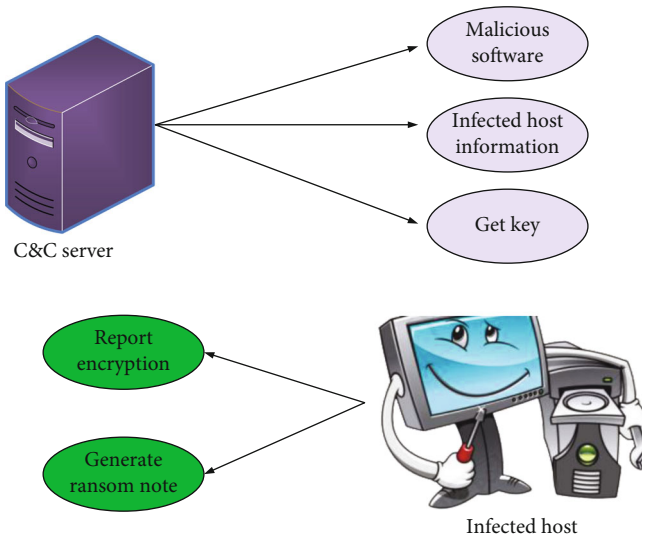


Figure 3: The flow of ransomware.

controlled by embedding malicious code into the computer through various methods, that is, the bot host that conducts malicious attacks [24]. Botnet refers to the use of one or more means of transmission to infect a large number of hosts with bot program viruses. It thus forms a one-to-many controllable network between the controller and the infected host. As shown in Figure 4.

As shown in Figure 4, according to the professional definition of a botnet, a botnet consists of 4 main elements. Malicious attackers control the botnet infected with malicious code through the C&C server, and the control channel implements malicious actions [25]. After the malicious attacker develops the malicious code of the program, the malicious code is embedded in multiple computers by various methods.

Malicious code is also known as malware, a code that can perform unauthorized operations on a computer system to destroy or steal information. Malicious code ranges widely and includes programmatic computer security threats that exploit various networks, operating system, software, and physical security vulnerabilities to deliver malicious payloads to computer systems. Some malicious codes will periodically send heartbeat packets to maintain the connection with the C&C server, notify the online status, and control the transmission speed of data packets [26, 27]. Therefore, the interval time between the arrival of data packets is also an important indicator used by malicious codes to characterize network communication patterns. The average time interval and standard deviation of the forward packets are shown in Figure 5.

Figure 5 shows the network data generated by the heartbeat mechanism of the malicious code. Compared with normal network services, the network traffic generated by malicious code is obviously different from the average time interval of the forwarded packets to the aggregated flow and the standard deviation of the arrival time of the transmitted packets. In addition, from the point of view of the time interval between the arrival of data packets, the network traffic generated by malicious code is significantly different from that of normal network access, and the standard deviation is smaller.

3.2. Support Vector Machine (SVM) Classification and Recognition Algorithm. Support vector machine, also known as "support vector network," is a discriminative machine learning classification algorithm. It uses decision boundaries (hyperplanes in this case) to separate data points into two classes at a time. The basic idea of SVM is to find an optimal classification hyperplane that can divide the sample points into two categories and make the distance between the sample points and the hyperplane the largest. This spacing represents the confidence that the sample is positive or negative. The earliest SVM was proposed for binary classification problems. As shown in Figure 6.

As shown in Figure 6, finding the optimal hyperplane is transformed into a minimization formula. In the linearly separable case, the SVM requires the solution to the minimum value of

$$\varphi(w, \xi) = \frac{1}{2}\|w\|^2, \tag{1}$$

where w is the normal vector of the hyperplane, and $b \in R$ is the threshold. In practical applications, and there is often a linear inseparability, so the slack variable should be added to formula (1), which is $\xi \geq 0$. When there is a classification error, the penalty factor of $C \succ 0$ is introduced as the wrongly classified sample as

$$\varphi(w, \xi) = \frac{1}{2}\|w\|^2 + C\sum_{i=1}^{n}\xi_i. \tag{2}$$

The Lagrangian function is a function of only conservative forces in the mechanical system and is a function that describes the dynamic state of the entire physical system. The introduction of the Lagrange function can be used to solve the penalty factor, and formula (3) is obtained:

$$L(w, b, a) = \frac{1}{2}w^T w + C\sum_{i=1}^{n}\xi_i, \tag{3}$$

where $a_i \geq 0$ is the Lagrange coefficient, and solving the hyperplane becomes the minimum value of the Lagrange function for w and b. If a_i^* is the optimal solution, then $w^* = \sum_{i=1}^{n} a_i^* b_i a_i$. The sample whose a_i^* is not zero is the support vector, and the optimal classification function obtained from this is

$$f(a) = \operatorname{sgn}\left((w^*)^T + b^*\right) = \operatorname{sgn}\left(\sum_{i=1}^{n} a_i^* b_i + b^*\right). \tag{4}$$

SVM uses the obtained best classification hyperplane to distinguish various types of samples. The optimal classification hyperplane is determined by the classification function and support vector. The crux of the problem is to find the most appropriate penalty factor under the

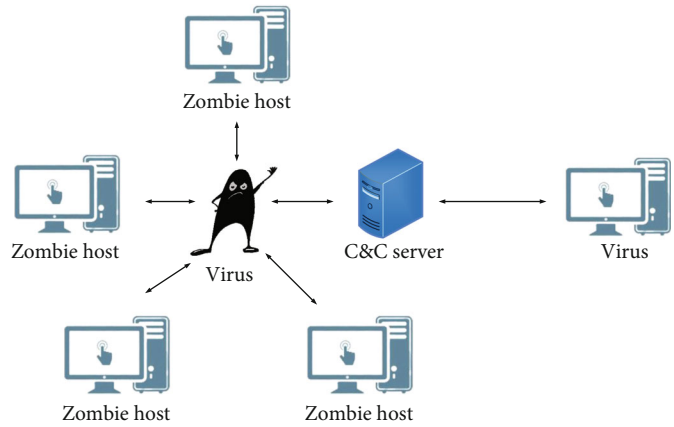
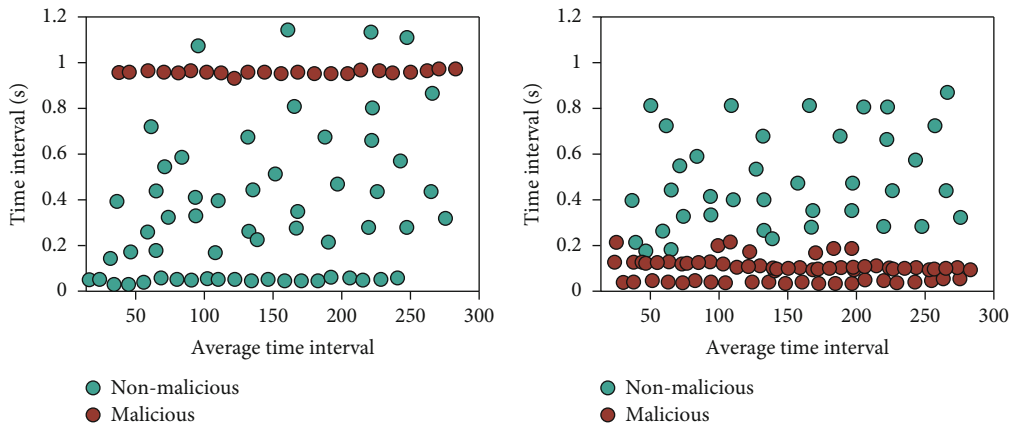


Figure 4: Botnet.



(a) Average time interval of forward packets

(b) Standard deviation of forward packet time interval

Figure 5: Packet arrival time interval.

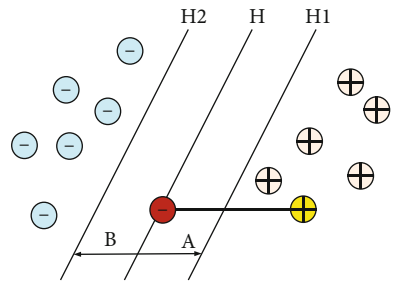


Figure 6: Graphical representation of hyperplane in high-dimensional space.

optimal kernel function for maximizing the correct classification rate.

3.3. Feature Selection Algorithm. Machine learning methods study how computers simulate human learning behavior. It acquires new knowledge or skills and reorganizes the existing knowledge structure to continuously improve itself. Computers learn patterns and patterns from data to apply to the task of making predictions on new data. When classifying or identifying samples using machine learning methods, it is often necessary to collect as many features as possible in order to represent the sample in as much detail as possible. When there are features that are not relevant for classification, the training of functions and models takes longer. In order to improve the efficiency of network traffic identification based on network data flow classification, it is of great significance to select the characteristics of network data flow to be classified. The general process of feature selection is shown in Figure 7.

As shown in Figure 7, the definition of feature selection is as follows: it selects a set of features corresponding to a specific evaluation standard from a set of N original feature sets and achieves the optimal feature set. Excellent feature subsets should have higher correlation and lower redundancy. It can measure the linear correlation between vectors through the linear correlation coefficient as

$$R(i) = \frac{\operatorname{cov}(A_i, B)}{\sqrt{\operatorname{var}(A_i)\operatorname{var}(B)}}. \tag{5}$$

Evaluating feature subsets with distance $\operatorname{cov}(A_i, B)$ is based on following the assumption: an excellent feature subset should make the same type of samples aggregate, and different types of samples are scattered. Commonly used

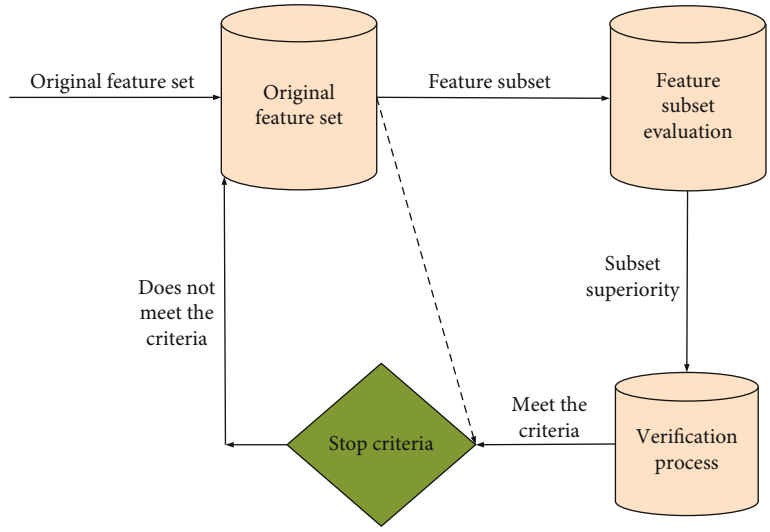


Figure 7: General process of feature selection.

distance calculation methods include Euclidean distance, data covariance distance, standardized Euclidean distance, etc. Euclidean distance is also called Euclidean distance. It is a commonly used definition of distance, which is the true distance between two points in m-dimensional space. Euclidean distance in 2D and 3D space is the distance between two points.

It assumes that there are discrete variables B, $B \in \{b_1, b_2, \cdots, b_m\}$, and b_i with probability P_i. Then, the information entropy of B is defined as

$$H(B) = -\sum_{i=1}^{m} P_i \log_2 P_i. \tag{6}$$

The more uniform the probability of the samples in B, the smaller the $H(B)$; the more special cases occur, the larger the $H(B)$.

3.4. Harris Corner Detection Algorithm. Harris corner detection is the basis of feature point detection. It proposes the concept of applying the grayscale difference of adjacent pixels to judge whether it is a corner, edge, or smooth area. In the Harris corner detection algorithm, the degree of gray value change of the pixels in the image can be represented by the so-called autocorrelation function. It then solves the curvature of the autocorrelation function to reflect its gradient change, so as to judge the corner points according to the above rules. It assumes that the autocorrelation function can be expressed as

$$E(a, b) = \sum_{u,v} w_{u,v} \left| I_{a+u,b+v} - I_{u,v} \right|^2. \tag{7}$$

In the formula, the average value of the image gray value change caused by moving the window size of (a, b) near pixel (u, v) is represented by $E(a, b)$. If the pixel is a corner point, $E(a, b)$ will have a larger change. I represents the grayscale of the pixels in the image, and $w_{u,v}$ represents the window of the image. It is then further rewritten as

$$E(a, b) = \sum_{u,v} w_{u,v} \left[aI_a + bI_b + o\left(a^{2,b^2}\right) \right]^2 \approx [a, b] M^T (a, b). \tag{8}$$

The Gaussian function has a wide range of applications and can be seen in the fields of natural science, social science, mathematics, and engineering. Then, a Gaussian function is used to smooth the four elements of M to obtain a new M. The filter function is as shown in

$$\text{Gauss} = \exp\left(-\frac{a^2 + b^2}{2\sigma^2}\right). \tag{9}$$

Next, a new concept is introduced to assist corner judgment. It uses M to calculate the corner point quantity ϕ of each pixel point as in

$$\phi = \frac{I_a^2 I_b^2 - (I_a I_b)^2}{I_a^2 + I_b^2}. \tag{10}$$

When the value of the corner point quantity ϕ is greater than a given threshold, and when it is the local maximum value in the neighborhood of the current point, it can be considered that the pixel point is a corner point.

After adding a descriptor to each feature point, it can be determined whether it is a pair of matching points by finding the similarity of the feature descriptors in the two images, as shown in

$$\rho(m, n) = \sqrt{\sum_{i=1}^{k} (m(i) - n(i))^2}, \tag{11}$$

where m represents the 64-dimensional feature description vector of the first feature point to be matched. n represents the m-dimensional feature description vector of the second feature point to be matched.

3.5. Consensus Decision-Making Method. The consensus decision-making method was aimed at achieving "universal agreement." It meets the opinions of as many people as possible through the decision-making process and is not opposed by a few people, so as to achieve universal approval. At the same time, in the discussion process of participants, new ideas are inspired, new ideas are obtained, more perfect conclusions are obtained, and consensus decision-making ideas are used. Each feature selection algorithm is equivalent to an expert as a decision-making participant, and the features selected by the algorithm are the opinions of each expert.

If q alternatives are selected, the evaluation value of each selected alternative is

$$w_i^k = \frac{1}{q}, (k = 1, 2, \cdots M, i = 1, 2, \cdots, N). \tag{12}$$

It first converts ordinal relation value σ_i^k to utility value u_i^k as

$$u_i^k = N - \sigma_i^k + 1. \tag{13}$$

It then normalizes the preference vector composed of utility values.

3.6. Hidden Markov Models. Hidden Markov models are statistical models that describe a Markov process with hidden unknown parameters. The difficulty is to determine the implicit parameters of the process from the observable parameters. It then uses these parameters for further analysis, such as pattern recognition. When it comes to the difference between Markov chains and hidden Markov models, the most obvious difference is whether the observed state is visible or not. In a Markov chain, the states are discrete. But it can be seen directly to the observer that the state transition probability $S_j(i)$ is the only parameter in the Markov chain, which is

$$S_j(i) = e_j(a_i)^* \max_k a_{kj} S_k(i-1). \tag{14}$$

But in a hidden Markov model, the only state is not directly visible. Instead it has two states, called observed state $P(a, \pi^*)$ and hidden state π_N^*, which is for

$$P(a, \pi^*) = \max_k S_k(N), \tag{15}$$

$$\pi_N^* = \arg \max_k S_k(N). \tag{16}$$

The function of the Markov model is to maximize all states k. It finds the most probable sequence at the end of the sequence, as

$$S_j(i) = e_j(a_i)^* \max_k a_{kj} S_k(i-1). \tag{17}$$

It can also solve three types of problems: evaluation problems, decoding problems, and learning problems. The model can be used in many fields, such as gene sequence discovery, computational linguistics, and speech recognition.

Naive Bayes is a classification method based on Bayes' theorem and the assumption of feature condition independence. The two most widely used classification models are decision tree models and naive Bayesian models. Naive Bayesian model is a generative supervised learning algorithm based on Bayesian theory. Compared with decision trees, Naive Bayesian models are less sensitive to missing data. At its core is the Bayesian formula. If b and a_n are given, and a_n is independent of each other, then formula (18) and formula (19) can be obtained:

$$P(a|b) = \frac{P(b|a)P(a)}{P(b)}, \tag{18}$$

$$P(a_1, \cdots, a_n|b) = P(a_1|b) \cdots P(a_n|b). \tag{19}$$

3.7. Trends in Anti-investigation Behavior

(1) The means of creating fakes are constantly being innovated. In some cases, it is concealed by remittances to the current balance of the unit or by means of remittances from the account of a commercial unit. For stock trading, the method of cooperating with the inside and the outside and knocking it down puts the investigation activities in an extremely unfavorable situation

(2) The initiative of anti-investigation behavior is enhanced. So far, suspects have rarely explored methods of evading searches before committing a crime, hiding accounts after committing a crime, etc. However, in the current search practice, the perpetrators in most cases make long-term careful planning. It investigates the case during the search phase and holds the leading power in the anti-investigation activities

(3) The diversity of anti-investigation methods is outstanding. In recent years, the original detailed accounts have been hidden and destroyed due to suspicion of corruption and bribery. Or the production of false evidence in order to resist investigation and avoid legal sanctions is increasingly evident, disturbing the sight of the investigators and hindering its orderly conduct of the incident handling work

(4) The cross-infection of anti-investigation behavior expanded. For example, detention centers, prisons, and labor farms are special social places where criminals are transformed into new people. These people can exchange criminal experiences and learn new and effective countermeasures. The constant imitation and learning among criminals improves the overall crime level

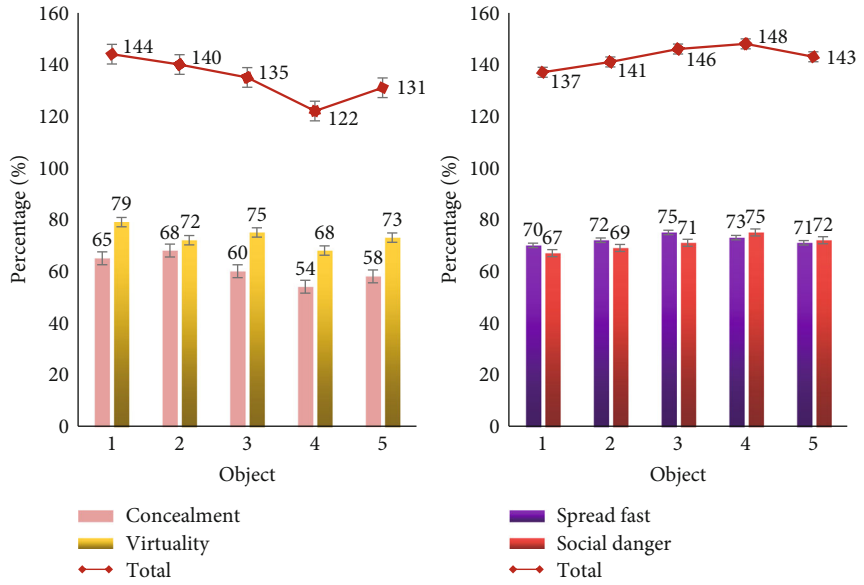


Figure 8: Characteristics of anti-investigation behavior in crime.

4. Experiment and Analysis of Anti-investigation Behavior in Crime

4.1. Characteristics of Anti-investigation Behavior in Crimes. In recent years, with the rapid development and widespread popularization of Internet technology, more and more traditional industries are integrated with "Internet +." With the rapid development of the Internet, many problems have also arisen and a large number of criminal risks have arisen. Among them, anti-investigation behaviors emerge in an endless stream. The characteristics of anti-investigation behavior in crime are shown in Figure 8.

As shown in Figure 8, the anti-investigation behavior in crime has the characteristics of strong concealment, strong virtuality, fast transmission speed, and great social harm. In addition, it also has its own unique characteristics in the form of expression and the reason for the event. Although the public security organs have accumulated a lot of experience in the countermeasures of criminal searches, the criminal behavior on the Internet still adds new difficulties.

Under the background of the continuous impact of a large amount of information, such as the Internet and big data, the anti-investigation awareness and ability of criminal subjects have been enhanced. The means of crime are increasingly hidden, complex, dynamic, and intelligent. The traditional criminal investigation methods and means have been unable to solve the problems of difficulty in finding, verifying, and dealing with cases. At present, the most basic source and fundamental work of criminal investigation is how to obtain and use information, expand the scope of investigation, and improve the ability of investigation.

Information technology and communication technology are developing rapidly. In order to effectively deal with the new characteristics of more concealed and intelligent crimes, the procuratorial organs must further strengthen the construction of information technology in the process of handling cases and promote the overall improvement of the investigation ability and level. This in turn strengthens the criminal investigation function of the procuratorate. However, in the practice of criminal investigation, traditional investigation methods and technical methods have been unable to meet the needs of the increasing expansion of investigation information and data and the increasing diversity of content.

Table 3: Comparison of original feature selection algorithms and consensus decision feature extraction classification.

	Genetic	Random	All feature	Best first
Number of support vectors	1060	4770	1007	6709
Accuracy	96.56%	98.05%	97.68%	95.97%
Mean squared error	0.43	0.41	0.40	0.39
Number of features	15	12	50	10

4.2. Characteristics of Antireconnaissance Behavior Recognition Based on Machine Fusion Algorithm. With the rapid development of social informatization and crime situation, the concept of informatization investigation came into being. "Intelligence and information lead policing" is the first concept of information-based investigation. Affected by this idea, countries around the world have gradually realized the informatization of police affairs and have achieved considerable results. This concept refers to the use of advanced information technology to integrate police information resources to obtain more faster and more accurate intelligence information. This improves the ability of police situation prediction, precise strike, and emergency handling.

(1) The scope of investigation is wide. Criminal informatization investigation is based on the procuratorial basic business information system and

Table 4: The effect of the number of features on the classification results.

Number of features	6	7	8	9	10	11
Training time (s)	584.5	260.4	301.5	246.8	231.6	212.7
Number of support vectors	32	45	68	31	54	36
Forecast time (s)	154.5	108.4	99.3	105.2	100.3	103.2
Accuracy	95.7%	96.1%	96.2%	96.3%	96.6%	96.7%

integrates the business system information of other social functional departments to carry out investigation activities. The criminal informatization investigation mode makes the investigation activities no longer limited by the scope of personnel, industries, and regions

(2) Quick response. In the traditional investigation mode, the investigation activities are mainly completed by people, and the workload of investigation activities is large, and the work cycle is too long. It involves a large range of personnel and low work efficiency, and investigators are prone to fatigue and fatigue. The crime informatization investigation mode mainly relies on the intelligence information system of the computer and uses the computer's high-speed operation, precise memory, and rapid judgment ability. It makes timely responses to intelligence information in the investigation activities, and the response is fast and accurate, which is helpful for the timely breakthrough of the case

(3) The process is kept confidential. Carrying out investigation with the help of intelligence information system and computer network is the characteristic of crime information investigation. Compared with the way that traditional investigation activities need to directly contact the relevant personnel of the case, the information-based investigation basically does not directly contact the relevant personnel of the case. It obtains relevant information in a more confidential way through the corresponding business information system. The entire investigation process has strong confidentiality

(4) It saves the cost of handling cases. The criminal informatization investigation mode liberates a lot of manpower from investigation activities. It makes the investigators do not have to rely on fatigued combat methods such as traditional enclosures, raids, and crowd tactics. This greatly eases the problems of the grassroots procuratorate's case-handling personnel and funding constraints

4.3. Feature Selection Experiment and Result Analysis Based on Consensus Decision. Limited to the hardware environment at the time, the cost of training time and test time is uncertain, so we only compare the accuracy rate and the number of features used for testing. It uses feature selection algorithm to reduce the number of features used for classification and still can ensure high classification accuracy. The comparison between the original feature selection algorithm and the consensus decision feature extraction classification is shown in Table 3.

As shown in Table 3, the feature set obtained by comparing the consensus decision algorithm and the feature set obtained by other feature selection algorithms adopt the same SVM classification algorithm. It can be seen that the features obtained using the consensus decision method are used for classification. It achieves the result of the highest classification accuracy with the smallest number of features, while the mean square error is the smallest, and the result is more stable.

4.4. The Influence of the Number of Features on the Recognition Results. While confirming the superiority of the feature selection of the consensus decision-making method, this paper further explores the influence of the number of features on the classification results according to the different support degrees of the features provided by the algorithm to the classification contribution.

The results for training time, number of support vectors, test time, accuracy, and mean squared error are listed in Table 4 for feature numbers from 4 to 14.

The change trend of these test experimental data after scaling is shown in Figure 9.

It can be seen from Figure 9 that with the increase of the number of features, the recognition accuracy gradually increases. The number of support vectors, training time, test time, and mean square error gradually decreases and stabilizes after the number of features is 8. It can be seen that the number of features has a significant impact on the system performance and can be properly adjusted according to actual needs. After selection or transformation, identification features are formed, and classification information is preserved as much as possible. On the premise of ensuring a certain classification accuracy, it reduces the feature dimension, so that the classifier can work quickly and accurately.

5. Discussion

This paper discusses how to use machine learning fusion algorithms to research and analyze trends and identification of anti-investigation behaviors in crime. The theoretical knowledge related to machine learning fusion algorithm and anti-investigation behavior is described, and the trend of anti-investigation behavior in crime is focused on. A more scientific method of data statistics is explored, and the effect of machine learning fusion algorithm on the trend and identification of anti-investigation behavior in crime is discussed

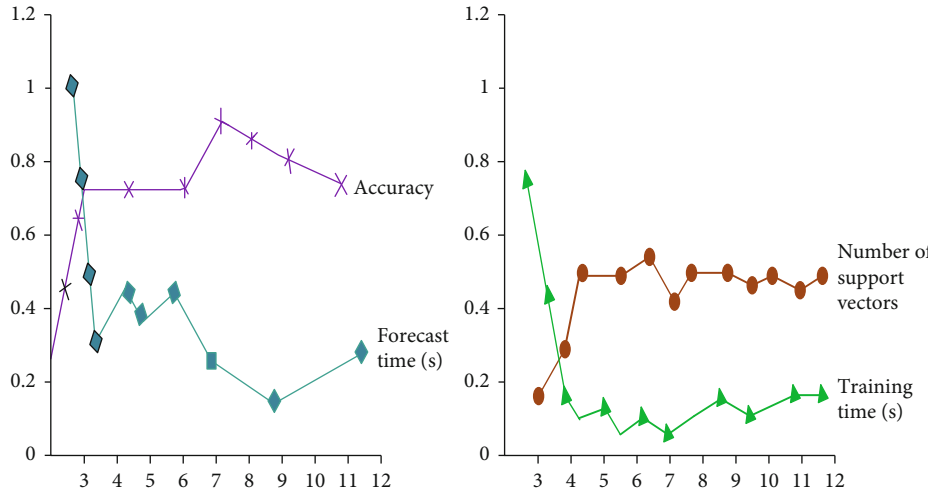


Figure 9: The influence trend of the number of features on the recognition results.

through experimental analysis. Its final finder learning fusion algorithm can make the trend and identification of anti-investigation behavior in crime more efficient.

In this paper, cluster analysis is also studied, and support vector machines and Harris corner detection algorithms are studied. It compares the traditional detection algorithm with the consensus decision method and finally finds that the feature selection based on consensus decision plays an important role in identification. It can make image or behavior recognition faster.

From the experimental analysis in this paper, we can know the method of using machine learning fusion algorithm in the trend and identification of anti-investigation behavior in crime. Not only can the trend of anti-investigation behavior in crime and the efficiency of identification become higher, but the accuracy of data statistics has also been greatly improved.

6. Conclusion

In this fast-developing society, crime still emerges in an endless stream. With the increase of the penetration rate of netizens and the continuous integration of the network and life, the virtual society is gradually formed. It also projects a dual social form in which real society and virtual society coexist. The role of the Internet in cybercrime is not only the tool and object of crime. And criminals are becoming more and more proficient in anti-investigation behaviors in crimes, which makes it difficult for law enforcement officers to work. Therefore, this paper proposes the use of machine fusion algorithm to identify and analyze the anti-investigation behavior of criminals in crime. This paper firstly introduces the machine fusion algorithm and antireconnaissance behavior. Then the method part analyzes the machine fusion algorithm and finds that the support vector machine algorithm in the machine fusion algorithm has a good recognition function. In the experimental part, the characteristics of anti-investigation behavior in crime are analyzed. It found that the anti-investigation behavior in the crime has the characteristics of strong concealment, strong virtuality, fast transmission speed, and great social harm. Therefore, it is very necessary to accurately identify it. At the end of the experiment, the feature selection based on consensus decision-making is tested and analyzed, and it is found that the recognition effect of feature selection based on consensus decision-making is also very good.

Data Availability

The data that support the findings of this study are available from the corresponding author upon reasonable request.

Conflicts of Interest

The authors declared no potential conflicts of interest with respect to the research, author-ship, and/or publication of this article.

Acknowledgments

This work was supported by the Humanities and Social Sciences Planning Funding Project of the Ministry of Education (20YJC820028), Research on Ecological Construction of Data Security Governance in Cyberspace, Research on Criminal Suspect Feature Prediction Method Based on Wavelet Neural Network, and Fujian Province Young and Middle-Aged Teachers' Education Research Projects (JAT190446).

References

[1] C. W. Coley, R. Barzilay, T. S. Jaakkola, W. H. Green, and K. F. Jensen, "Prediction of organic reaction outcomes using machine learning," *ACS Central Science*, vol. 3, no. 5, pp. 434–443, 2017.

[2] C. Voyant, G. Notton, S. Kalogirou et al., "Machine learning methods for solar radiation forecasting: a review," *Renewable Energy*, vol. 105, pp. 569–582, 2017.

[3] L. Zhou, S. Pan, J. Wang, and A. V. Vasilakos, "Machine learning on big data: opportunities and challenges," *Neurocomputing*, vol. 237, pp. 350–361, 2017.

[4] I. Kavakiotis, O. Tsave, A. Salifoglou, N. Maglaveras, I. Vlahavas, and I. Chouvarda, "Machine learning and data mining methods in diabetes research," *Biotechnology Journal*, vol. 15, no. C, pp. 104–116, 2017.

[5] S. Liu, X. Wang, M. Liu, and J. Zhu, "Towards better analysis of machine learning models: a visual analytics perspective," *Visual Informatics*, vol. 1, no. 1, pp. 48–56, 2017.

[6] S. Kolouri, S. R. Park, M. Thorpe, D. Slepcev, and G. K. Rohde, "Optimal mass transport: signal processing and machine-learning applications," *IEEE Signal Processing Magazine*, vol. 34, no. 4, pp. 43–59, 2017.

[7] E. Brynjolfsson and T. Mitchell, "What can machine learning do? Workforce implications," *Science*, vol. 358, no. 6370, pp. 1530–1534, 2017.

[8] J. H. Thrall, X. Li, Q. Li et al., "Artificial intelligence and machine learning in radiology: opportunities, challenges, pitfalls, and criteria for success," *Journal of the American College of Radiology*, vol. 15, no. 3, pp. 504–508, 2018.

[9] I. Goodfellow, P. Mcdaniel, and N. Papernot, "Making machine learning robust against adversarial inputs," *Communications of the ACM*, vol. 61, no. 7, pp. 56–66, 2018.

[10] T. H. Nguyen, S. Sridharan, V. Macias, A. Kajdacsy-Balla, J. Melamed, and P. G. Do MN, "Automatic Gleason grading of prostate cancer using quantitative phase imaging and machine learning," *Journal of Biomedical Optics*, vol. 22, no. 3, pp. 280–291, 2017.

[11] S. Rajasoundaran, A. V. Prabu, J. B. V. Subrahmanyam et al., "Secure watchdog selection using intelligent key management in wireless sensor networks," *Materials Today: Proceedings*, 2021.

[12] D. Chen, P. Wawrzynski, and Z. Lv, "Cyber security in smart cities: a review of deep learning-based applications and case studies," *Sustainable Cities and Society*, vol. 66, article 102655, 2021.

[13] M. Fatima and M. Pasha, "Survey of machine learning algorithms for disease diagnostic," *Journal of Intelligent Learning Systems and Applications*, vol. 9, no. 1, pp. 1–16, 2017.

[14] M. Gastegger, J. Behler, and P. Marquetand, "Machine learning molecular dynamics for the simulation of infrared spectra," *Chemical Science*, vol. 8, no. 10, pp. 6924–6935, 2017.

[15] K. T. Butler, D. W. Davies, H. Cartwright, O. Isayev, and A. Walsh, "Machine learning for molecular and materials science," *Nature*, vol. 559, no. 7715, pp. 547–555, 2018.

[16] T. M. Malta, A. Sokolov, A. J. Gentles et al., "Machine learning identifies stemness features associated with oncogenic dedifferentiation," *Cell*, vol. 173, no. 2, pp. 338–354.e15, 2018.

[17] G. L. Nedjati-Gilani, T. Schneider, M. G. Hall et al., "Machine learning based compartment models with permeability for white matter microstructure imaging," *Image*, vol. 150, pp. 119–135, 2017.

[18] O. I. Khalaf and G. M. Abdulsahib, "An improved efficient bandwidth allocation using TCP connection for switched network," *Journal of Applied Science and Engineering*, vol. 24, no. 5, pp. 735–741, 2021.

[19] I. K. Osamh and G. M. Abdulsahib, "Energy efficient routing and reliable data transmission protocol in WSN," *International Journal of Advances in Soft Computing and its Application*, vol. 12, no. 3, pp. 45–53, 2020.

[20] O. I. Khalaf, C. A. T. Romero, S. Hassan, and M. T. Iqbal, "Mitigating hotspot issues in heterogeneous wireless sensor networks," *Journal of Sensors*, vol. 2022, Article ID 7909472, 14 pages, 2022.

[21] J. Zhang, W. Zhuo, and N. Verma, "In-memory computation of a machine-learning classifier in a standard 6T SRAM Array," *IEEE Journal of Solid-State Circuits*, vol. 52, no. 4, pp. 915–924, 2017.

[22] F. Lamperti, A. Roventini, and A. Sani, "Agent-based model calibration using machine learning surrogates," *Journal of Economic Dynamics & Control*, vol. 90, pp. 366–389, 2018.

[23] N. Poret, R. R. Twilley, and R. M. Coronado-Molina, "Object-based correction of LiDAR DEMs using RTK-GPS data and machine learning modeling in the coastal Everglades," *Environmental Modelling and Software*, vol. 112, no. 3, pp. 491–496, 2018.

[24] J. H. Chen and S. M. Asch, "Machine learning and prediction in medicine — beyond the peak of inflated expectations," *New England Journal of Medicine*, vol. 376, no. 26, pp. 2507–2509, 2017.

[25] J. X. Wang, J. L. Wu, and H. Xiao, "Physics-informed machine learning approach for reconstructing Reynolds stress modeling discrepancies based on DNS data," *Physical Review Fluids*, vol. 2, no. 3, article 034603, 2017.

[26] F. P. Reiter, L. Ye, F. Bösch et al., "Antifibrotic effects of hypocalcemic vitamin D analogs in murine and human hepatic stellate cells and in the CCl_4 mouse model," *Laboratory Investigation*, vol. 99, no. 12, pp. 1906–1917, 2019.

[27] J. Z. Ma, L. P. H. Shao Fang, J. Liu, and D. M. Chen, "Network security behavior recognition based on consensus decision-making feature selection," *Applied Mechanics and Materials*, vol. 602, pp. 2188–2194, 2014.