

Construction of Computer Vision Security Model Based on Machine Learning and Artificial Intelligence Networks

Nan Si^{1,a}, Lingli Tan^{2,b,*}, Lu Yin^{3,c} and Zituo Liu^{4,d}

¹*School of Marxism, Xinyang Vocational and Technical College, Xinyang 464000, Henan, China*

²*School of Computer Science, Wuhan Donghu University, Wuhan 430212, Hubei, China*

³*Institute for Research on Portuguese-speaking countries, City University of Macao, Macao 999078, China*

⁴*School of Resources and Safety Engineering, Central South University, Changsha 410012, Hunan, China*

Computer vision is being widely used today, but due to the inadequacies of computer vision systems, security issues have become a serious challenge. In this current study, a computer vision security model based on machine learning and artificial intelligence (AI) networks was constructed to improve the security and robustness of existing computer vision models, and provide effective solutions for computer vision problems in practical application scenarios. Moreover, the technology application of machine learning and AI network in the construction of computer vision security model was analysed to build a computer vision security model with four parts: data acquisition, data pre-processing, network construction and model training. Three real-life cases were selected for experimental analysis to verify the advantages of the proposed model. The accuracy, precision and recall of 100 facial samples using a computer vision security model constructed using machine learning and AI network technology were compared with those using traditional computer vision security models. According to the results, the accuracy, precision and recall of the proposed computer vision security model improved by 18%, 16% and about 18.2%, respectively. These findings indicate that the computer vision security model based on machine learning and AI networks constructed in this paper offers significant advantages in terms of object detection and good performance. The proposed model is of great relevance for the current security issues facing computer vision systems, providing new ideas and methods for research and practice in computer vision security.

Keywords: machine learning, artificial intelligence network, face recognition, computer vision security model, model construction

1. INTRODUCTION

Today, digital video and images are collected and used more widely in all walks of life, such as video surveillance systems, autonomous vehicles and social media. With the emergence of a large amount of visual data, how to analyse these data effectively, quickly and automatically has become a major challenge. To address these needs, the building of a computer

vision security model is particularly important. Building a computer vision security model by collecting relevant data in this field has become an important direction of current research and application.

With the development and maturity of computer technology, the development of computer vision technology has also received the attention of many scholars. Zhao believed that in recent years, computer vision has seen an amazing growth, which is driven mainly by the progress made in the field of convolutional neural networks, and focused on the application of machine vision methods to network security

*Corresponding author. Email: ^ainan66@126.com, ^btl@wdu.edu.cn, ^cA24091100226@cityu.edu.mo, ^dLiuzituo618@gmail.com

to detect attacks or devise security solutions [1]. Sood introduced various technologies based on computer vision and machine learning, and comprehensively reviewed food safety using computer vision and statistical methods to meet people's needs for healthy foods [2]. Yang believed the accurate, safe detection of blast furnace bearings to ensure equipment safety is a great challenge, and he proposed a computer vision technology based on sensor data and a hybrid deep learning method as a solution [3]. Arabi analysed a computer vision solution for engineering vehicle detection based on deep learning, which improved the accuracy of vehicle detection [4]. Abbas believed vehicle detection is an important function in the design of an intelligent transportation system, and he used computer vision to review vehicle detection comprehensively, emphasized the advantages and disadvantages of existing technologies, and made a valuable contribution to the field of vehicle detection [5]. Computer vision technology has great advantages in security detection, but it is not yet technologically mature, and further analysis of computer vision security detection needs to be conducted using new technologies.

With the development of computer vision, it is gradually being integrated with other fields and disciplines to leverage its unique advantages. Many experts have analysed the integration of machine learning. Wiley found that computer vision security has been integrated with many disciplines and fields. He reviewed the latest technologies and theoretical concepts of computer vision security, and explained the development of computer vision, especially the use related to image processing [6]. Sadeghi believed machine learning has achieved great success in many computer vision and language processing applications, but it is extremely susceptible to adversarial attacks. He applied machine learning to classification in wireless signals and proposed practical methods for creating white box and universal black box adversarial attacks in applications [7]. Yadav proposed an efficient method using machine learning and computer vision to focus on automatic monitoring of personnel to detect safe social distance and mask wearing in public places to create a safe environment that contributes to public safety [8]. Machine learning has many applications in computer vision, but it has not yet been analysed in helping computer vision build security models.

Artificial intelligence (AI) is an indispensable technology in modern intelligence development, and its combination with various fields has shown its unique advantages. The perspective of its combination with computer vision has attracted some scholars' analysis. Hansen believed the accurate marking of source data is still the rate limiting step of such projects, which is a difficult, inefficient and time-consuming process. He explained the new AI driver software greatly reduced the time required for marking in computer vision security [9]. Sharab believed availability is one of the three main goals of information security. He utilized an AI-based computer vision system with multi-objective functionality to achieve video communication, adapting video live streaming to limited network bandwidth and limited power, thereby helping improve system availability [10]. Singh believed virtual fences have certain effects on monitoring people, vehicles and their movements. He proposed a computer-

vision-based virtual fence security system based on AI, which improved the security performance of computer vision [11–12]. In response to various problems, the performance of computer vision systems utilizing AI technology has been improved in various respects, but its use for the construction of security models has not yet been addressed.

This paper aims to construct a computer vision security model that adapts to network changes based on machine learning and AI networks. By utilizing machine learning and AI methods, adaptive security models can be generated and effectively respond to network changes. This model greatly improves the security and efficiency of the computer vision field, and is of great relevance for research and application in related fields.

2. BUILDING MODELS FOR COMPUTER VISION SECURITY

2.1 Methods for Building Computer Vision Security Model

2.1.1 Machine Learning

Computer vision, as an important field of AI, focuses on how to make machines 'see' and understand the surrounding environment, which has importance in many applications [13]. Solving these problems often involves many complex mathematical and statistical models, and the emergence of machine learning, especially deep learning technology, has greatly advanced the development of this field.

In this paper, the main challenge of computer vision is how to extract meaningful features from a large amount of unordered pixel information. Traditional computer vision methods rely on manually defined feature extraction algorithms, but this method cannot cover all possible scenarios. Machine learning can automatically extract high-level features by using its parameters to learn the distribution and structure of data, greatly improving the performance of computer vision tasks.

In the field of security, the demand for building computer vision security models is becoming increasingly prominent [14–15]. In the field of public safety, the monitoring of large-scale surveillance videos in real-time is necessary to identify suspicious behaviours or items. In the field of biometric recognition, identifying fingerprints, faces or irises is necessary for identity verification or permission control. These tasks require processing a large amount of visual data and extracting meaningful information from them. Machine learning provides effective tools for this, as shown in Figure 1.

Figure 1 shows the specific process of machine learning application in building a computer vision security model. Firstly, a large amount of data on the website is pre-processed. A large amount of data information is on the website, which includes various forms of information such as text, language and images. The information is filtered and processed to select the required data information, followed by the data detection of the pre-processed information. The main

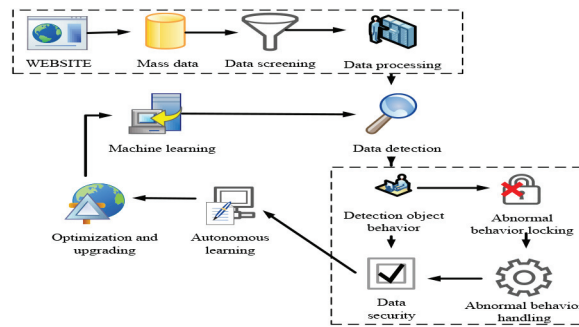


Figure 1 Application of machine learning in building a computer vision security model.

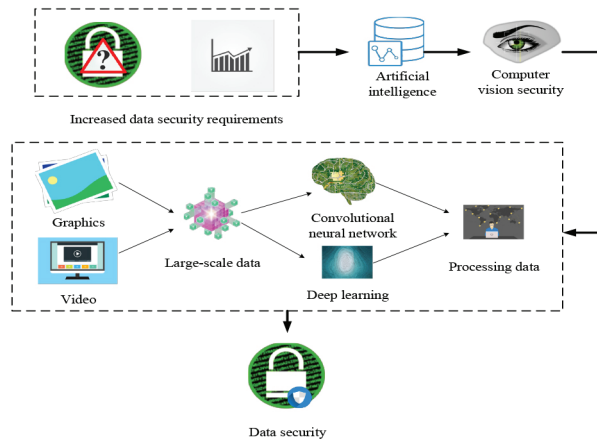


Figure 2 Constructing a computer vision security model using artificial intelligence network technology.

purpose of this paper is to maintain the security of computer vision, so identifying abnormal behaviour of the detected object is necessary. The detection results are examined for abnormal behaviour in the detection object, and the solution for abnormal behaviour is to lock the detection object and process the abnormal behaviour to convert it into safe data. Secondly, the detected object is classified as a data security situation if no abnormal behaviour is perceived. Then, the methods and processes for handling abnormal behaviours are analysed, and better solutions are sought for self-learning to handle abnormal behaviours better and ensure the security of computer vision. Through self-learning, machine learning techniques are continuously optimized and upgraded through self-learning.

In summary, using machine learning to construct a computer vision security model is of great relevance for achieving automated, efficient monitoring and preventing security risks. The application of machine learning to construct a computer vision security model can greatly improve the performance and efficiency of modern security protection systems, ensuring the safety of people's lives and property.

2.1.2 Artificial Intelligence Network

In today's information society, the application of computer vision has become increasingly widespread [16]. Traditional computer vision methods often rely on manually-designed feature extraction and classification algorithms, making it difficult to handle large-scale, complex visual tasks. With the development of AI and deep learning technology,

especially the emergence of convolutional neural networks, new possible solutions to these problems have emerged. By using large-scale datasets for training, deep learning models can automatically learn and extract features with high representativeness, and perform complex pattern recognition and classification through network hierarchy, as shown in Figure 2.

Figure 2 shows AI network technology is utilised in this paper to construct a computer vision security model. Firstly, the purpose of constructing a computer vision security model is determined. With the increasing attention to security and privacy in society, the demand for effective computer vision security models is also increasing. This model can be used for face recognition door security, abnormal behaviour detection and image malicious attack detection to improve security and protect personal and public security. Secondly, through AI technology, image and video data in computer vision systems are collected and stored, providing sufficient data resources for training neural networks with complex pattern recognition capabilities. In addition, large-scale data are processed by convolutional neural network and deep learning algorithm to ensure the safety of data. Taking face image acquisition as an example, the specific image data collection is shown in Figure 3.

In Figure 3, the left side shows an example of a portrait that collects facial information, and on the right side, part *a* shows the facial information collected by the eyes of the portrait in open and closed states, whereas parts *b* and *c* show the facial information collected by the facial expressions of the portrait in states with and without expression. By

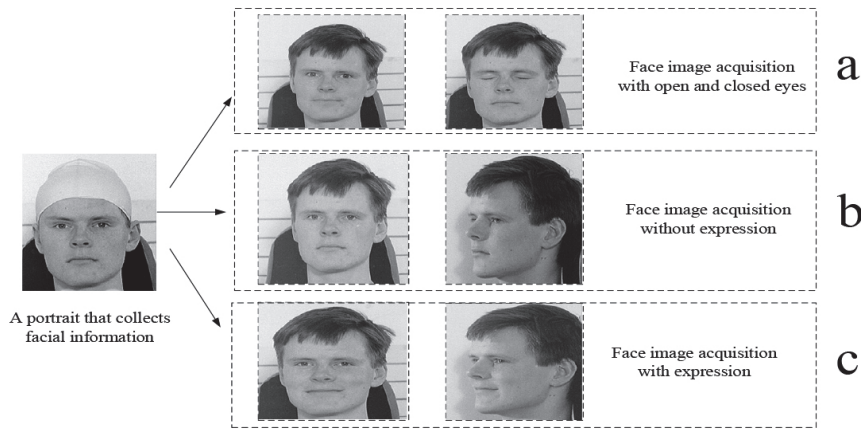


Figure 3 Information collection diagram of facial recognition image data.

collecting information from multiple directions, angles and states of the face, the accuracy of face recognition can be enhanced, and the occurrence of security risks caused by incorrect recognition can be avoided.

In summary, the construction of a computer vision security model aims to provide more powerful, efficient and accurate security solutions for computer vision systems using AI network technology [17].

2.2 Role of Building Computer Vision Security Model

Security models play a crucial role in data protection. The application of security models can effectively protect the privacy and integrity of data, providing reliable access control mechanisms for data.

Firstly, the security model can protect the privacy of data through authentication and permission management. By verifying the user's identity and assigning corresponding permissions to them, the security model ensures that only authorized users can access sensitive data.

Secondly, the security model can ensure the integrity and confidentiality of data through encryption technology. Data may be threatened by hacker attacks or malicious tampering during transmission and storage. The application of security models can encrypt data, making them unreadable during transmission and storage, thereby preventing unauthorized personnel from tampering with the data.

In addition, security models can provide effective access control to data through anomaly detection and behaviour analysis. By establishing a model and analysing user behaviour, the security model can identify abnormal behaviour and take corresponding measures. The application of this security model can timely identify potential data security threats and respond to them.

Through authentication and permission management, encryption technology as well as anomaly detection and behaviour analysis, security models can effectively protect the privacy and integrity of data, providing reliable access control mechanisms for data. Strengthening the application and research of security models in data protection is of great importance in the face of increasing data security threats.

2.3 Process of Building Computer Vision Security Model

2.3.1 Data Acquisition

Data acquisition is the foundation of model construction and requires collecting a large amount of data for training. Two datasets are common in the field of computer vision security: the Canadian Institute for Advanced Research (10 CIFAR-10) dataset and the Mixed National Institute of Standards and Technology (MNIST) dataset. Both datasets can obtain the required data through web crawling methods.

2.3.1.1 MNIST Dataset The MNIST dataset is a large handwritten digit database often used to train various image processing systems. The MNIST dataset contains 60000 training samples and 10000 test samples. Each sample is a 28*28-pixel grayscale handwritten digital image with a corresponding label. These numbers have undergone normalization and centralization processing. The role of the MNIST dataset is manifested in the following aspects. The first is in terms of benchmark testing. Due to the moderate size and publicly available MNIST dataset, it is often used as a benchmark for new algorithms and models. The second aspect is the introductory research on machine learning and deep learning.

2.3.1.2 CIFAR-10 Dataset The CIFAR-10 dataset is a common computer vision dataset. The '10' in its name refers to the number of categories contained in the dataset. The CIFAR-10 dataset is mainly used for the recognition of multi-category objects, and it is widely used for the benchmark test of computer vision, such as image classification, object detection and other tasks, as shown in Figure 4.

Figure 4 is a graphical representation of the testing method for the CIFAR-10 dataset. The CIFAR-10 dataset contains 60000 32*32-pixel colour images, of which 50000 are training sets and 10000 are testing sets. These images are divided into 10 categories, namely, aircraft, cars, birds, cats, deer, dogs, frogs, horses, ships and trucks, each with 6000 images.

The CIFAR-10 dataset has a wide range of applications and important roles in the field of computer vision. Firstly,

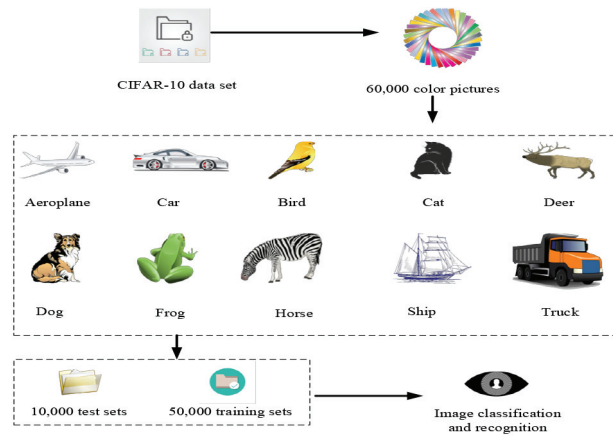


Figure 4 Graphical representation of the testing method for the CIFAR-10 dataset.

in terms of algorithm evaluation and comparison, because the CIFAR-10 dataset contains multiple types of images and has training and testing sets, it is often used for algorithm evaluation and comparison.

2.3.2 Data Training

With the development of technology, computer vision and AI have increasingly become important tools in the field of security [18]. Whether surveillance cameras in the field of public safety or facial unlocking functions on personal devices, a large amount of visual data needs to be processed and analysed. Computer vision security also faces many challenges, so the training and optimizing of models is particularly important. Moreover, data training for computer vision security can accurately identify and predict various security issues, thereby achieving prevention and early detection. For the safety of public places, computer vision can identify individuals with abnormal behaviour. For the security of personal devices, computer vision can recognise user identity and prevent unauthorized access. Therefore, computer vision security data training is of great importance for improving the security level of society and individuals. The following are the specific methods used for training data.

2.3.2.1 Data Pre-Processing The collected data needs to be pre-processed using methods including data cleansing, data format conversion, data normalization and other steps. Amongst them, data normalization is the most used pre-processing method because different data may have dissimilar scales and distributions. If data are not normalized, the accuracy of the model may be compromised.

2.3.2.2 Data Cleansing Data cleansing includes null value processing, outlier processing, format consistency, string processing, repeated value processing and other cleaning methods. The specific method depends on the characteristics of the data and the goal of data cleansing. The identification of abnormal data is explained in this paper. The quartile formula for outlier processing is used to determine the distribution of data and whether there are outliers in the data.

Calculating the lower quartile Q_1 : For a data set with n observations, the lower quartile is the value of the 25%

digit m after all observations are sorted in ascending order, as follows:

$$Q_1 = (n + 1) * m \quad (1)$$

If m is not an integer, interpolation is required.

The upper quartile Q_2 is calculated as follows:

$$Q_2 = (n + 1) * 0.75 \quad (2)$$

The interquartile range Q_3 is calculated as follows:

$$Q_3 = Q_2 - Q_1 \quad (3)$$

Determining outlier: Generally, if a data point is less than $Q_1 - 1.5Q_3$ or greater than $Q_2 + 1.5Q_3$, it is considered an outlier. The '1.5' can be properly adjusted as needed. The larger the value is, the higher the tolerance for outliers. On the contrary, it is stricter. The common adjustment ratio is 1.5 or 3.

2.3.2.3 Data Conversion Data conversion is an important component of data pre-processing, which is of great importance for further data analysis and training of computer vision security models. Firstly, it is necessary to improve data compatibility. The conversion of data formats can ensure the smooth transmission of data between different systems and applications, and can be correctly parsed by the receiving party. Secondly, to adapt the data to the needs of analysis or modelling, many machine learning algorithms require data to be input in a specific format. This enhances data quality and certain data format conversion operations can help improve the quality of the data. For example, the cleaning and formatting of data can eliminate unnecessary spaces, correct spelling errors and unify data formats. Then, data compression converts the data format in some way to compress and save the data, reducing storage space.

2.3.2.4 Linear Normalization Linear normalization is a common data pre-processing method. Its purpose is to scale a group of original data to a specific interval, usually $[0, 1]$ interval or $[-1, 1]$ interval. The linear normalization formula is as follows:

$$x^c = \frac{x - \min(x)}{\max(x) - \min(x)} \quad (4)$$

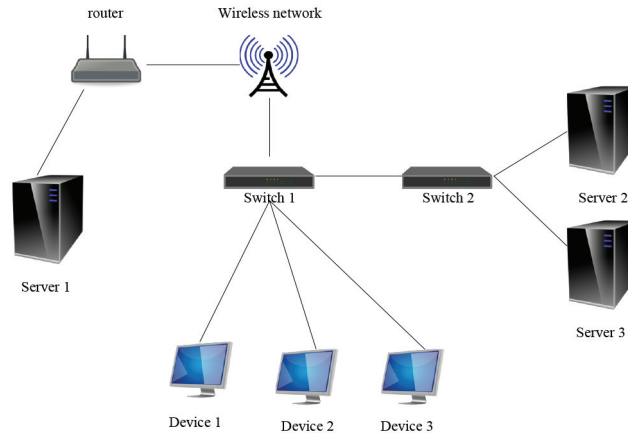


Figure 5 Network of computer vision security model based on machine learning and artificial intelligence network technology.

where x^c represents the normalized data, and x represents the original data. $\min(x)$ and $\max(x)$ represent the minimum and maximum values of the original data, respectively.

The main advantage of linear normalization is that the original data of different scales or units can be converted to the same scale for comparison or further data processing. However, linear normalization has limitations. When the new data exceed the maximum or minimum value of the original data, they need to be normalized again.

2.3.3 Network Construction

Security models, as an important means of protection, are widely used in the field of network security. These models are based on machine learning and AI networks, which can help identify and respond to various network threats, and improve network security and reliability, as shown in Figure 5.

Figure 5 shows the network comprising routers, wireless networks, servers, switches and devices, making it of great importance to the construction of a computer vision security network. Firstly, the security model can detect and prevent network attacks by analysing network traffic and behaviour patterns. Secondly, the security model can establish a multilevel network defence system. By utilizing machine learning and AI technologies to deploy multiple defence nodes in the network, each node is responsible for monitoring and defending against specific types of attacks. The security models can also be used for automated network protection and response. Based on machine learning and AI algorithms, an intelligent security model can be trained, which can continuously learn and adapt to constantly changing network threats.

In summary, the application of security models in network protection is diverse and extensive. By constructing models based on machine learning and AI networks, network security can be better protected. Network attacks can be identified and prevented, and reliable, stable operation of the network can be achieved.

2.3.4 Data Protection

This study focuses on the protection of data and uses the Rivest Shamir Adleman asymmetric encryption algorithm to

encrypt the data. A public key is used to encrypt the data, which can only be decrypted when the user holds the private key, greatly protecting the security of the data. The specific algorithm formulas are as follows:

$$n = p * q \quad (5)$$

$$\phi(n) = (p - 1) * (q - 1) \quad (6)$$

$$ed = 1 \mod \phi(n) \quad (7)$$

$$c = m * e \mod n \quad (8)$$

$$m = c * d \mod n \quad (9)$$

As shown in Formulas (5)–(9), e and n are public, and p , q and d are confidential. p and q are two large prime numbers, and e is the public key. n is the product of two large prime numbers, and m and c are plaintext and ciphertext, respectively.

Data protection measures protect the private information of individuals or organizations, preventing such information from being accessed, leaked, damaged or lost by unauthorized persons or entities. Therefore, it plays an important role in the construction of a computer vision security model in this paper.

2.3.5 Model Training

Model training is the most critical and complex step in building computer vision security models, typically using algorithms such as support vector machines (SVM) for model training. SVM first needs to partition the plane where the sample data set is located according to the plane partition formula. This partition can obtain a decision boundary with the largest sample data set interval [19], as shown in Formula (10).

$$Y = W_T x + b \quad (10)$$

where W_T represents the weight of the sample, and b represents the bias vector. Then, the distance from any data of the sample data set in the hyperplane to the hyperplane is calculated, as shown in Formula (11).

$$R = \frac{\|W_T x + b\|}{\|w\|} \quad (11)$$

Then, the Lagrange multiplier method is used to obtain the sum of the distances between the data in two different types

Table 1 Analysis results of the effectiveness of the computer vision security model.

	Number of experiments	Accuracy of abnormal data identification	Accuracy of face recognition	Average accuracy
The computer vision security model constructed in this paper	1	97%	99%	98.3%
	2	98%	100%	
	3	97%	99%	

of sample data sets and the hyperplane, as shown in Formula (12).

$$L = f(x) + \sum_{i=1}^n a_i g(x) + \sum_{j=1}^m b_j h(x) \quad (12)$$

where w and b in the above operations are subjected to partial differentiation operations, as shown in Formulas (13) and (14).

$$w = \sum_{i=1}^m a_i y_i x \quad (13)$$

$$b = \sum_{i=1}^m a_i y \quad (14)$$

With the above operation, whether the position of the input sample data is on the boundary of the maximum interval of the Hyperplane can be ascertained to determine whether the data set is a support vector.

2.3.6 Model Effect

After constructing a computer vision security model using machine learning and AI network technology, the effectiveness of the model needed to be verified. Taking the security camera of a certain company as the experimental object, different amounts of abnormal data were input three times into the security system, and facial recognition tests were conducted on five randomly-selected company employees and five noncompany employees [20–21]. Abnormal data and facial recognition data were recorded separately, and the accuracy was calculated, as shown in Table 1.

Table 1 shows that the accuracy of abnormal data recognition and facial recognition obtained by running three tests was above 95%. After calculation, the average accuracy of the computer vision security model constructed in this paper was about 98.3%, which showed the recognition effect of the proposed computer security model was good, and the effect of the practical application of the model needed to be determined through specific cases.

3. CASES AND EXPERIMENTS ON COMPUTER VISION SECURITY

3.1 Cases

Machine learning and AI networks are widely used in the construction and analysis of security models in computer vision. This section explores the application of computer vision through several case studies.

Firstly, a deep-learning-based face recognition security model is introduced. The model uses the deep convolutional neural network to learn the facial feature representation and is trained through the training data set. The security model performs well in face recognition tasks, accurately identifying faces and recognizing possible spoofing. This security model based on machine learning and AI networks not only improves the accuracy of facial recognition systems, but also strengthens the system's security and resistance to attack.

Secondly, the security model for abnormal behaviour detection based on machine learning is explored. This model learns the feature representations of normal behaviour by training the normal behaviour patterns in the dataset and detects possible abnormal behaviour based on these feature representations.

3.2 Facial Recognition Experiment

In this paper, 50 of the 100 employees were randomly selected as experimental subjects, and then 50 noncompany personnel were randomly chosen as control subjects. To ensure the accuracy of the experiment, company employees and noncompany personnel were mixed, and computer vision security models were used to perform five rounds of identification on 100 individuals with 10 times per round. The experimental results were recorded, and the experimental data were analysed, as shown in Figure 6.

Figure 6 shows the data statistics of a company's security camera for the facial recognition of employees and noncompany personnel. Figure 6A shows the number of people who correctly recognized the faces of company employees and noncompany personnel. The number of people who correctly recognized faces in the five rounds of recognition was over 94, indicating that more people correctly recognized faces, and the recognition accuracy was high. Figure 6B shows the number of people (below 6) who mistakenly recognized faces as being those of company employees and noncompany personnel. This suggests that the company's security camera had a higher accuracy in facial recognition after using the established model to train the data. Figure 6C shows the number of correctly identified employees and noncompany personnel in the first round. Not much difference was noted in the number of people who could correctly recognize the faces of company employees and noncompany personnel, indicating the model was more accurate in classifying faces. Figure 6D shows the number of people who mistakenly identified company employees and noncompany personnel in the first round. The number of facial recognition errors for company employees and noncompany personnel were

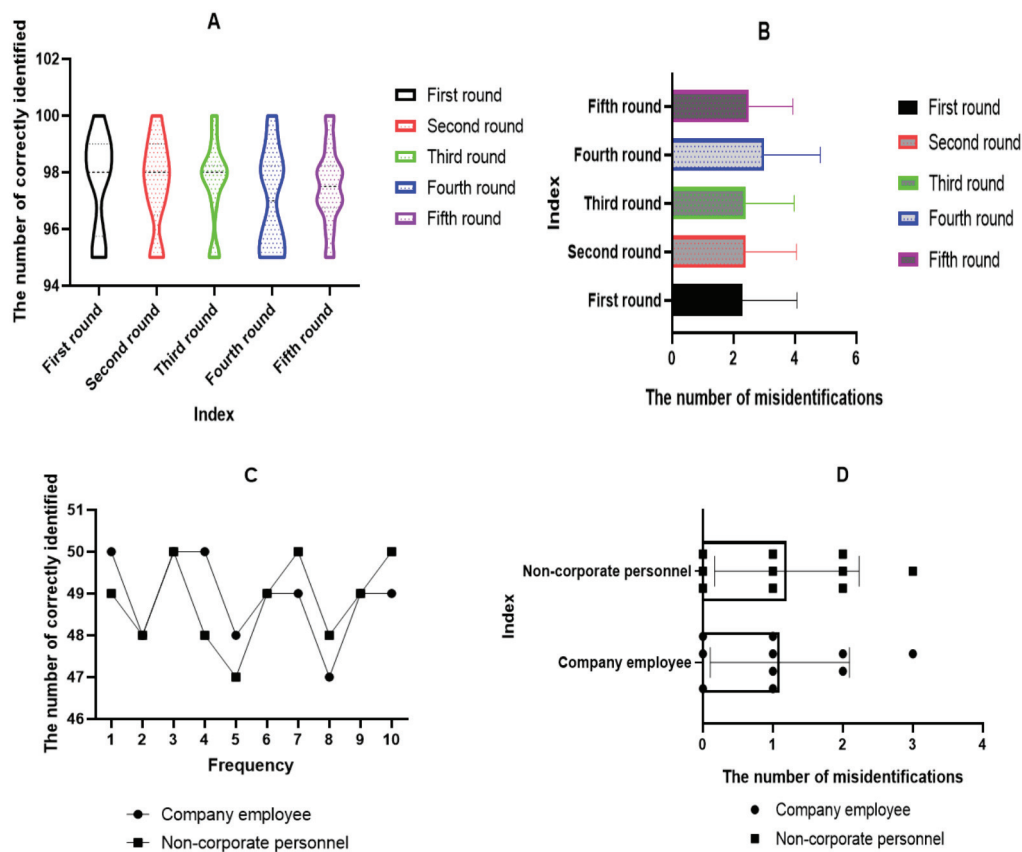


Figure 6 Statistics for facial recognition of company employees and noncompany personnel. (A) Number of people who correctly identified the faces of company employees and noncompany personnel. (B) Number of people who mistakenly recognized the faces of company employees and noncompany personnel. (C) Number of correctly identified employees and noncompany personnel in the first round. (D) Number of misidentified employees and noncompany personnel in the first round.

Table 2 Statistics for abnormal data detection results.

	Total number of detected data	Number of abnormal data	Number of abnormal data detected	Accuracy of detection	Average accuracy of the detection
First time	100	10	9	90%	95.95%
Second time	200	20	19	95%	
Third time	300	30	27	90%	
Fourth time	400	40	38	95%	
Fifth time	500	50	49	98%	
Sixth time	600	60	57	95%	
Seventh time	700	70	70	100%	
Eighth time	800	80	78	97.5%	
Ninth time	900	90	90	100%	
Tenth time	1000	100	99	99%	

similar, and the number was relatively small, indicating that the model can accurately recognize faces.

3.3 Abnormal Data Detection

In this paper, a computer from a company was taken as the experimental object. After establishing a model in this paper, real-time detection was carried out on the computer of company personnel, and a large amount of data was pre-processed, followed by network construction and model training. Then, a relatively complete computer vision security model was constructed. However, the accuracy of the

anomaly data detection in this model needed to be verified. Furthermore, the detection accuracy must be qualified and meet the company's requirements before it can be applied to actual production environments. Every hour, an indefinite number of attacks was launched on the company's computer. The experiment lasted for 10 hours and attacks were launched once every hour. The attacks were sequentially recorded as the first, second, third, fourth, fifth, sixth, seventh, eighth, ninth and tenth attacks. Every hour, 100 data and 10 abnormal data were added, as shown in Table 2.

Table 2 shows that the accuracy rates of 10 abnormal data detections were 90%, 95%, 90%, 95%, 98%, 95%, 100%, 97.5%, 100% and 99%, and they were all 90%

Table 3 Data statistics of computer vision security model based on machine learning and artificial intelligence networks for image detection.

Confusion matrix	Detected as containing the faces of company employees	Detected as not including the faces of company employees
Actually contains the faces of company employees	48 (TP)	2 (FP)
Does not actually contain the faces of company employees	4 (FN)	46 (TN)

Table 4 Data display after identifying action samples based on traditional action recognition algorithm models.

Confusion matrix	Detected as containing the faces of company employees	Detected as not including the faces of company employees
Actually contains the faces of company employees	40 (TP)	10 (FP)
Does not actually contain the faces of company employees	14 (FN)	36 (TN)

or above. The average accuracy rate of 10 abnormal data detections was 95.95%, indicating the computer vision security model constructed using machine learning and AI network technology had a high accuracy rate for abnormal data detection and can effectively maintain network security.

4. PERFORMANCE TESTING OF COMPUTER VISION SECURITY MODELS

In this paper, the performance of computer vision security models constructed was tested based on machine learning and AI networks. The evaluation indicators for model performance testing were: accuracy, precision and recall. The computer vision security model of a company's facial detection was used as the experimental object, and the accuracy, precision and recall of the facial recognition of the computer vision security model before and after using machine learning and AI network technology were analysed. In the detection experiment, 100 face samples were selected for the security model to detect. Of these 100 image samples, 50 samples contained the faces of company employees, and 50 did not. The classification result of this model recognition is shown in Table 3.

The formula for the accuracy rate of face detection G is:

$$G = \frac{TP + TN}{TP + TN + FP + FN} \times 100\% \quad (15)$$

where TP represents the actual number of face samples containing the faces of company employees. Combined with the computer vision security model constructed in this paper, the number of samples containing the faces of company employees was detected. FN indicates the facial samples that do not actually contain the faces of company employees, while the proposed computer vision security model can detect the number of samples containing the faces of company employees. FP represents the actual number of samples that do not include the faces of company employees; however,

the proposed computer vision security model detects the number of samples that do not include the faces of company employees. TN represents the actual number of samples that do not include the faces of company employees, and the proposed computer vision security model detects the number of samples that do not include the faces of company employees. Therefore, by combining Formula (15) with the data in Table 3, the computer vision security model constructed in this paper had an accuracy of 94% for face detection.

The formula with a precision rate of A for facial detection is analysed, and its formula is as follows:

$$A = \frac{TP}{TP + FP} \times 100\% \quad (16)$$

By combining Formula (16) with the data in Table 3, the computer vision security model constructed in this paper had a precision of 96% for face detection.

The recall rate of R for the computer vision security model is calculated with:

$$R = \frac{TP}{TP + FN} \times 100\% \quad (17)$$

According to the result obtained with Formula (17) and the data in Table 3, the recall rate of the computer vision security model constructed for face detection in this paper can be calculated, with a recall rate of approximately 92.3%.

Subsequently, the face detection performance of computer vision security models without utilizing machine learning and AI networks was analysed, and the same 100 face samples were used for detection. The data display is shown in Table 4.

For determining the accuracy rate of face detection G_1 the formula is:

$$G_1 = \frac{40 + 36}{40 + 36 + 10 + 14} \times 100\% \quad (18)$$

According to the result obtained with Formula (18), the accuracy of traditional computer vision security models for face detection was 76%.

The formula for calculating the precision rate of facial detection A_1 is:

$$A_1 = \frac{40}{40 + 10} \times 100\% \quad (19)$$

Formula (19) shows that the precision of traditional computer vision security models for face detection is 80%.

The recall rate R_1 of the computer vision security model constructed in combination with this paper is calculated as follows:

$$R_1 = \frac{40}{40 + 14} \times 100\% \quad (20)$$

The recall rate of traditional computer vision security models for face detection was calculated with Formula (20), and the recall rate was approximately 74.1%.

In this paper, the application of machine learning and AI networks in computer vision security models and traditional computer vision security models, the accuracy, precision and recall of 100 facial samples for facial detection of company employees were compared. According to the calculation results, the accuracy, precision and recall of the computer vision security model constructed in this paper improved by 18%, 16% and by about 18.2%, respectively.

5. CONCLUSIONS

Computer vision security is of great importance in the modern information environment, and the development of machine learning and AI network technology provides new solutions for such security. In this paper, the computer vision security model constructed based on machine learning and AI network technology shows great potential in practical applications. By utilizing computer vision security models, the security, accuracy and attack resistance of computer vision systems can be improved, providing strong support and guaranteeing the security of residents' data and information. In the future, further research and development of these security models can further the development and innovation of computer vision security.

ACKNOWLEDGEMENTS

This work was supported by Teaching Research Project: "Construction and Research on the Ideological and Political Education System in Computer Science Courses under the 'Party Building +' Model".

REFERENCES

1. Zhao, J. W., Rahat, M., Suranga, S. A review of computer vision methods in network security. *IEEE Communications Surveys & Tutorials*, 2021, vol. 23, no. 3, p. 1838–1878. DOI: 10.1109/COMST.2021.3086475
2. Sood, Shivani, Harjeet, S. Computer vision and machine learning based approaches for food security: A review. *Multimedia Tools and Applications*, 2021, vol. 80, no. 18, p. 27973–27999. DOI: 10.1007/s11042-021-11036-2
3. Yang, Ai, M., Zhi, J.M., Yang, K., Jia-Hao, Wang, T. X. Computer vision technology based on sensor data and hybrid deep learning for security detection of blast furnace bearing. *IEEE Sensors Journal*, 2021, vol. 21, no. 22, p. 24982–24992. DOI: 10.1109/JSEN.2021.3077468
4. Arabi, Saeed, Arya, H., Anuj, S. A deep-learning-based computer vision solution for construction vehicle detection. *Computer-Aided Civil and Infrastructure Engineering*, 2020, vol. 357, p. 753–767. DOI: 10.1111/mice.12530
5. Abbas, Aymen, F., Usman, U.S., Fahad, T. A. D., Mohd, N. H. A comprehensive review of vehicle detection using computer vision. *TELKOMNIKA (Telecommunication Computing Electronics and Control)*, 2021, vol. 19, no. 3, p. 838–850. DOI: 10.12928/telkomnika.v19i3.12880
6. Wiley, Victor, Thomas, L. Computer vision and image processing: a paper review. *International Journal of Artificial Intelligence Research*, 2018, vol. 2, no. 1, p. 29–36. DOI: 10.29099/ijair.v2i1.42
7. Sadeghi, Meysam, Erik, G. L. Adversarial attacks on deep-learning based radio signal classification. *IEEE Wireless Communications Letters*, 2018, vol. 8, no. 1, p. 213–216. DOI: 10.1109/LWC.2018.2867459
8. Yadav, Shashi. Deep learning based safe social distancing and face mask detection in public areas for covid-19 safety guidelines adherence. *International Journal for Research in Applied Science and Engineering Technology*, 2020, vol. 8, no. 7, p. 1368–1375. DOI: 10.22214/ijraset.2020.30560
9. Hansen, Ulrik, S., Eric, L., Mehul, P., Hayee, B. H. Novel artificial intelligence-driven software significantly shortens the time required for annotation in computer vision projects. *Endoscopy International Open*, 2021, vol. 9, no. 04, p. E621–E626. DOI: 10.1055/a-1341-0689
10. Sharrab, Yousef, O., Izzat, A., Nabil, J. S. Towards the availability of video communication in artificial intelligence-based computer vision systems utilizing a multi-objective function. *Cluster Computing*, 2022, vol. 25, no. 1, p. 231–247. DOI: 10.1007/s10586-021-03391-4
11. Singh, Anuj, Tanmay, A., Namrata, P. Artificial Intelligence Based Computer Vision for Virtual Fencing Security System. *Elementary Education Online*, 2022, vol. 20, no. 4, p. 3903–3903. DOI: 10.17051/ilkonline.2021.04.426
12. Liu, Y., He, W., Zhu, J., Yang, R., Yang, X. Intelligent Decision-Making System for Power Grid Dispatching Based on Generative AI. *Engineering Intelligent Systems*, 2026, vol. 34, no. 1, p. 5–16.
13. Zeng, X., Wang, Z., Hu, Y. Enabling Efficient Deep Convolutional Neural Network-based Sensor Fusion for Autonomous Driving. *arXiv preprint arXiv*, 2022, vol. 22, no. 02, p. 11231. DOI: 10.1145/3489517.3530444
14. Suma, D. V. Computer vision for human-machine interaction-review. *Journal of Trends in Computer Science and Smart Technology*, 2019, vol. 1, no. 2, p. 131–139. DOI: 10.36548/jtc-sst.2019.2.006
15. Zhang, T. Discourse Strategies of Artificial Intelligence in Cross-Cultural Business Communication. *Engineering Intelligent Systems*, 2026, vol. 34, no. 1, p. 601–71.
16. Cho, Brian, H., Deepak, K., Zoe, B., Cheung, I., Ye, B., Tang, R., Amy, A. Automated measurement of lumbar lordosis on radiographs using machine learning and computer vision. *Global spine journal*, 2020, vol. 10, no. 5, p. 611–618. DOI: 10.1177/2192568219868190
17. Tian, H. K., Wang, T. H., Liu, Y. D., Qiao, X., Li, Y. Z. Computer vision technology in agricultural automation—A review. *Information Processing in Agriculture*, 2020, vol. 7, no. 1, p. 1–19. DOI: 10.1016/j.inpa.2019.09.006

18. Chen, Joy, I. Z., Chang, J. T. Applying a 6-axis mechanical arm combine with computer vision to the research of object recognition in plane inspection. *Journal of Artificial Intelligence and Capsule Networks*, 2020, vol. 2, no. 2, p. 77–99. DOI: 10.36548/jaen.2020.2.002
19. Hawkins, M. Metaverse live shopping analytics: retail data measurement tools, computer vision and deep learning algorithms, and decision intelligence and modeling. *Journal of Self-Governance and Management Economics*, 2020, vol. 10, no. 2, p. 22–36. DOI: 10.22381/jsme10220222
20. Yu, H. Trajectory Tracking Control Method for Flexible Robot of Construction Machinery Based on Computer Vision. *Kinetic Mechanical Engineering*, 2023, Vol. 4, no. 1, p. 20–29. DOI: 10.38007/KME.2023.040103
21. Bissan, Ghaddar, Joe, N. S. High dimensional data classification and feature selection using support vector machines. *European Journal of Operational Research*, 2018, vol. 265, no. 3, p. 993–1004. DOI: 10.38007/KME.2023.040103

