Hindawi
Security and Communication Networks
Volume 2021, Article ID 1224333, 10 pages
https://doi.org/10.1155/2021/1224333

Research Article

Security Analysis of Intelligent System Based on Edge Computing

Yibo Han,[1] Weiwei Zhang,[2] and Zheng Zhang[3]

[1]*Nanyang Institute of Big Data Research, Nanyang Institute of Technology, Nanyang, Henan 473000, China*
[2]*Nanyang Fangyuan Limited Liability Accountant Firm, Nanyang, Henan 473000, China*
[3]*School of Computer and Software, Nanyang Institute of Technology, Nanyang, Henan 473000, China*

Correspondence should be addressed to Zheng Zhang; zhangzheng@nyist.edu.cn

Received 1 June 2021; Revised 1 July 2021; Accepted 31 July 2021; Published 18 August 2021

Academic Editor: Shahram Babaie

At present, artificial intelligence technology is widely used in society, and various intelligent systems emerge as the times require. Due to the uniqueness of biometrics, most intelligent systems use biometric-based recognition technology, among which face recognition is the most widely used. To improve the security of intelligent system, this paper proposes a face authentication system based on edge computing and innovatively extracts the features of face image by convolution neural network, verifies the face by cosine similarity, and introduces a user privacy protection scheme based on secure nearest neighbor algorithm and secret sharing homomorphism technology. The results show that when the threshold is 0.51, the correct rate of face verification reaches 92.46%, which is far higher than the recognition strength of human eyes. In face recognition time consumption and recognition accuracy, the encryption scheme is basically consistent with the recognition time consumption in plaintext state. It can be seen that the security of the intelligent system with this scheme can be significantly improved. This research provides a certain reference value for the research on the ways to improve the security of intelligent system.

1. Introduction

With the rapid development of mobile network, multimedia data on network edge devices are increasing rapidly. The network communication load and storage space of the traditional cloud computing intelligent system are impacted. With the improvement of the real-time requirements of the network, the edge computing arises at the historic moment [1]. Relevant research shows that as of October 30, 2020, 50% of multimedia data have been preprocessed, forwarded, stored, and other operations through the Internet edge [2, 3]. The cloud computing mode of centralized processing will fall into the demand of real-time and privacy protection that cannot complete the common processing of all programs, and edge computing has become a new direction of development [4]. Face recognition has the advantages of incompatibility, mobility, uniqueness, directness, and friendliness and has become the mainstream technology for user authentication in intelligent systems [5]. Face recognition technology mainly distinguishes different faces through the distinguishability of faces. Due to the openness of the Internet environment, the authentication system based on biometrics has a great risk of privacy leakage [6]. To improve the security of user identity authentication in intelligent system, an identity authentication scheme based on edge computing is proposed. The original face image is processed by convolution neural network, and the feature vector of face is extracted. The user identity registration technology based on secure nearest neighbor algorithm and the user identity authentication technology based on secret sharing homomorphism are introduced.

With the development of industrial Internet of things, the type and number of industrial equipment increase. Through established a noninvasive load monitoring system through recurrent neural network long-term memory and identified the power equipment through edge calculation. The research results show that the average random recognition rate of the system can reach 88% [6]. The mobile Internet of things can process a large amount of real-time data. To alleviate the contradiction between the resource constraints of mobile devices and the requirements of users to reduce processing delay and extend battery life, Huang

et al. and other scholars proposed a computing offload method for cloud edge computing supporting the Internet of things and solved the multiobjective optimization problem of task offload in cloud computing through nondominant sorting genetic algorithm III [7]. Researchers proposed that mobile edge computing and UAV base station have become a promising technology in the Internet of things and designed an online edge processing scheduling algorithm based on Lyapunov optimization. When the data rate is low, it tends to reduce the frequency of edge processor. When the data rate is high, it will flexibly allocate bandwidth for edge data unloading [8]. After investigating the development of artificial intelligence, edge computing, and the occurrence of big data, scientific team believe that when people extract intelligent information from Internet of things nodes, the user's information data are vulnerable to network attacks and information leakage, that is, the data richness and data analysis of intelligent management system form a great risk of infringement on the user's privacy [9]. With the development of intelligent transportation system, video analysis technology has become a potential technology to improve vehicle network security, but a large number of video data transmission brings great pressure to vehicle network. A video analysis framework is proposed, which integrates multiaccess edge computing and block chain technology into the Internet of things to optimize the transaction throughput of block chain system [10]. Researchers proposed a vehicle edge planner based on two-stage machine learning, to provide better driving service for drivers [11].

Face recognition is the main way for most intelligent systems to identify users, especially for intelligent monitoring systems. When the distance between monitoring and face is too far, the success and accuracy of capturing face are reduced. Therefore, Scholars use deep convolution neural network to improve the resolution of captured image and complete face feature extraction and classification [12]. In image recognition, the Science team applied hierarchical clustering technology to divide the database into some interrelated clusters and sort them and then compared the classification effect through deep convolution neural network [13]. A lightweight convolutional neural network structure is proposed, which uses smaller filter size and depth separable convolution to improve the nonlinear performance of the model and complete the mapping from the original low-resolution image to the high-resolution image [14]. Other researchers have successfully extracted the host's watermark image under various attacks by using the nonembedded blind image watermarking algorithm based on mapping residual convolution neural network [15]. Modern team proposed a distributed storage computing k-nearest neighbor algorithm for data processing in the Internet of things. By performing distributed computing on each storage node, the algorithm effectively performs k-nearest neighbor search and improves the speed of data processing [16]. Scholars have proposed an automatic license plate image recognition technology, which uses the boundary tracking method to segment the contour, and then uses the nearest neighbor algorithm to complete the image recognition, which has high security [17]. To solve the problem of encrypted traffic identification, some scholars proposed an encrypted network behavior identification method based on dynamic time warping and k-nearest neighbor [18].

To sum up, a lot of research has been carried out in edge computing, secure nearest neighbor algorithm, face recognition, intelligent system, user data privacy protection, and so on. However, in the aspect of improving the security of intelligent system, there is still a lack of research on using edge computing, convolutional neural network face feature extraction, and secure nearest neighbor algorithm to improve the security of face recognition. In view of this, this paper proposes an intelligent system security enhancement scheme based on edge computing, which uses convolution neural network to extract the feature vector of face image and uses secure nearest neighbor algorithm to protect the user privacy.

2. Research on Security Enhancement Technology of Intelligent System Based on Face Recognition

2.1. Face Feature Vector Extraction Based on CNN. Edge in edge computing refers to network devices with data storage capacity and data computing capacity, which are distributed between terminal data source and cloud server [19]. Edge computing is both the data owner and the data user, which also means that the data requests between cloud computing center and edge computing devices are bidirectional requests [20, 21]. At the same time, the data at the edge of edge computing is divided into uplink and downlink. Uplink refers to cloud computing services, and downlink refers to Internet of things services. While sending and receiving data to the cloud service center, edge computing also takes into account part of the data computing and storage tasks of the cloud Computing Center. See Figure 1 for details.

Due to the uniqueness, incompatibility, direct friendliness, and other characteristics of face recognition, it has become an authentication method in a variety of intelligent systems, and its security directly determines the security of intelligent systems. Therefore, this paper proposes a privacy protection technology in an intelligent face authentication system based on edge computing [22]. The main technologies of face recognition include face detection, face data preprocessing, face feature extraction, similarity measurement, and discriminant classification, and finally output the recognition results [23]. In this study, convolutional neural network (CNN) is used to assist in face authentication of intelligent system. Through learning a large number of face data, the face information is digitally represented to form a deep CNN model for face feature extraction. The basic structure of CNN includes convolution layer, pooled sampling layer, and full connection layer; see Figure 2 for details.

In convolution layer, convolution core is used to traverse the image, and the corresponding data in the same region of the image are accumulated to activate function operation as the output of a single neuron.

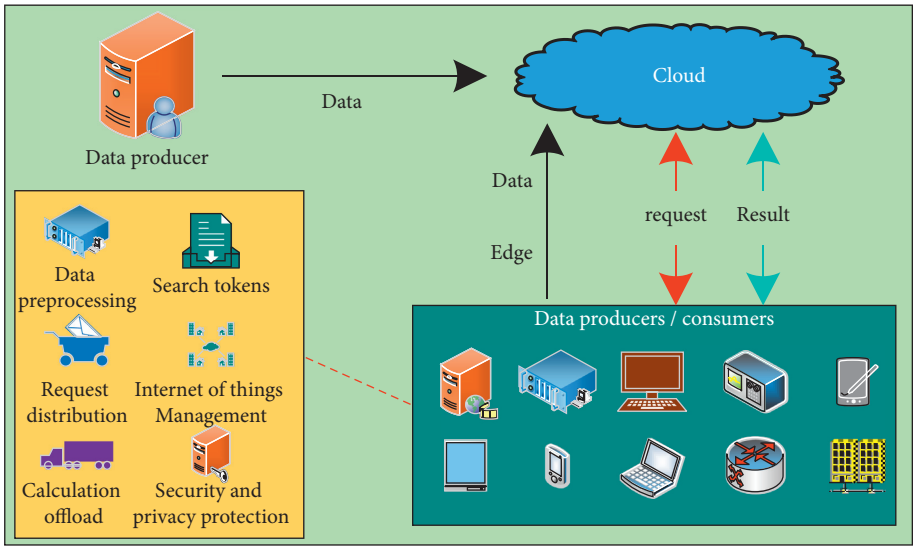

Figure 1: Edge computing model.

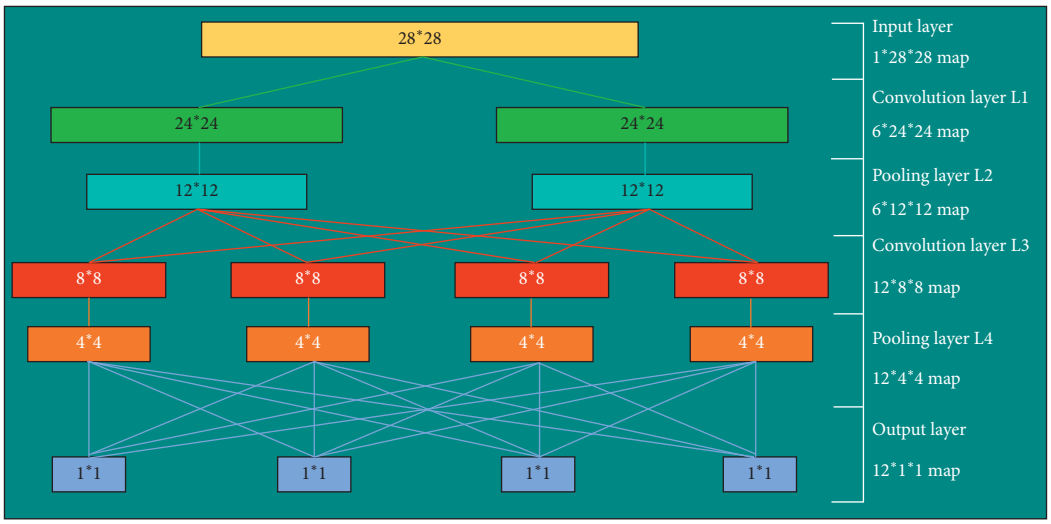

Figure 2: Basic structure of convolutional neural network.

$$x_j^l = F\left(\sum_{i,j} \omega_{ij}^l \otimes x_i^{l-1} + b_j^l\right). \tag{1}$$

In formula (1), x_j^l refers to the j characteristic graph on the l layer of CNN; $F(\cdot)$ is the activation function in the network; and ω_{ij}^l and b_j^l refer to the weight parameter and bias parameter in turn.

$$H_\theta(x) = \begin{bmatrix} p\left(y^i = 1|x^i;\theta\right) \\ p\left(y^i = 2|x^i;\theta\right) \\ \cdots \\ p\left(y^i = m|x^i;\theta\right) \end{bmatrix} = \frac{1}{\sum_{j=1}^m e^{\theta_j^T x^i}} \begin{bmatrix} e^{\theta_1^T x^i} \\ e^{\theta_2^T x^i} \\ \cdots \\ e^{\theta_m^T x^i} \end{bmatrix}. \tag{2}$$

In formula (2), x^i is the input vector of the classifier; y^i is the sample category, $y^i \in \{1, 2, \ldots, m\}$ is the sample category, and m is the total number of samples, so $p(y^i = m|x^i;\theta)$ is the probability estimate.

$$J(\theta) = -\frac{1}{N}\left[\sum_{i=1}^N \sum_{j=1}^m 1\left\{y^i = j\right\} \log \frac{e^{\theta_j^T x^i}}{\sum_{j=1}^m e^{\theta_j^T x^i}}\right]. \tag{3}$$

Equation (3) is the objective loss function of softmax classifier, where the meaning of each letter is the same as above. In the research process, the cosine similarity function is used to verify whether the two feature vectors belong to different face images of the same person, as shown in equation (4).

$$\mathrm{COS}(f_1, f_2) = \frac{f_1^T f_2}{\|f_1\|\|f_2\|}. \tag{4}$$

In equation (4), f_1 and f_2 are all arbitrary face feature vectors, where $f_1 = (a_1, a_2, \ldots, a_m)$ and

$f_2 = (b_1, b_2, \ldots, b_m)$ obey Gaussian distribution of 0-means. Whether two eigenvectors belong to the same person or not is measured by calculating the similarity of two eigenvectors in multidimensional space. In the process of research, Shamir threshold scheme is selected to protect sensitive data. The secret information is recorded as s, divided into n parts, and distributed to n users. A perfect (t, n) secret sharing threshold requires at least T Information holders to reconstruct the secret information.

$$f(x) = \sum_{i=1}^{t} f_i(x) = \sum_{i=1}^{t} y_i \prod_{j=1, j\neq i}^{t} \frac{x - x_j}{x_i - x_j}. \tag{5}$$

Equation (5) shows the process of secret information reconstruction by t information cooperators, and $(x_i, x_j)(1 \le i \le t)$ is the subkey owned by t information holders; x_i is a nonzero constant, which is open to all information holders; and y_i is the unique subkey of a single information holder.

Figure 3 shows the CNN structure responsible for face feature extraction, which consists of four convolution layers and maximum pooling to recognize face features hierarchically; The output of one-dimensional feature is realized by a fully connected layer; The softmax output layer is used to output feature categories.

Figure 4 shows the specific model parameters of convolutional neural network used in the research process. Totally, 2800 categories are selected as the training data, that is, the final output size of softmax output layer is 2800. It can be seen that with the extension of network structure, the dimension of feature graph is decreasing, and it becomes a highly abstract feature vector in the last hidden layer.

$$y^{j(r)} = F\left(b^{j(r)} + \sum_i k^{ij(r)} * x^{i(r)}\right). \tag{6}$$

In equation (6), x^i refers to the feature map of the input of layer i; y^j refers to the feature map output by the j layer; k^{ij} is the convolution kernel between x^i and y^j; "$*$" calculate the symbol for convolution; b^j is the configuration parameter corresponding to the characteristic graph of the jth output layer; and r is the weight sharing area.

$$F(x) = \begin{cases} ax, & x < 0, \\ x, & x \ge 0. \end{cases} \tag{7}$$

Equation (7) is the parametric relu activation function of activated neurons, where a is the parameter involved in training.

$$y_{j,k}^{i} = \max_{0 \le m,n < s} \left\{x_{j\cdot s+m, k\cdot s+n}^{i}\right\}. \tag{8}$$

Formula (8) is the maximum pooling formula, y^i is the ith output characteristic graph, in which each neuron comes from the nonoverlapping region with the size of $s \times s$ in x^i.

$$y_j = F\left(\sum_i x_i^1 \cdot \omega_{i,j}^1 + \sum_i x_i^2 \cdot \omega_{i,j}^2 + b_j\right). \tag{9}$$

Formula (9) is the calculation formula of the neurons in the last hidden layer. The corresponding neurons in the last convolution layer are expressed as x^1 and x^2, the weight parameters are expressed as ω^1 and ω^2, the bias parameter is b, and the activation function is $F(\cdot)$.

$$y_i = \frac{\exp(y_i')}{\sum_{k=1}^{n} \exp(y_k')}, \tag{10}$$

$$y_k' = \sum\nolimits_{i=1}^{1} 60 x_i \cdot \omega_{i,k} + b_k. \tag{11}$$

Equation (10) is responsible for predicting the probability distribution of n categories. In equation (11), the calculation result of 160-dimensional eigenvector is used as the input of category k, and the output is y_k. The bias parameter of class k is b_k. The input of the i layer is characterized by x_i; $\omega_{i,k}$ are the weights corresponding to the features of class k and layer i.

2.2. Privacy Protection Scheme for Intelligent System. After extracting face feature data through CNN, privacy protection scheme should be set to protect face data stored in the location of edge computing node [24]. When users register their identity through an edge computing node, a privacy protection scheme based on the nearest security neighbor is set.

As shown in Figure 5, when the user registers, the camera collects face data and uploads it to the edge computing node. The authority allocation agency is responsible for transmitting the corresponding encrypted authority vector to the edge computing node, and the edge computing node extracts face features and encrypts them [25]. In this process, there is a 160-dimensional random bit vector s and two 160 * 160 random invertible matrices M1 and M2. The key is shared by all n edge computing nodes.

$$f_i = \left(f_{i,1}, f_{i,2}, \ldots, f_{i,160}\right)^T. \tag{12}$$

Formula (12) is the expression of face feature vector of registered user f_i, where T is the threshold value of face verification, i is the output feature map, and the edge computing node transforms formulae (12) into (13).

$$\widehat{f}_i = \left(\frac{f_{i,1}}{\|f_i\|}, \frac{f_{i,2}}{\|f_i\|}, \ldots, \frac{f_{i,160}}{\|f_i\|}\right)^T. \tag{13}$$

In equation (13), $\|f_i\|$ refers to the 2- norm of the face feature vector $f_i = (f_{i,1}, f_{i,2}, \ldots, f_{i,160})^T$.

$$\begin{cases} \widehat{f}_{ia}[j] = \widehat{f}_{ib}[j] = \widehat{f}_i[j], & \text{if } S[j] = 0, \\ \widehat{f}_{ia}[j] + \widehat{f}_{ib}[j] = \widehat{f}_i[j], & \text{if } S[j] = 1. \end{cases} \tag{14}$$

In equation (14), $j \in [1, 160]$, when $[j] = 0$, there is $\widehat{f}_{ia}[j] = \widehat{f}_{ib}[j] = \widehat{f}_i[j]$, When $S[j] = 1$, $\widehat{f}_{ia}[j]$ is an arbitrary real number and $\widehat{f}_{ia}[j] + \widehat{f}_{ib}[j] = \widehat{f}_i[j]$ exists. Where S is the encryption key, the vector $(\widehat{f}_{ia}, \widehat{f}_{ib})$ can be obtained by substituting $\widehat{f}_i$ and S into equation (14). Combined with the encryption key M_1, M_2, $(M_1^T \widehat{f}_{ia}, M_2^T \widehat{f}_{ib})$ can be obtained as the feature vector for encryption in the privacy protection scheme. The fluorite protection scheme based on the secure nearest neighbor algorithm makes a lightweight encryption

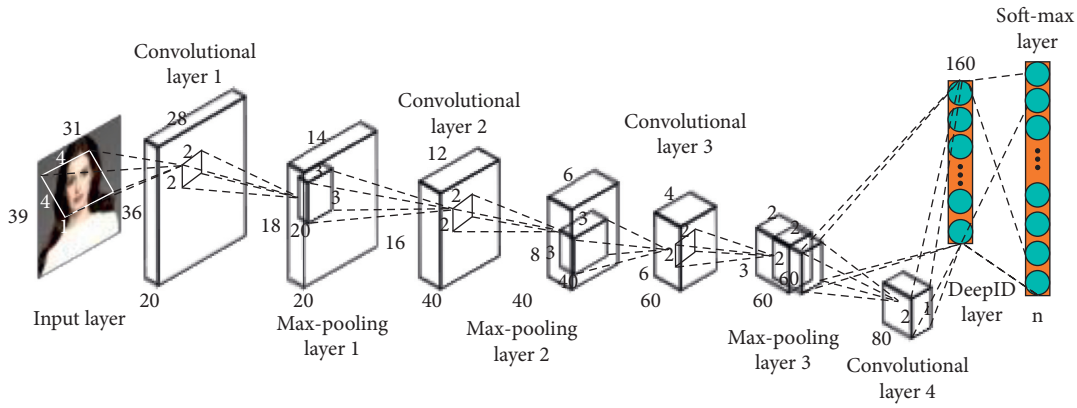

Figure 3: CNN structure for face feature extraction.

Network level	Passageway	Filter size	Step	Enter the size	Output size
Convolution layer 1	20	4*4	1	39×31×1	36×28×20
Pooling layer 1	20	2*2	2	36×28×20	18×14×20
Convolution layer 2	40	3*3	1	18×14×20	16×12×40
Pooling layer 2	40	2*2	2	16×12×40	8×6×40
Convolution layer 3	60	3*3	1	8×6×40	6×4×60
Pooling layer 3	60	2*2	2	6×4×60	3×2×60
Convolution layer 4	80	2*2	1	3×2×60	2×1×80
Fully connected layer	1	-	-	2×1×80	160×1
Softmax layer	1	-	-	160×1	2800

Figure 4: Parameters of convolution neural network model.

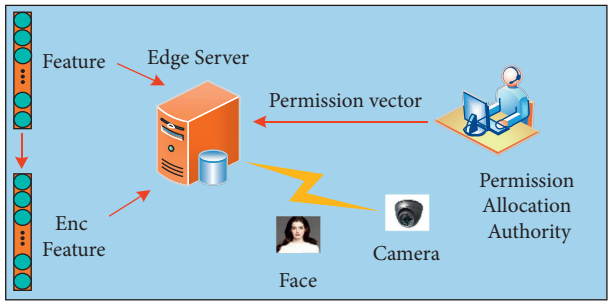

Figure 5: Identity registration process of privacy protection scheme based on secure nearest neighbor algorithm.

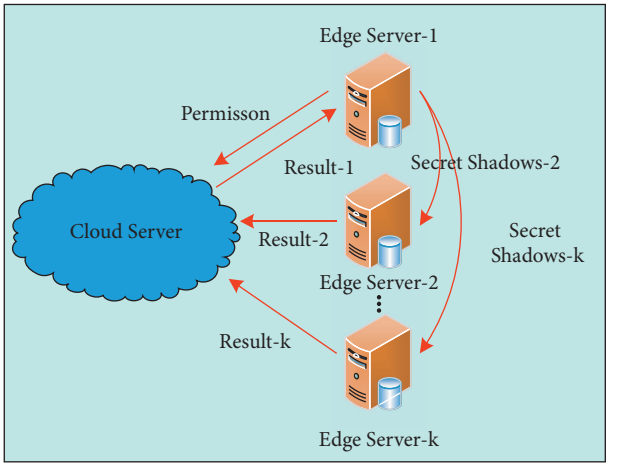

Figure 6: Identity authentication process of privacy preserving scheme based on secret sharing homomorphism.

of face feature vectors and stores the local database with edge computing equipment. Users can obtain the corresponding information access rights after they pass the identity authentication, so as to realize the privacy protection of users.

When an edge computing node is requested to perform identity authentication, the node randomly selects $(t-1)$ devices, which come from other edge computing. The two devices cooperate through secret sharing homomorphism technology and aggregate the obtained calculation results through cloud computing center to complete the acquisition of user permission information [25]. The details are shown in Figure 6.

After a series of preprocessing, such as redundant data clipping, interference noise filtering, image scaling, and so on, a 160-dimensional feature vector $f_q = (f_{q,1}, f_{q,2}, \ldots, f_{q,160})^T$ is proposed from the image through CNN model, in which f_q is the face feature vector of the authenticated user, and T is the threshold value of face verification.

$$Q[j] = \begin{cases} -1, & f_{i,j} < 0, \\ 1, & f_{i,j} \geq 0. \end{cases} \quad (15)$$

In equation (15), Q is the user requesting authentication, j is the dimension, and $j \in [1, 160]$ and f_i are the face feature vectors of registered users.

$$U_j^i[k] = \left(\widetilde{f}_{qj}[k] + \widetilde{f}_{ij}[k]\right) \prod_{l=1, l \neq j}^{t} \frac{-x_l}{x_j - x_l} (\text{mod } p). \quad (16)$$

Equation (16) is the expression of the intermediate vector U_j^i, where $k \in [1, 160]$, $(\widetilde{f}_{q1}[k], \widetilde{f}_{q2}[k], \ldots, \widetilde{f}_{qj}[k])$ is the t sub secret of the eigenvector $\widetilde{f}_i[k]$, t is the threshold value in secret sharing homomorphism, and p is a large prime number greater than n. t edge computing encrypts U_j^i and sends it to the cloud server. The cloud server summarizes all the information and compares the cosine similarity between the eigenvector f_q and the eigenvector f_i through equation (17). Cosine similarity can calculate the similarity between any two feature vectors in multidimensional space and measure the similarity mainly by the angle. According to the definition of cosine similarity, the cosine values of the angles between all matching vectors and reference vectors are similar. When using cosine similarity as a constraint condition for face recognition, it can effectively reduce the false matching points.

$$\text{COS}\left(f_q, f_i\right) = \sum_{k=1}^{160} R_i[k] Q[k] 2^{\sum_{j=1}^{n} U_j^i[k]}, \quad (17)$$

where R is the symbol vector of registered users, Q is the symbol vector of authenticated users, f_q and f_i are the feature vectors of human face, and $\text{COS}(\cdot)$ is the calculation formula of cosine similarity, $k \in [1, 160]$.

3. Analysis of Security Effect of Intelligent System

3.1. Training Effect of Convolution Neural Network. CASIA Webface data set is selected as the training set of convolutional neural network. The data set contains more than 10000 categories of data, a total of ab better. It can be seen that when the false-positive rate (FPR) is the same, the true rate (TPR) of CNN model is always higher than that of ANN moing set. After the research process, LFW face data set is selected as the verification set of CNN model. There are 5749 categories of objects in the data set, including 13233 face images, of which 1680 objects have two or more face images. The maximum number of iterations of the network is 240000, the test interval is 2000, the number of iterations to complete a test is 129, and the learning rate is 0.001. Every 40000 iterations of the network, 0.1 is used as an index to update the learning rate, and the network is trained in CPU mode [26].

Figure 7 shows that with the increase of the number of iterations, the test loss value in the network training process decreases gradually. When the number of iterations is 50000, the loss value decreases to the minimum, and then gradually becomes stable. In the process of network training, the model test accuracy increases with the increase of the number of iterations. When the number of iterations is 50000, the test accuracy reaches the maximum, and then gradually becomes stable, and the convolutional neural network training is successful. The LFW data set is selected as the validation set of the convolutional neural network model after training, and 6000 pairs of face images are selected. In total, 3000 pairs of face data in these images are positive examples, marked as 1, and the remaining images are from different objects and are marked as 0. The trained convolution neural network is used to extract the feature vectors of 6000 pairs of faces in the data set. According to the specific situation of the feature vectors, the cosine similarity between the feature vectors is calculated and normalized to the [0, 1] interval. Different thresholds between 0.2 and 0.8 are selected to calculate the accuracy of 6000 pairs of face verification under different thresholds.

As can be seen from Figure 8, with the increase of the threshold value from 0.2 to 0.8, the accuracy rate of face verification first increases and then decreases. When the threshold value is 0.51, the accuracy of face verification reaches the maximum value, which is 92.46%, which also indicates that the accuracy of face verification of the intelligent system designed in this study can reach 92.46%, which is far beyond the recognition strength of human eyes, indicating that the proposed scheme can significantly increase the security of the intelligent system.

In the field of machine learning, receiver operating characteristic curve (ROC) is often used to evaluate the performance of the model. The true-positive rate (TPR) = [true case TP/(false counterexample FN + true case TP)] and the false-positive rate (FPR) = [false-positive case FP/(true counterexample TN + false-positive case FP)]. ROC curve is drawn with TPR and FPR as indicators. The larger the area under ROC curve is, the better the effect of the model is. Figure 9 shows that the model works well.

Figure 10 shows an example of data matching failure in the verification process, in which two images in each column are the same object. It can be seen that the reasons for the failure include exaggerated expression, special shooting angle, and partial occlusion of face. That is to say, when facial expression, action, and expression are in normal state, the model designed in this paper has good recognition and matching effect, that is, the model proposed in this paper has good application effect in protecting the privacy of data set.

3.2. Security Effect Analysis of Face Recognition in Intelligent System. To verify the face recognition security of the intelligent system designed in the research, the experiment selects the intelligent face recognition system with artificial neural network (ANN) as the core and the intelligent face recognition system with deep neural network (DNN) as the core and selects CASIA webface data set as the test set, The accuracy of the three systems in CASIA webface data set is compared. CASIA webface data set contains more than 10000 categories of data and about 500000 face images.

It can be seen from Figure 11(a) that the ROC curves corresponding to Ann and DNN are all included in the range

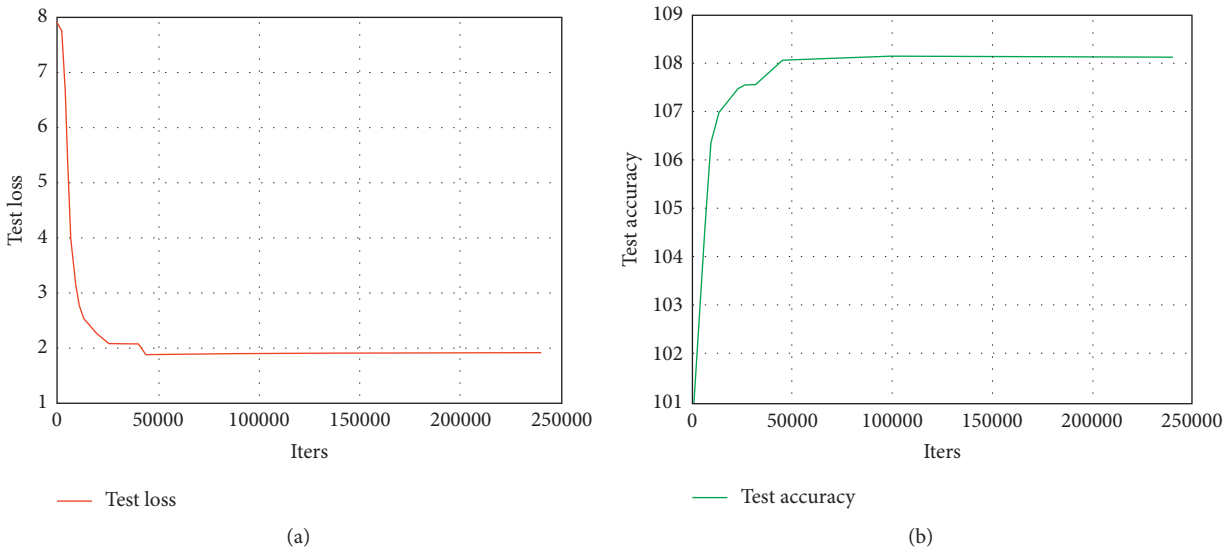

Figure 7: Test precision curve and test loss value curve in the process of network training. (a) Test loss value in the process of network training. (b) Test accuracy curve in the process of network training.

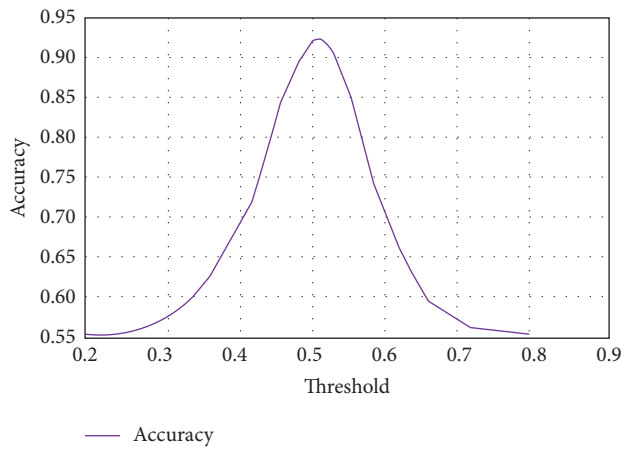

Figure 8: Curve of face verification accuracy with threshold.

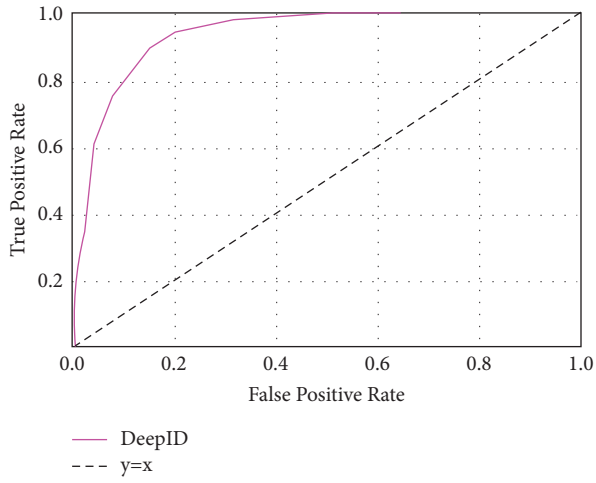

Figure 9: ROC curve drawn by cosine similarity of feature vector plaintext.

of the ROC curves corresponding to CNN. When the false-positive rate (FPR) is the same, the performance of the model represented by the curve with higher true rate (TPR) is better. It can be seen that when the false-positive rate (FPR) is the same, the true rate (TPR) of CNN model is always higher than that of ANN model and DNN model, and the true rate (TPR) of DNN model is always higher than that of ANN model. That is to say, the performance of CNN model is always better than ANN model and DNN model. At this time, the area under the ROC curve of ANN, DNN, and CNN is 0.8826, 0.9278, and 0.9359, respectively, which indicates that the intelligent system based on convolutional neural network designed in this paper can achieve better application effect in the process of face recognition verification. Figure 11(b) shows that the convergence speed of the intelligent system based on convolutional neural network (CNN) is faster than that based on ANN and DNN, which indicates that the former can complete the whole process faster in face recognition and verification.

As can be seen from Figure 12, the time consumption of the privacy protection scheme based on the secure nearest neighbor algorithm combined with the secret sharing homomorphism technology is mainly concentrated on the feature vector extraction, recognition, and encryption. It can be seen that the time consumption of face recognition in plaintext state is the lowest, and the time consumption of face recognition in the proposed algorithm is basically equal to that in plaintext state, which indicates that the proposed technology can quickly complete the user's identity registration and verification without too much interaction process on the premise of protecting the user's privacy and security, The role of edge fitting computing in the system also reduces the security degradation of intelligent system caused by too much interaction to a certain extent. In addition, the convolution neural network is used to extract the features of face image instead of the original face image,

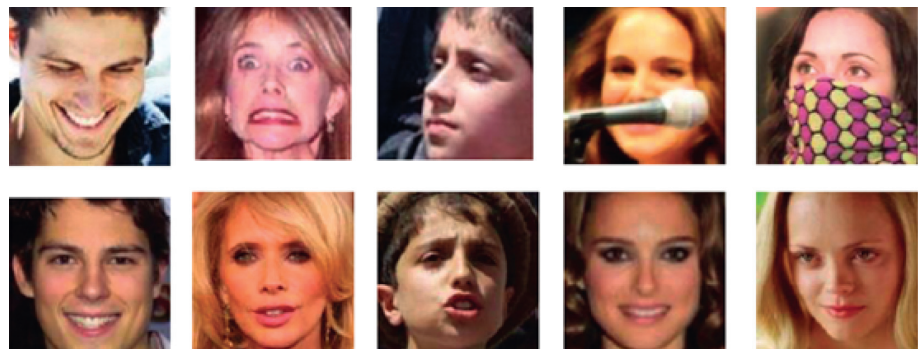

Figure 10: Failed data instance validation set matching.

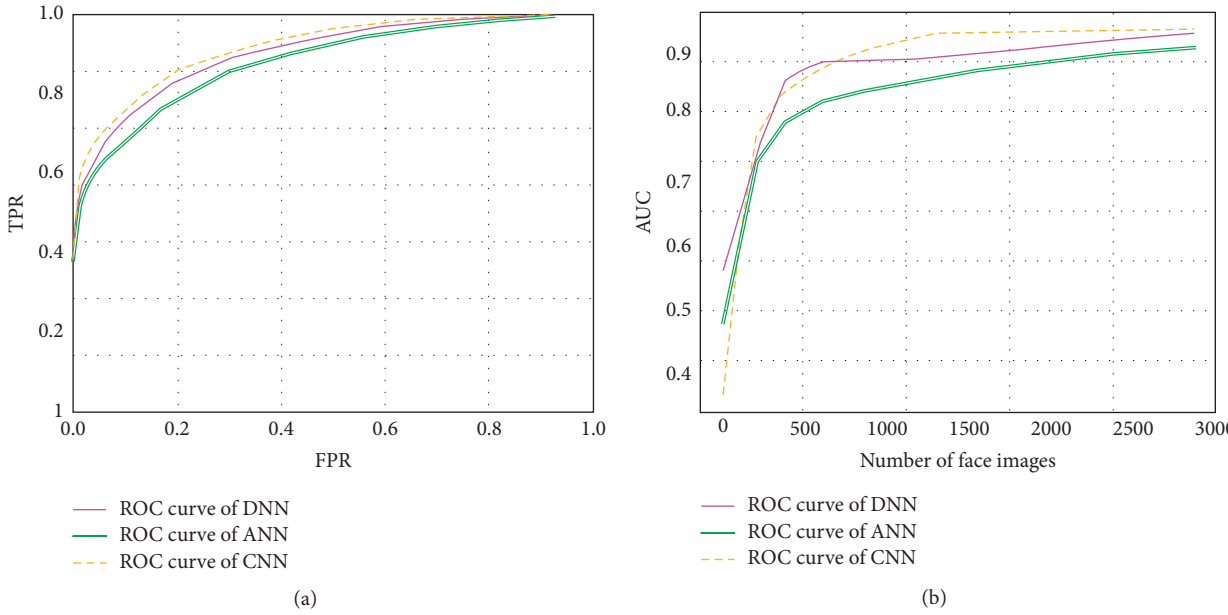

Figure 11: ROC curve and AUC curve of DNN, ANN, and CNN. (a) ROC curve of DNN, ANN, and CNN. (b) AUC curve of DNN, ANN, and CNN.

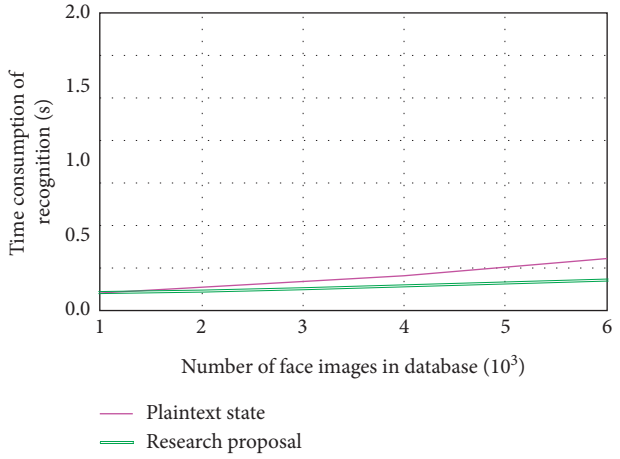

Figure 12: Time consumption in privacy preserving scheme.

which can save a lot of computing space. In the research process, the data space occupied by 10000 face images and 10000 face feature vectors are compared, and the results show that the former occupies 85504.53 Kb. The latter only takes up 7031.21 kB of space, that is to say, the face feature vector data only take up about 10% of the space of the original face image. Therefore, edge computing is used to process the face image to improve the security of the intelligent system, and the face feature vector is used to replace the corresponding face image for subsequent operations, It can greatly reduce the storage pressure and communication load of intelligent system.

4. Conclusion

With the development of computer hardware technology, artificial intelligence technology ushered in the heyday of development, intelligent systems in various industries began to popularize, biometric identification has become the mainstream technology of intelligent system to achieve user identity authentication, but also an important part of measuring the security of intelligent system. To improve the security of intelligent system, a privacy protection scheme

based on edge computing, secure nearest neighbor, and secret sharing homomorphism is designed. The results show that with the increase of the number of iterations, the test loss value decreases and the test accuracy increases. When the number of iterations is 50000, the test loss value decreases to the minimum, the test accuracy reaches the maximum, and then gradually becomes stable; With the increase of the threshold, the face verification accuracy first increases and then decreases; When the threshold is 0.51, the correct rate of face verification reaches 92.46%, which is far higher than the recognition strength of human eyes; The ROC curves of ANN and DNN are all included in the range of CNN. The area under ROC curve of ANN and DNN was 0.8826 and 0.9278, respectively, which was less than that of CNN (0.9359). The convergence speed of the intelligent system based on CNN is faster than that based on ANN and DNN. The time consumption of the proposed algorithm is almost equal to that of the plaintext face recognition. Based on face feature vector data, only about 10% of the original face image space is needed. The above results show that the proposed privacy protection scheme based on edge computing can greatly improve the security of users using the intelligent system and effectively avoid user information leakage and data loss. In this research process, cosine similarity technology is used to measure the similarity of encrypted face feature vectors. The next step is to make full use of machine learning technology to accurately classify face feature vectors in ciphertext state. Although some achievements have been made in the research, the high-intensity demand of response time in application scenarios is not considered. In the future, encryption scheme should be further improved and response time should be shortened.

Data Availability

All the data in this study are from experimental data statistics.

Consent

Informed consent was obtained from all individual participants included in the study references.

Conflicts of Interest

The authors declare that there are no conflicts of interest.

Acknowledgments

This work is supported by Henan Science and Technology Plan Project (202102210355). Research on key technologies of CCN-based service deployment, discovery and scheduling optimization in MEC Environment.

References

[1] P. Bagga, A. K. Das, and M. Wazid, "On the design of mutual authentication and key agreement protocol in internet of vehicles-enabled intelligent transportation system," *IEEE Transactions on Vehicular Technology*, vol. 99, p. 1, 2021.

[2] H. Chen, C. C. Chang, and K. Chen, "Reversible data hiding schemes in encrypted images based on the paillier cryptosystem," *International Journal on Network Security*, vol. 22, no. 3, pp. 523–533, 2020.

[3] C. Chen and X. Zhao, "Separate analysis of cell-edge and cell-centre user performance for irregular massive MIMO network with interference cancellation," *IET Communications*, vol. 13, no. 3, pp. 354–362, 2019.

[4] Q. Feng, D. He, and S. Zeadally, "BPAS: blockchain-assisted privacy-preserving authentication system for vehicular Ad-Hoc networks," *IEEE Transactions on Industrial Informatics*, vol. 16, p. 4146, 2019.

[5] T. M. Ghanim, M. I. Khalil, and H. M. Abbas, "Comparative study on deep convolution neural networks DCNN-based offline Arabic handwriting recognition," *IEEE Access*, vol. 99, p. 1, 2020.

[6] S. J. Horng, J. Supardi, W. Zhou, C.-T. Lin, and B. Jiang, "Recognizing very small face images using convolution neural networks," *IEEE Transactions on Intelligent Transportation Systems*, vol. 99, pp. 1–13, 2020.

[7] S. Huang, C. Yang, S. Yin, Z. Zhang, and Y. Chu, "Latency-aware task peer offloading on overloaded server in multi-access edge computing system interconnected by metro optical networks," *Journal of Lightwave Technology*, vol. 38, p. 1, 2020.

[8] S. Jangirala, A. K. Das, M. Wazid, and A. V. Vasilakos, "Designing secure user authentication protocol for big data collection in IOT-based intelligent transportation system," *IEEE Internet of Things Journal*, vol. 8, p. 1, 2020.

[9] A. Jolfaei, P. Ostovari, and M. Alazab, "Guest Editorial special issue on privacy and security in distributed edge computing and evolving IoT," *IEEE Internet of Things Journal*, vol. 7, no. 4, pp. 2496–2500, 2020.

[10] C. F. Lai, W. C. Chien, L. T. Yang, and W. Qiang, "LSTM and edge computing for big data feature recognition of industrial electrical equipment," *IEEE Transactions on Industrial Informatics*, vol. 4, p. 1, 2019.

[11] C. Lin, D. He, and X. Huang, "BCPPA: a blockchain-based conditional privacy-preserving authentication protocol for vehicular AD HOC networks," *IEEE Transactions on Intelligent Transportation Systems*, vol. 99, pp. 1–13, 2020.

[12] C. Liu, X. Zhang, and Q. Hu, "Image super resolution convolution neural network acceleration algorithm," *Journal of National University of Defense Technology*, vol. 41, no. 2, pp. 91–97, 2019.

[13] W. Liu, C. Qin, and K. Gao, "Research on medical data feature extraction and intelligent recognition technology based on convolutional neural network," *IEEE Access*, vol. 7, p. 1, 2019.

[14] N. Padhy, R. K. Mishra, C. Satapathy, and K. Raju, "An automation API for authentication and security for file uploads in the cloud storage environment," *Intelligent Decision Technologies*, vol. 14, no. 3, pp. 393–407, 2020.

[15] R. K. P. Varma, S. Ganta, B. H. Krishna, and S. Praveen, "A novel method for Indian vehicle registration number plate

detection and recognition using image processing techniques," *Procedia Computer Science*, vol. 167, pp. 2623–2633, 2020.

[16] S. K. Sharma and B. Khuntia, "Integrated security for data transfer and access control using authentication and cryptography technique for Internet of things," *International Journal of Knowledge-Based and Intelligent Engineering Systems*, vol. 24, no. 4, pp. 303–309, 2021.

[17] C. Sonmez, C. Tunca, and A. Ozgovde, "Machine learning-based workload orchestrator for vehicular edge computing," *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 4, pp. 2239–2251, 2021.

[18] S. Sun, G. Zhang, and H. Mei, "Optimizing multi-uav deployment in 3d space to minimize task completion time in UAV-enabled mobile edge computing systems," *IEEE Communications Letters*, vol. 25, p. 1, 2020.

[19] Y. Tang, K. Guo, J. Ma, Y. Shen, and T. Chi, "A smart caching mechanism for mobile multimedia in information centric networking with edge computing," *Future Generation Computer Systems*, vol. 95, pp. 590–600, 2019.

[20] S. Wan, J. Lu, P. Fan, and K. B. Letaief, "Toward big data processing in IOT: path planning and resource management of UAV base stations in mobile-edge computing system," *IEEE Internet of Things Journal*, vol. 7, no. 7, pp. 5995–6009, 2020.

[21] X. Jiang, F. R. Yu, T. Song, and C. M. Leung, "Intelligent resource allocation for video analytics in blockchain-enabled internet of autonomous vehicles with edge computing," *IEEE Internet of Things Journal*, vol. 99, p. 1, 2020.

[22] X. Wang, D. Ma, and K Hu, "Mapping based residual convolution neural network for non-embedding and blind image watermarking," *Journal of Information Security and Applications*, vol. 59, no. 1, Article ID 102820, 2021.

[23] L. Xiong, X. Zhong, N. N. Xiong, and R. W. Liu, "Qr-3S: a high payload QR code secret sharing system for industrial internet of things in 6G networks," *IEEE Transactions on Industrial Informatics*, vol. 17, p. 1, 2020.

[24] X. Xu, Q. Liu, and Y. Luo, "A computation offloading method over big data for IoT-enabled cloud-edge computing," *Future Generation Computer Systems*, vol. 95, pp. 522–533, 2019.

[25] W. Zhang, X. Chen, Y. Liu, and Q. Xi, "A distributed storage and computation k-nearest neighbor algorithm based cloud-edge computing for cyber-physical-social systems," *IEEE Access*, vol. 8, p. 1, 2020.

[26] H. Zhu and L. Zhu, "Encrypted network behaviors identification based on dynamic time warping and k-nearest neighbor," *Cluster Computing*, vol. 22, no. 1, pp. 1–10, 2019.