Design of Digital Image Information Security Encryption Method Based on Deep Learning

Licheng Sha(✉), Peng Duan, Xinchen Zhao, Kai Xu, and Shaoqing Xi

State Grid Beijing Electric Power Company, Beijing 100031, China
shalichenglihai@163.com

Abstract. Due to the high degree of overlapping of digital image information, the security encryption ability of digital image information is weak and the encryption accuracy is low. A security encryption method for digital image information based on deep learning is designed. Determine the connection form of the deep learning network, and based on this, select the key learning function, decipher the digital image information, and complete the digital image analysis based on deep learning. According to the scrambling result of the image information, a circular index table structure is established, and then the secure encryption of digital image information is realized by solving the value range of the security parameter. The experimental results show that the maximum value of the information overlapping index of this method can only reach 1.36, which has strong digital image information security encryption ability and can effectively improve the security encryption accuracy of digital image information.

Keywords: Deep Learning · Digital Image · Information Security Encryption · Learning Function · Scrambling Processing · Circular Index Table · Security Parameters

1 Introduction

Digital image encryption is a branch of cryptography, and it is also the combination of digital image processing technology and cryptography. Understanding the basic system composition of cryptography is the key to putting forward image encryption technology. The most fundamental problem of cryptography is how to securely transmit information on open channels, and the development of the Internet has provided a shortcut for the rapid transmission and acquisition of information. However, since each participating individual can obtain information on the Internet, the encryption of information is particularly important, and preventing illegal individuals from obtaining encrypted information is exactly the subject faced by cryptography.

At present, scholars in related fields have carried out research on image encryption. Reference [1] proposes an image information encryption and compression algorithm based on the transport layer in the Internet of Things. On the basis of the original two-dimensional encryption method of square image, combined with the principle of

B. Wang et al. (Eds.): ICMTEL 2023, LNICST 534, pp. 19–32, 2024.
https://doi.org/10.1007/978-3-031-50577-5_3

image supplementary encryption algorithm of two-dimensional chaotic map, a chaotic encryption algorithm suitable for rectangular image encryption is proposed and simulated. This method has good pixel distribution but low encryption accuracy. Reference [2] proposed an image encryption algorithm based on chaotic set. The encryption algorithm can select different chaotic system combinations according to the requirements of encryption strength, use the pixel mean value and pixel coordinate value of image pixels to control the generation of chaotic keys, and enhance the connection between chaotic keys and plaintext data. On the basis of encryption, the ciphertext is cut into 3 pieces of data bit by bit and then disguised and hidden in a processed public image, which changes the appearance characteristics of the ciphertext. Through the image histogram analysis, adjacent pixel correlation analysis and image information entropy analysis of the encrypted image, the effectiveness of the encryption algorithm is shown, but the encryption ability of this method needs to be improved.

Aiming at the above problems, a security encryption method for digital image information based on deep learning is designed. According to the deep learning network connection form, the learning function is selected, the image information is deciphered, and the digital image is analyzed. The digital image information security encryption is realized through scrambling processing, cyclic index table construction and security parameter calculation. This method has stronger encryption ability and higher encryption accuracy.

2 Digital Image Analysis Based on Deep Learning

According to the deep learning network connection form, the learning function is selected to decipher the image information, and the input analysis of the digital image information can be realized. This chapter will conduct research on the above content.

2.1 Deep Learning Network Fundamentals

The deep learning network architecture contains a large number of data sample parameters, most of which are located in the fully connected layer, and the risk of overfitting is serious. Therefore, two main measures are also adopted in the training process to reduce the risk of overfitting. The first is the increase of data. The most direct measure to prevent overfitting is to expand the training data set, allowing the network to learn more features of different images under the same category. Data augmentation is a simple method to expand the data set, such as flipping, cutting, and shifting the image without changing the core elements of the original image. If all images classified as the same standard in the original training set belong to the same set space, the misclassification behavior can be avoided during testing. In addition, you can change the RGB pixel value of the original image, add specific data to the three components to simulate the effect of the original image under different light intensities and colors, and change the brightness, contrast and saturation of the original image. The second measure to reduce the risk of overfitting is based on the dropout operation of the fully connected layers. Ensemble learning emphasizes that combining the outputs of multiple models can achieve better output results than a single model. The second method is based on the same principle,

randomly selecting some neurons to inactivate to avoid mutual adaptation between different neurons. It is inclined to let each neuron combine other randomly selected neurons in the learning process, and learn different features of the image to help get a better output in the end.

For the derivation of the deep learning network connectivity criteria, it involves the joint solution of the neuron coefficient a and its supplementary description condition a'. The specific calculation formula is as formula (1):

$$a = \lim_{\delta \to \infty} \delta \left| \beta \hat{S} - \overline{S}^2 \right|_{\beta \geq \delta} \tag{1}$$

In the formula, δ represents the RGB pixel definition coefficient, and β represents the data information discarding coefficient in the original image space. And the inequality value condition of $\beta \geq \delta$ is always established, $\hat{S}$ represents the transmission characteristics of data information in digital images, and $\overline{S}$ represents the average value of data information transmission per unit time. The supplementary explanation conditions of neuron coefficient are as formula (2):

$$a' = \frac{\sqrt{\chi \frac{a}{\alpha_{\max} - \alpha_{\min}}}}{d' \cdot |\Delta S|} \tag{2}$$

In the formula, $\alpha_{\max}$ represents the maximum value of the neuron learning vector, $\alpha_{\min}$ represents the minimum value of the neuron learning vector, χ represents the learning behavior standard of digital image information, ΔS represents the unit accumulation of image data information in the deep learning network, d' represents the orientation index.

On the basis of formula (1) and formula (2), let $s_1, s_2, ..., s_n$ represent n unequal sample information parameters, and the inequality conditions of $s_1 \neq 0, s_2 \neq 0, ..., s_n \neq 0$ are established at the same time, and combining the above physical quantities, the standard expression of deep learning network connection is deduced as formula (3):

$$A_{a'} = (n! - 1)^2 \cdot \left({}^{a'}\!/_{s_1 \cdot s_2 \cdot \cdots \cdot s_n} \right) \tag{3}$$

Since the value of the n index belongs to the numerical range of $(0, +\infty)$, the deep learning network framework has a very strong bearing capacity for data information samples.

The layout of the complete deep learning network architecture is shown in Fig. 1.

It can be seen from Fig. 2 that the pooling layer extracts the features in the image, compresses the feature map to reduce parameters, and alleviates overfitting. There are two types of pooling layers: the maximum pooling layer and the average pooling layer. The former is sensitive to image texture and the latter can better preserve the image background. The maximum pooling layer is commonly used. The specific role of the pooling layer:

(1) Scale invariance: The pooling operation is performed on local regions in the image. When the image is translated horizontally, vertically or diagonally, the largest feature will remain in the local area, and the pooling layer focuses on the details of the image that can best represent the feature.

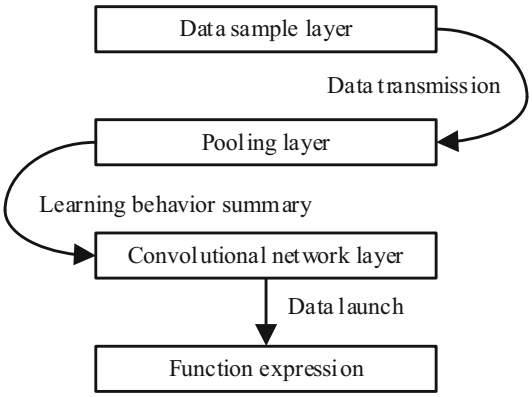

Fig. 1. Deep learning network basic connection architecture

(2) Remove redundant information: The pooling layer compresses the image information most intuitively. An image contains many pixels and has many image features, but the network does not need to fully remember these features when learning. The pooling layer can just remove most of the redundant features, allowing the convolutional network to learn the details of the essence of the image and alleviate overfitting.

2.2 Learning Function Selection

The learning function is built on the deep learning network architecture, and uses the security parameters configured by the handshake protocol to support functions such as compression, encryption and encapsulation of the upper layer data. The complete learning function includes the handshake protocol, the cipher specification change protocol, and the warning protocol. The handshake protocol mainly negotiates session parameters. That is, the version of the protocol that the encryption parties agree to use, the other party can be selected for authentication, the information about the session ID is exchanged, the encryption and compression algorithms are selected, and the shared key used to generate the key, etc. The cryptographic specification change protocol primarily signals changes to the encryption policy [3]. The protocol consists of a single message sent by the client or server, which informs the other party that the subsequent transmission process needs to be performed with a new key. The warning protocol is primarily about reporting error conditions or changes in session state to the counterparty.

When the deep learning-based function expression encrypts digital image information, the client first sends a Client Hello message to the server, which mainly informs the server of the list of cipher suites and compression algorithms it supports. After receiving the message, the server will reply a Server Hello message, the content of which is mainly to clarify which encryption algorithm the two parties want to use from the lists provided by the client. At the same time, both parties also need to verify each other's identities, that is, the server will provide the other party with its own certificate and ask the client to provide its own certificate, but this process is not necessary, because it is possible that the two parties have had a normal session before. When the client receives the certificate

of the other party, it will authenticate to the certification authority. If the authentication is passed, the client will encrypt the shared key used to encrypt the transmitted data and send it to the other party. After the above process is completed, the two parties start to change the cipher specification, that is, the two parties will use the negotiated key to conduct a conversation. At this point, the handshake process is completed, and the data transmission begins.

When selecting a learning function, it is first necessary to determine the data mutual transmission relationship between the two parties of information encryption. The specific calculation formula is as formula (4):

$$D = \left(\sum_{\varepsilon=1}^{+\infty} \gamma^2 \dot{g} + A_{a'} \right) \tag{4}$$

In the formula, ε represents the encoding coefficient of the information to be encrypted, γ represents the real-time encoding vector, and $\dot{g}$ represents the encryption feature of the information text in the digital image.

Then, the value range of encrypted information can be determined on the basis of the relational expression of data transmission;

Finally, the complete learning function expression is obtained by solving, and the calculation process is as formula (5):

$$H = 1 - \left| \frac{\log_D h}{f \times (\phi - 1)^2} \right|^2 \tag{5}$$

Among them, h represents the data sample that is executing the encryption instruction in the deep learning architecture, ϕ represents the transcoding coefficient of the digital image information, and f represents the encryption template definition item.

Also, the key must be very sensitive. The original image can only be decrypted correctly with the correct key. When encrypting the image information in the deep learning network, the processing host can find that it matches a rule in the library, and the current situation indicates that the application traffic is successfully identified. In other words, this method requires a large feature rule database to achieve better encryption effect.

2.3 Image Information Cracking

Image information cracking identifies applications based on the port numbers in the headers of deep learning network packets, that is, classifying traffic by mapping the port numbers to specific applications. The principle of this classification method is very simple. It only needs to read the first data packet in the network data stream to be successfully identified. The identification efficiency is very high and the specific implementation is extremely simple. However, with the development of network technology, this method faces many problems: some application ports may not be registered. Some applications use dynamic ports, which may change during data transfer. Some applications use ports of other common protocols for data transmission in order to avoid system restrictions, so as to achieve port concealment. Moreover, since the header port information is hidden

after the traffic is encrypted, it is difficult to identify the encrypted traffic by the port number.

The so-called deep learning is to use the labeled data to continuously train the model, so that the model can predict the results of any given range of data. In order to be able to judge the quality of model training, the input sample data is usually labeled, and when the model training ends, the parameter variables of the model at this time are loaded into the classifier that recognizes unknown types [4]. Usually, the recognition accuracy of this method is better, so this method is also used by researchers in the field of encrypted traffic recognition and classification.

Let k_1 and k_2 represent two unequal digital image information training parameters, and their values satisfy formula (6):

$$k_1, k_2 \in (0, 1) \tag{6}$$

By combining formula (5) and formula (6), the digital image information cracking expression can be defined as formula (7):

$$J = \frac{\sum_{\iota=1}^{+\infty} \frac{\varphi \cdot \tilde{L}}{|k_1 - k_2|^2}}{\sum_{\iota=1}^{+\infty} \vec{q} \times \vec{j}} \times H \tag{7}$$

In the formula, ι represents the initial value of the encryption node labeling coefficient, and $\tilde{L}$ represents the value feature of the digital image information sample in the deep learning network, φ represents the sequential encryption parameter of digital image information, $\vec{q}$ represents the learning vector of digital image information, and $\vec{j}$ represents the encryption vector of digital image information.

The so-called image information cracking is to use a small number of labeled and a large number of unlabeled sample data for model training, and to associate the unlabeled data with the labeled sample data in some way, so as to introduce the information contained in the unlabeled data. The main reason is that the deep learning framework is expensive to label data, so when deciphering image information, it first tries to model the unlabeled sample data, and then predicts the labeled data [5]. The main premise of considering deep learning algorithms is that the distribution of data must not be completely random. Therefore, better classification results can be achieved through the local features of a few labeled samples and the overall distribution of a large number of unlabeled samples.

3 Security Encryption of Digital Image Information

With the support of the deep learning network architecture, according to the execution process of scrambling processing, cyclic index table construction, and security parameter calculation, the secure encryption of digital image information is completed, and the smooth application of the deep learning-based digital image information security encryption method is realized.

3.1 Scrambling

The scrambling of digital image information needs to be organized by binary tree. A binary tree is a tree structure where each node has at most two subtrees, called the left subtree and the right subtree. For a complete binary tree, the capacity of each layer of node organization for data samples is exactly the same.

Its depth and number of nodes are w_0 and e_0, respectively, and the numerical relationship between the two can be described as formula (8):

$$\begin{cases} w_0 \geq 1 \\ e_0 \geq 1 \\ w_0 \neq e_0 \end{cases} \tag{8}$$

Binary tree is a common way to implement binary search tree and binary heap. The basic operation of a binary tree is traversal. Since the structure of a binary tree is nonlinear, traversal essentially transforms each node of the binary tree into a linear sequence according to certain rules and order.

Generally speaking, the reproduction process of digital image information encryption behavior by deep learning network can be understood as computer simulation reproduction or optical reproduction. The computer simulation reproduction process can be realized using only a computer. In the optical reproduction method, a corresponding experimental framework needs to be built. In the framework of the optical reproduction experiment, when the beam emitted by the laser is collimated and expanded, the spatial light modulator loads the hologram. The expanded beam is then irradiated on the spatial modulator, reflected by the spatial light modulator, and then the reflected beam passes through the lens to adjust the size and position of the reproduced image. Finally, it is received by the basic learning node and transmitted to the computer for display.

The deep learning network can divide the collected information into real object information and virtual object information. The real object information can obtain object information through related image acquisition instruments [6]. The virtual object information can be simulated and obtained by computer-related software. In the encryption process, the random phase plate is regarded as the key to restore the original image, and only by obtaining the correct random phase distribution can it be decrypted correctly.

Digital image information can be viewed as a collection of many point clouds of data samples, or it can be decomposed into a collection of many levels. The encryption method is to divide the digital image information into a plane layer with a certain surface spacing to obtain the cross-section of each layer, and then project the cross-section of each layer to reconstruct the object [7]. The digital image information can be divided at equal intervals along the direction of the given coordinate axis, and then the complex amplitude distribution of the light field of each layer section at the holographic surface is calculated, and then the complex amplitude of each layer section is superimposed to obtain the total light field distribution of the holographic surface.

The solution expression for scrambling processing of digital image information is as formula (9):

$$R = \frac{\sqrt{\frac{1}{J}\sum_{\kappa=1}^{+\infty}|w_0 \times e_0|^2}}{\tilde{y} \cdot |\Delta T|} \tag{9}$$

Among them, κ represents the digital image information division coefficient, ΔT represents the unit execution time of the digital image information encryption instruction, and $\tilde{y}$ represents the projection length of the digital image information to be encrypted in the deep learning network architecture.

In each deep learning network connection layer structure, each neuron sums up the local output digital image information of the previous layer according to a certain weight, and then inputs the weighted result into the activation function. The activation function is a non-linear change, which prevents the deep learning network from learning only simple linear combinations of inputs.

3.2 Loop Index Table

The index matrix can be used to scramble image data. The specific steps of indexing the matrix include: first, establishing an indexing matrix. Second, find each specific number of positions from 1 to n in each row of the index matrix, and generate a permuted index matrix. Then the data in these positions are rotated to the next position in turn to obtain the result of scrambled encryption.

However, the index matrix is fixed once it is determined. Therefore, if the key for encryption is obtained, the encrypted image can be easily cracked. In order to avoid this problem effectively, a scrambling structure based on dynamic circular scrambling index table is proposed. The corresponding operation steps are as follows: First, use plaintext and standard sequence conditions generated by the deep learning network framework. Then, use the chaotic sequence to control the cyclic shift of the reference sequence to generate a matrix table [8]. Finally, transpose the matrix to get a circular index table. The circular index table is dynamically generated and has a strong correlation with the plaintext, which can effectively resist selective plaintext attacks.

Let $\lambda_1, \lambda_2, ..., \lambda_n$ represent n different digital image plaintext information value indicators, and $i_1, i_2, ..., i_n$ represent n different digital image plaintext information sample value results, and formula (9) can be combined, and the cycle index coefficient $Y_1, Y_2, ..., Y_n$ can be expressed as formula (10):

$$\begin{cases} Y_1 = 1 - \dfrac{i_1}{\lambda_1 R} \\ Y_2 = 1 - \dfrac{i_2}{\lambda_2 R} \\ \vdots \\ Y_n = 1 - \dfrac{i_n}{\lambda_n R} \end{cases} \tag{10}$$

Using the circular index table to calculate the encrypted expression of any digital image information, the calculation time can be reduced by algorithm optimization. However, in practical applications, the computing time and computing efficiency of fully encrypted information parameters will vary with the change of the tilt angle of the image. When the inclination angle is too large, a problem of computational inefficiency is caused, and the display quality of the reproduced image is also degraded.

On the basis of formula (10), let μ represent the tilt angle of the digital image. In the deep learning architecture, the value of μ always belongs to the numerical range of $\left(0, \frac{\pi}{2}\right]$, $\tilde{u}$ represents the encryption efficiency, and $\vec{p}$ represents the encryption calculation vector based on deep learning. Combining the above physical quantities, the calculation expression of the loop index table is formula (11):

$$P = \frac{\left|\cos\mu - \frac{1}{\tilde{u}}(Y_1 + Y_2 + \cdots + Y_n)\right|}{\vec{p} \cdot \sin\mu} \tag{11}$$

For the image information diffusion part, a parameter fine-tuning method is proposed. The method effectively combines the plaintext image and the key, and at the same time improves the diffusion effect of the diffusion algorithm, and also uses the parameter fine-tuning method to improve the diffusion effect for the existing encryption algorithm. There are Gaussian noise signals in digital images. Gaussian noise is a kind of noise whose probability density function obeys Gaussian distribution and is uniformly distributed in image information density. For Gaussian noise, the second moment is uncorrelated and the first moment is constant, which refers to the temporal correlation of continuous information. In the process of encrypting digital image information, Gaussian noise is used as additive noise, which improves the encryption security of information.

3.3 Security Parameters

The number of occurrences of each pixel value in a digital image accounting for the total pixel value of the plaintext can be regarded as a probability value. Therefore, an advantage of using deep learning coding to encrypt plaintext images is that the result of deep learning coding and encryption changes according to the change of plaintext, which can solve the problem that some algorithms are not strongly related to plaintext. At the same time, deep learning coding also has a certain compression effect, which can maximize the lossless compression of image information, and combine it with the circular index table and scrambling processing mechanism. Finally, embed the obtained secret image into a carrier image to realize hiding, which will be a secure encryption algorithm. Chaos has the property of being sensitive to initial conditions, and for a system without inherent randomness, as long as the two initial values are close enough, the two trajectories from them will remain close enough throughout the course of the system. But for a chaotic system with inherent randomness, two trajectories starting from two very close initial values may become "enough" apart after a long period of evolution, showing extreme sensitivity to the initial values.

The steps to solve the security parameters in the process of digital image information encryption are shown in Fig. 2.

It can be seen from Fig. 2 that a significant quality evaluation index for the encrypted image is the histogram analysis of the image. The histogram of the original image is

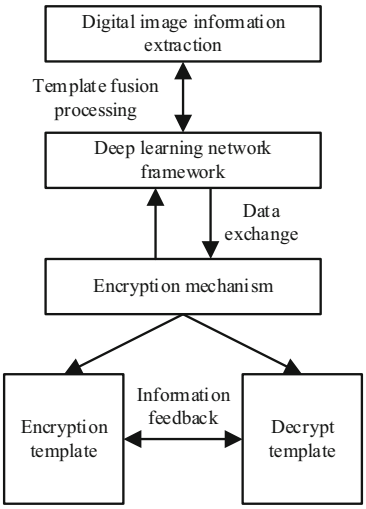

Fig. 2. Security parameter solution steps

based on the theme that the image needs to express, and some pixel values are very high and some are very low. However, all encrypted images must meet the condition of histogram equalization, that is, the histogram of the encrypted image is equalized, and the pixel values are evenly distributed in the predetermined value interval of the interval [9]. The uniform histogram can mask the information of the encrypted image and prevent the attacker from using the frequency statistics attack. According to the characteristics of the image, the pixel values between adjacent pixels are roughly similar, and the colors of the images transition smoothly, thus forming different color blocks to express different content themes. However, the encrypted image pixel values are approximately randomly distributed, and the correlation coefficient can be used to analyze the adjacent pixel correlation coefficient between the original image and the encrypted image.

Let $\tilde{z}$ represent the compression coefficient of digital image information, ξ represent the data information encryption authority based on the deep learning network, ΔX represent the unit accumulation of encryption operation instructions, and C represent the directional encryption coefficient. With the support of the above-mentioned physical quantities, formula (11) is combined, and the calculation result of deriving digital image information encryption security parameters is shown in formula (12):

$$M = \frac{1 - \tilde{z}\left|\frac{1}{\xi \times P}\right|^2}{C \times |\Delta X|} \tag{12}$$

A deep learning network is used to extract the feature maps of the fixed hidden layer of the style image and the content image, and the hidden layer selected for the general content image is close to the output layer. The style image needs to select multiple hidden layers approximately uniformly, so that the obtained style transfer image does not deviate from the original image in content and is close to the style image to be converted in style [10]. A differential attack is a chosen-plaintext attack. The attacker often makes some

changes to the original image and then uses the proposed encryption algorithm to encrypt the original image and the changed image, and analyzes the relationship between the encrypted images before and after the change, hoping to find clues about the encryption key. In order to resist differential attacks, the encrypted image must be completely inconsistent even if the original image is only one pixel different. Two evaluation criteria are often used in analysis to test the degree of differentiation of images after encryption. One is the pixel change rate, and the other is the normalized pixel value change intensity.

4 Experimental Analysis

In order to highlight the practical value of the digital image information security encryption method based on deep learning, the method of reference [1] (Image information encryption and compression method based on the transport layer in the Internet of Things) and the method of reference [2] (An image encryption method based on chaotic sets) are used as comparison methods, the following comparative experiments are designed.

4.1 Experiment Preparation

In order to test the encryption effect of the proposed method, build a network system as an experimental environment, as shown in Fig. 3.

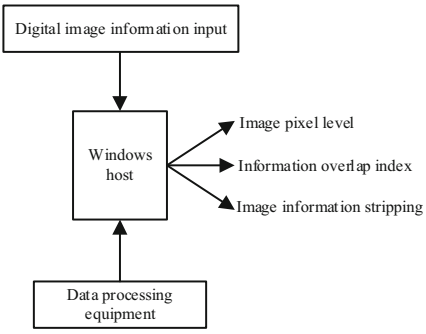

Fig. 3. Experimental environment

According to Fig. 3, input the selected digital image into the Windows host, close the control switch, and judge the processing capability of the selected encryption method for digital image information according to the indication level of the relevant equipment components.

In order to ensure the authenticity of the experimental results, when changing the encryption algorithm, the model of the selected experimental component remains unchanged.

4.2 Steps and Processes

Step 1: Control the Windows host using the deep learning-based digital image information security encryption method, and record the specific numerical changes of the information nesting index, the degree of information stripping, and the image pixel level;
Step 2: Clear the existing experimental results and debug the Windows host to the initial state;
Step 3: Use the neural network-based digital image information security encryption method to control the Windows host, and record the specific numerical changes of the information nesting index, the degree of information stripping, and the image pixel level;
Step 4: Clear the existing experimental results again, and debug the Windows host to the initial state;
Step 5: Utilize the digital image information security encryption method based on the kernel function to control the Windows host, and record the specific numerical value changes of the information nesting index, the degree of information stripping, and the image pixel level;
Step 6: Compare the obtained experimental results and summarize the specific experimental rules.

4.3 Analysis of Experimental Results

The information overlapping index can affect the security encryption ability of the network host for digital images. Without considering other interference conditions, the lower the numerical level of the information overlapping index, the stronger the security encryption ability of the network host for digital images.

The specific experimental results of the information overlap index of the three groups of experimental methods are shown in Fig. 4.

According to Fig. 4, the information overlap index of the proposed method shows a numerical change trend of increasing first and then decreasing, and the maximum value can only reach 1.36 during the whole experiment. The information overlap index of the method of reference [1] also shows a numerical change trend of increasing first and then decreasing. However, the rising trend of its value in the early stage of the increasing stage is significantly larger than that in the later stage. During the whole experiment, its maximum value reaches 2.00, which is much higher than the information overlap index level of the proposed method. The information overlap index of the method of reference [2] shows a numerical change trend of increasing first and then stabilizing. During the whole experiment, its maximum value reached 2.40, and the duration of the extreme value level reached 15 min, and its average level was also much higher than the information overlap index level of the proposed method. It can be seen that the proposed method has strong security encryption ability for digital image information.

It is specified that ψ' represents the security vector, and its value is always equal to 1 during this experiment. The calculation formula of encryption accuracy of digital image information is as formula (13):

$$B = \frac{\psi'}{\hat{\omega}_{\max}} \times 100\% \tag{13}$$

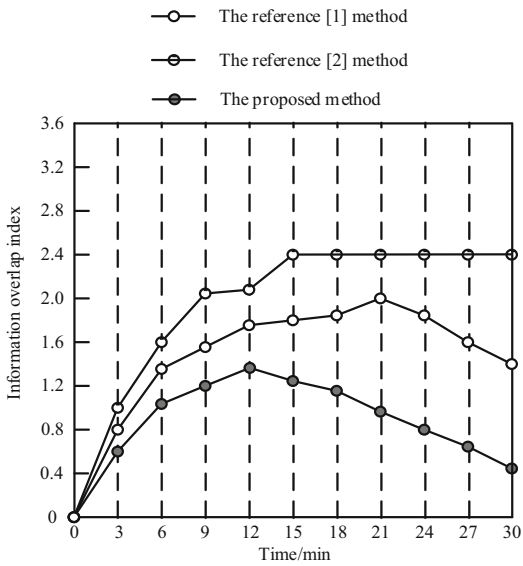

Fig. 4. Experimental value of information overlap index

Among them, $\hat{\omega}_{\max}$ represents the maximum value of the information overlap index.

Formula (13) is used to calculate the encryption accuracy of digital image information of the three methods, and the specific calculation results are shown in Table 1.

Table 1. Encryption accuracy of digital image information by different methods

Different methods	Encryption accuracy
The reference [1] method	85.6%
The reference [2] method	89.2%
The proposed method	97.4%

According to Table 1, the encryption accuracy of the method of reference [1] and the method of reference [2] are 85.6% and 89.2% respectively, while the encryption accuracy of the proposed method is 97.4%, which proves that the digital image information encryption accuracy of the proposed method is higher.

To sum up, the proposed method can effectively control the value result of the information overlap index. Compared with the method of reference [1] and the method of reference [2], the proposed method has stronger security encryption ability of digital image information. It can effectively improve the security encryption accuracy of digital image information, and is more in line with the application requirements of security encryption of digital image information.

5 Conclusion

This paper designs a security encryption method for digital image information based on deep learning. Determine the connection form of the deep learning network, select the key learning function, and decipher the digital image information. The image information is scrambled, the structure of the circular index table is established, and the security encryption of digital image information is realized by solving the value range of the security parameters. The experimental results show that the maximum value of the information overlap index of this method can only reach 1.36, which has a strong ability of digital image information security encryption and can effectively improve the accuracy of digital image information security encryption. It solves the problem of weak security encryption ability and low encryption accuracy of digital image information due to the high degree of overlap of digital image information. However, in this study, building a network system as an experimental environment is limited in practical application. Therefore, in the future research, VC software can be considered for programming, and the generated files can be applied in the Windows system to expand the application scope of image encryption.

References

1. Feng, N.: Algorithm of image information encryption and compression based on transmission layer in Internet of Things. J. Jixi Univ. **20**(04), 85–88 (2020)
2. Li, F., Liu, J., Wang, G., et al.: An image encryption algorithm based on chaos set. J. Electron. Inf. Technol. **42**(04), 981–987 (2020)
3. Gan, T., Liao, Y., Liang, Y., et al.: Partial policy hiding attribute-based encryption in vehicular fog computing. Soft. Comput.Comput. **25**(16), 10543–10559 (2021)
4. Shuai, H., Xu, X., Liu, Q.: Backward attentive fusing network with local aggregation classifier for 3d point cloud semantic segmentation. IEEE Trans. Image Process. **30**, 4973–4984 (2021)
5. Ao, J., Wu, T., Ma, C.: A deep learning reconstruction approach for underwater distortion image. Comput. Simul. **37**(08), 214–218 (2020)
6. Abdulwahed, M.N., Ahmed, A.K.: Improved anti-noise attack ability of image encryption algorithm using de-noising technique. TELKOMNIKA (Telecommun. Comput. Electron. Control) **18**(6), 3080–3087 (2020)
7. Mohammed, S.J., Basheer, D.: From cloud computing security towards homomorphic encryption: a comprehensive review. TELKOMNIKA (Telecommun. Comput. Electron. Control) **19**(4), 1152–1161 (2021)
8. Varkuti, K.S., Manideep, G.: A novel architectural design of light weight modified advanced encryption standard for low power and high speed applications. High Technol. Lett. **27**(2), 360–370 (2021)
9. Abdalla, M., Benhamouda, F., Pointcheval, D.: Corrigendum: public-key encryption indistinguishable under plaintext-checkable attacks. IET Inf. Secur. **14**(3), 365–366 (2020)
10. López-Santos, F., May-Pat, A., Ledesma-Orozco, E.R., et al.: Measurement of in-plane and out-of-plane elastic properties of woven fabric composites using digital image correlation. J. Compos. Mater. **55**(9), 1231–1246 (2021)