Hindawi
Advances in Multimedia
Volume 2023, Article ID 9857282, 1 page
https://doi.org/10.1155/2023/9857282

Retraction

Retracted: Algorithm of Encrypting Digital Image Using Chaos Neural Network

Advances in Multimedia

Received 12 December 2023; Accepted 12 December 2023; Published 13 December 2023

This article has been retracted by Hindawi, as publisher, following an investigation undertaken by the publisher [1]. This investigation has uncovered evidence of systematic manipulation of the publication and peer-review process. We cannot, therefore, vouch for the reliability or integrity of this article.

Please note that this notice is intended solely to alert readers that the peer-review process of this article has been compromised.

Wiley and Hindawi regret that the usual quality checks did not identify these issues before publication and have since put additional measures in place to safeguard research integrity.

We wish to credit our Research Integrity and Research Publishing teams and anonymous and named external researchers and research integrity experts for contributing to this investigation.

The corresponding author, as the representative of all authors, has been given the opportunity to register their agreement or disagreement to this retraction. We have kept a record of any response received.

References

[1] Y. Mao, "Algorithm of Encrypting Digital Image Using Chaos Neural Network," *Advances in Multimedia*, vol. 2022, Article ID 4160083, 10 pages, 2022.

Hindawi
Advances in Multimedia
Volume 2022, Article ID 4160083, 10 pages
https://doi.org/10.1155/2022/4160083

Research Article

Algorithm of Encrypting Digital Image Using Chaos Neural Network

Ying Mao

Jiangsu Vocational College of Business, Nantong 226002, China

Correspondence should be addressed to Ying Mao; 2014180@jsbc.edu.cn

Received 6 July 2022; Revised 16 August 2022; Accepted 8 September 2022; Published 21 September 2022

Academic Editor: Tao Zhou

With the rapid development of digital communication technology, data and image encryption methods will get more and more in-depth research in these aspects. Although the original cipher method can keep the image confidential, because of the storage method of the image data, for the image with too high pixel value, the process of keeping the two-dimensional information confidential and decoding will bring a large amount of computation, and the accuracy of encryption and decryption cannot be guaranteed. This paper presents a visual image encryption algorithm based on the compressed sensing method of the Hopfield chaotic neural network. Different from the existing visual image encryption methods, our method can directly embed the noise like information after encryption into the alpha channel of the carrier image, thus increasing the visual stability of the computer. Finally, through the comparison and analysis of simulation experiments, we find that the image encryption algorithm proposed in this paper has the advantages of wide password space, low risk, good visual stability, good decoding effect, and good robustness.

1. Introduction

With the development of technology, the current computer science is constantly changing the world again and again. However, the information-based life also brings to human society a problem that has never been considered: how to protect the security of personal information in the process of such extensive information exchange [1].

As the most important part of multimedia in the digital society, the vivid information of digital image is the most important means for human to describe information. Therefore, the security protection methods for digital images are not only extremely important but also representative, that is, digital images contain a large amount of data and a high degree of data correlation. Therefore, the current research on image information encryption is constantly developing and innovating. In the current image encryption technology, the research means for most images are to use ciphertext at the transmitting end and the receiving end first and then decrypt with the key [2].

The advantage of this is that both parties do not need to spend a great deal of energy on the protection of the communication channel, and it can also reduce the risk of intrusion when transmitting on the channel that cannot be verified as safe. Therefore, even if the picture in transmission is intercepted, the interceptor will think that it is not a key and thus cannot get the real information content of the picture. However, once the image is saved in the traditional password mode, although the surface information can be hidden, since the unique relevance and statistical information of the image are not saved, the attacker can still attack the image from other aspects [3]. However, with the further study of chaos theory, image encryption methods based on chaos also began to appear in the research. Chaos is essentially a phenomenon with pseudorandom characteristics in the running track of nonlinear dynamic system. However, chaos is generally a pseudorandom phenomenon and is very sensitive to the initial value. These characteristics are very necessary for the encryption process. However, because the dynamic characteristics of the high-dimensional chaotic system are more complex and the dynamic analysis is more difficult, its chaotic characteristics are also relatively stronger [4]. The main purpose of this paper is to encrypt the plaintext content of the image by using these characteristics of the

chaotic system, so as to obtain the ciphertext whose content is similar to the noise and propagate it. Even if the information can be tapped, it cannot be cracked without a key. Up to now, a kind of color image encryption algorithm based on chaos theory is still being mentioned, and this chaotic encryption technology has gradually become the dominant mode and main research direction of image encryption methods.

Artificial neural network is an artificial intelligence simulation technology based on connection technology. It has the advantages of distributed data storage, network, and large-scale planning parallel processing technology, as well as the functions of self-adaptation, self-teaching, and self-management [5]. In theory, the artificial neural network is learnable and can approach the dynamic system mode with any accuracy, but there are any nonlinear problems and uncertainties in the simulation. In the encryption of chaotic nondynamic systems, artificial neural networks provide a new way and idea for this behavior.

With the rapid development of the modern network and the expected changes of the future network, another key and important area of the network is the modern network security research, especially the information network security, which urgently needs some new and effective information transmission technologies, a process method for solving the qualitative thinking and quantitative analysis of chaotic systems [6]. It is also used to study dynamic systems. Continuous data relationships are needed to interpret and predict behavior [7].

Because many characteristics of chaos can be used to study cryptography, but it is also an uncertain problem, so now we can consider introducing chaos into cryptography. We can use some characteristics of chaos to study more credible and reliable cryptographic communication. Compared with the conventional encryption technology, the encryption technology with chaotic technology has greater advantages in the encryption and transmission of images and dynamic images.

When they obtained the above research results, it further stimulated their urgency in the application of chaotic neural networks. Because some characteristics of chaotic networks, such as complexity, can be found through cryptography, they gradually applied to the research network of chaos [8], used in confidential communications. Public key encryption was first provided in 1976 to ensure data integrity. In addition, even if duplicate data packets are not received during the transmission of data information, once a third party (eavesdropper) changes the information of the data packet, the transmitted information cannot be leaked [9]. At present, mobile information threat and static data threat are the two most common information threats in information communication transmission. Among them, information threats against static data generally include the following three areas: first, password guessing threat; second, IP address spoofing attack; and the third type is a specific route attack. The attack on mobile information can be divided into active attack and active attack. The ground adversary (attacker) usually performs specific manipulation on the data stream information transmitted through the network or modifies the information of the whole or partial data stream and then makes an active attack. This method is generally divided into: copying, delaying, and deleting data streams: edit, arrange, insert information, etc. Eavesdroppers usually listen to data transmitted in network communication. It is these technologies that realize the purpose of passive information intrusion. After the attack, the eavesdropper can understand the information of the data, the number of transmissions, and other information. People can establish an Internet security system composed of protection, response, test, and repair. This system maintains the data security of the whole computer network transmission process through the security assurance technology. Therefore, the network security protection system should establish a basic security framework, provide security assurance through the establishment of security technology, form an internal security management mechanism, ensure the normal and effective operation of the Internet, meet the reasonable requirements of users, and maintain security.

The security service mechanism generally relies on password, but it is also realized by security mechanism. At present, experts and scholars in the field of information security in China unanimously point out that comprehensive and efficient information security transmission between computers and the Internet also needs to rely on the mature development of computational cryptography. With the vigorous development of cryptography theory, this major has covered many professional theoretical fields such as bioinformatics, number theory, Lie algebra, and probability theory and is a comprehensive major closely related to microelectronic technology, computer network, and data communication [10]. Through the research, development, and use of new codes such as neural network information, genetic code, particle information, and chaotic information, it has been proved that secrets have great vitality and broad application prospects.

With the rapid development of science and technology, and with the long-term competition and competition between decoding and decoding, the application of cryptography in some advanced scientific and technological fields has gradually evolved into a comprehensive field. Information theory, acoustic, computer, cryptography, electronics, linguistics, and computer technology have a very close and deep relationship with cryptography. Many password systems and deciphering technologies currently adopted by some foreign governments are highly confidential [11].

At present, the question of information security in computer and network communication will be the focus of future network development. The core content of network security is cryptography. Among them, cryptography is the core concept of information security. In the future of Internet communication, in order to adapt to the information security characteristics of real-time communication, we must use an encryption algorithm: first, the secret must be very complex; then, the secret data must be information that can guarantee security [12]. After deciding which encryption algorithm to use, the method needs to realize high-speed operation in parallel and have the shortest encryption and decoding time to ensure instant messaging. In addition to

Table 1: Comparison of traditional cryptography and chaotic cryptography.

Feature	Chaos cryptography	Traditional cryptography
Similarity	Sensitivity to initial value	Diffusion of plaintext information
	Divergence of motion trajectories	Pseudorandomness of ciphertext information
	Diffusion is accomplished by an iterative process	Relying on multiple rounds of encryption to complete the diffusion
	Take the initial parameters as the starting point of evolution	Use the initial key as the starting point for encryption
Difference	The motion space is all real numbers on the range	Limited range

the effective and rapid parallel computing function, the artificial neural network also has some functions of chaotic dynamics, which is more than ideal. Based on the characteristics of chaos technology, it will play an important role in the encryption of digital image data. At present, these application technologies have formed perfect functions and encryption technologies.

At present, in the field of secure communication, the basic theory and application of neural networks are developing rapidly. Many experts and scholars are optimistic about the application prospect of neural network encryption. The wide application of neural network in secure communication has brought a new idea and implementation to the modern Internet in the field of secure communication. It will have more and better research value and more optimistic development prospects [13]. In terms of the current development trend of information technology and security technology, the use of neural networks to make cryptography practical, reliable, and easy to apply has become the main development trend. The research and development of encryption technology will play an increasingly important role.

2. State of the Art

According to the data of relevant institutions, digital images account for about 50% of the current network information content transmission. Compared with text, it is easier to read and attractive. Compared with video, the required technology is simpler, but the transmission speed is faster. It dominates most media-based information dissemination. When such a large-scale digital image is used for information exchange, the consequence will be the gradual development of information attacks on the image. In order to avoid possible information leakage, researchers in relevant fields at home and abroad in China continue to carry out relevant research and obtain some results [14]. In the research on the way of image encryption, it can be divided into different ideas, which are roughly as follows [15].

2.1. Image Encryption Using Matrix Transformation. Because the analysis of digital images in computer technology generally adopts two-dimensional or multidimensional matrix, the technology of digital upconversion matrix has become a key point of image encryption [16]. At present, people have provided a variety of image processing methods based on matrix transformation, such as Arnold's transformation, magic square transformation, and Baker's transformation. These changes can effectively change the positions of adjacent images in the matrix and even completely disrupt the relationship between adjacent pixels in the image [1]. At the same time, with the development of more scientific computing applications, matrix-based computing technology is also growing rapidly. However, this technology also has some shortcomings: in the actual use environment, the statistical data such as the pixels of the digital image cannot be changed. This makes us realize that in the future digital image encryption, the scrambled data may exist in the form of rings, but it still needs to make some changes to the pixel values. The cross-application of chaos theory and digital cryptography not only promotes the development of chaos theory and chaos technology but also completely changes the design method in the field of cryptography and the traditional calculation method. The comparison between traditional key technology and chaotic cryptography is shown in Table 1.

2.2. Image Encryption Based on Transform Domain. Because the method of using matrix transformation has specific reference value, researchers have also provided different solutions. Some researchers in signal processing also adopt the transform domain image encryption method for image encryption to convert small signal data of images into large-frequency interval data, which is a better treatment. At present, the common conversion methods mainly include the Fourier transform and wavelet transform [17]. With this transform domain image processing, people can easily find the key signals of the image, so only these key information can be effectively protected, which is fast and effective. Therefore, on the basis of matrix transformation, it has made a big step forward. At present, the research method of image encryption based on transform domain is also developing, and the new algorithm has good effectiveness and great practical value [18].

2.3. Image Encryption Method Based on Chaos Theory. Chaos theory has good pseudorandomness, high sensitivity to the initial value, and low divergence to the moving path in a given spatial area and is consistent with the low diffusion and key sensitivity required by image encryption. These advantages also prompt us to consider the feasibility of combining chaos theory with image encryption technology. At present, chaos theory has been widely used in the field of image encryption. For example, compound chaotic features

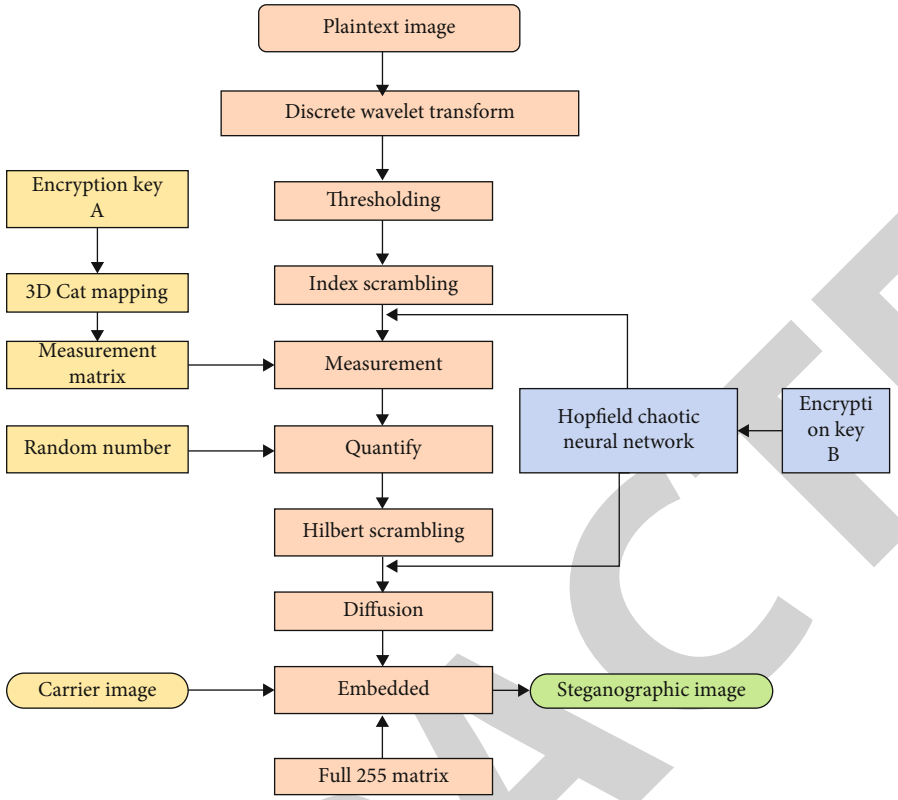

Figure 1: The proposed encryption algorithm flow.

are studied and applied to image encryption, and three-dimensional chaotic features are studied and applied to image encryption. In this paper [19], a one-time pad color image encryption technology based on the Sha-negative three multichaotic system is presented. In recent years, due to the vigorous development of the next generation computer, the neural network technology with complex chaotic characteristics has also begun to receive people's attention. It is a new research hotspot in the process of image encryption [20].

With the development of computer technology, people pay more and more attention to the security of data in the process of using network to realize data interaction. Digital image is one of the important communication methods of multimedia, and its security has become the key and difficult problem of data protection. However, in the current technological development, there are still some defects to be overcome in the chaotic image encryption, such as follows:

(1) When the stream cipher and the block cipher are used simultaneously, the stream cipher only generates strong encryption for the image because of its security logic. However, it is not possible to use information that has a strong correlation with images, such as images. Block cipher is slow because of its security mechanism

(2) In the current scientific research, due to the emergence of new computers, the research of neural networks has entered a period of rapid development. Neural network has excellent association ability and complex processing characteristics, which can meet the demand of chaotic encryption for the rapid diffusion of plaintext signals. However, in the process of combining neural network and chaotic encryption technology, many chaotic technologies are relatively simple or lack of practical application scenarios, which also makes the algorithm face certain security problems

(3) At present, the main research on chaotic neural networks is on the integer order; in addition, there is a discussion on its chaotic function, but there is a lack of more detailed discussion on the hierarchical neural networks. The study of fractional stage system is not only general, but also the integer stage chaotic system is regarded as a special case of fractional stage chaotic system. The best one can be selected after comparison

3. Methodology

3.1. Hopfield Chaotic Neural Network. Hopfield's chaotic neural network was first invented by the American physicist Hopfield in 1982. It is mainly used to imitate the motion mechanism of biological neural networks. The model of three-dimensional Hopfield chaotic neural network is shown in the following formula:

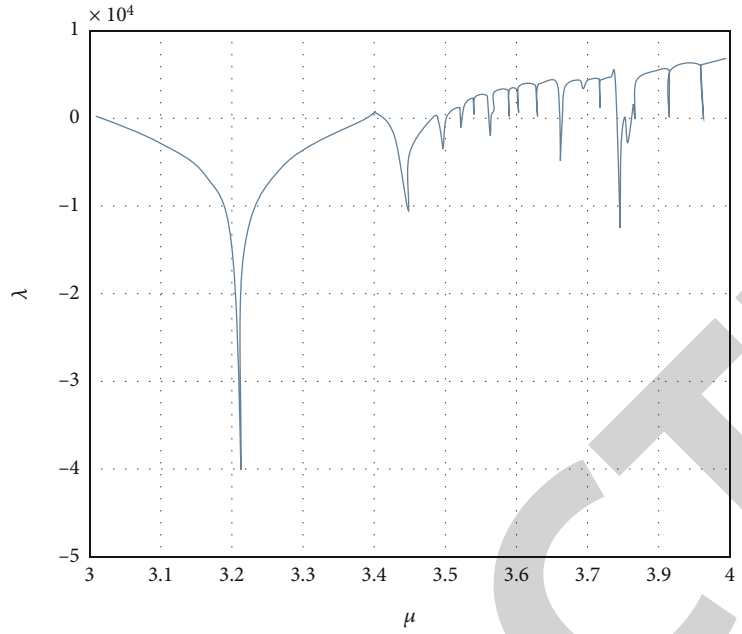

Figure 2: The Lyapunov exponent plot of logistic mapping.

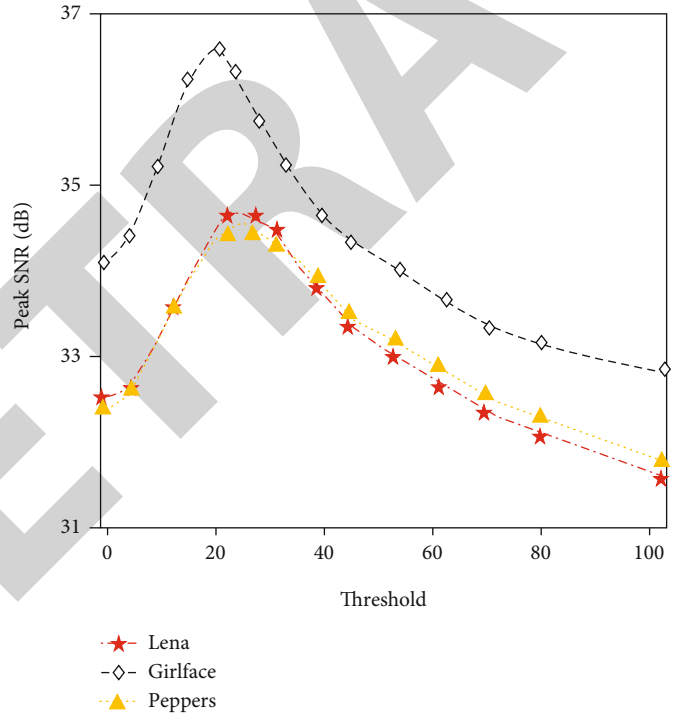

Figure 3: Influence of threshold TS on decryption quality.

$$\begin{cases} x_1' = -x_1 + 2f(x_1) - f(x_2) \\ x_2' = -x_2 + 1.7f(x_1) + 1.7f(x_2) + 1.1f(x_3) \\ x_3' = -x_3 - 2.5f(x_1) - 2.9f(x_2) + 0.56f(x_3), \end{cases} \quad (1)$$

where $f(xi)$ is a hyperbolic tangent function:

$$f(x_i) = \tanh(x_i). \quad (2)$$

3.2. Compressed Sensing Technology. Donoho proposed a new signal sampling theorem based on the sparsity of the signal and named it compressed sensing. For a signal u of length N, it can be linearly represented by a set of sparse basis $\psi = \{\psi_1, \psi_2, \psi, \cdots, \psi_N\}$, that is

$$u = \sum_{i=1}^{N} a_i \psi_i, \quad (3)$$

where $a_i = u, \psi_i$. When $K \ll N$, the signal u is said to be K -sparse in the ψ domain. The compressed signal v is obtained by linear projection of the sparse signal u on the measurement basis, namely

$$v = \Phi u, \tag{4}$$

where $\Phi \in R_{M\times N}$ is the measurement matrix. When the measurement matrix Φ is incoherent with the sparse matrix Ψ, a perfect reconstruction of the sparse signal u can be achieved. In addition, the reconstruction of the sparse signal u can be expressed as solving the l1 norm problem, namely

$$\min \|u\|_1, s.t. v = \Phi u. \tag{5}$$

3.3. Generating Measurement Matrix. The construction of measurement matrix is one of the important foundations of compressed sensing technology, which will directly change the efficiency of reconstructed information. This paper will get the required measurement matrix through three-dimensional cat mapping. The mathematical model of three-dimensional chaotic mapping is expressed as

$$\begin{cases} x_{i+1} = (2x_i + y_i + 3z_i) \bmod 1 \\ y_{i+1} = (3x_i + 2y_i + 5z_i) \bmod 1 \\ z_{i+1} = (2x_i + y_i + 4z_i) \bmod 1, \end{cases} \tag{6}$$

where $[x, y, z]^T$ is the state variable of the chaotic map. Then, the generated chaotic sequence is sampled and combined according to the following formula:

$$w_i = 1 - \frac{2}{3}\left(x_{j+id} + y_{j+id} + z_{j+id}\right). \tag{7}$$

In the formula, j is a fixed positive integer used to eliminate the instantaneous effect of chaotic mapping, and d is the sampling interval.

Finally, normalize the obtained chaotic sequence wn (as shown in the following equation) to obtain the measurement matrix Φ:

$$\Phi = \sqrt{\frac{2}{M}} \begin{bmatrix} w_1 & w_{M+1} & \cdots & w_{M(N-1)+1} \\ w_2 & w_{M+2} & \cdots & w_{M(N-1)+2} \\ \vdots & \vdots & & \vdots \\ w_M & w_{2M} & \cdots & w_{MN} \end{bmatrix}. \tag{8}$$

3.4. Discrete Hopfield Neural Networks. A discrete Hopfield neural network, if it has n neurons, can be represented by the formula $N(T, H)$, and each neuron has and only two states, namely 0 or 1, and can be represented by the following state equation to represent

$$S_i(t+1) = \operatorname{sgn}\left(\sum_{j=0}^{N-1} t_{ij} S_j(t) + h_i\right). \tag{9}$$

Table 2: Correlation of adjacent pixel pairs before and after image encryption.

Correlation coefficients corresponding to adjacent pixels in different directions	Plaintext	Ciphertext
Horizontal direction	0.99524	0.00451
Vertical direction	0.95171	0.00477
Diagonal direction	0.966788	0.00410

Among them, $si(t)$ represents the state of neuron i at time t and the sign function sgn (x) is defined as

$$\operatorname{sgn}(x) = \begin{cases} 1, & x \geq 0 \\ 0, & x < 0. \end{cases} \tag{10}$$

The energy function of the system at time t is:

$$E(t) = -\frac{1}{2}\sum_{i,j=0}^{n-1} t_{ij} S_i(t) S_j(t). \tag{11}$$

Hopfield shows that when the function of a network is declining, but the capacity of the network is only limited, even in the initial state, the network will eventually converge to a stable state, that is, the attractor. By increasing the network weight, the balance and stability can be saved on the Internet in the form of data. However, after the continuous exploration of experts, we found that this is an attractor. In general, the number of storage modes cannot be greater than the maximum storage capacity of the system, because these attractors must converge through the minimum Hamming distance. If the amount of stored information is greater than the storage capacity of the information, then if the capacity of the neural network increases, the function of the whole neural network will also be chaotic, and there will be unpredictable correlation between the attractors in the information. If the connection weight matrix changes, the relationship between the attractor and the corresponding attraction domain also changes.

After introducing the random transformation matrix H, the original initial state s and the absorber s will become the new initial state s and the absorber, respectively:

$$\begin{aligned} \widehat{S}^u &= S^u \times H, \\ \widehat{S}^u &= S \times H. \end{aligned} \tag{12}$$

Figure 1 is the flow chart of the proposed algorithm.

4. Result Analysis and Discussion

4.1. Experimental Data and Environment. In order to verify the correctness of the visual encryption method in this paper, a simulation test was carried out on a desktop computer equipped with 3.0 GHz CPU and 16 GB ram. The simulation platform is MATLAB r2019a. Four 256 pictures were randomly selected × 256 clear text pictures, and 4 512 × 512 carrier images are simulated. In the process of encryption

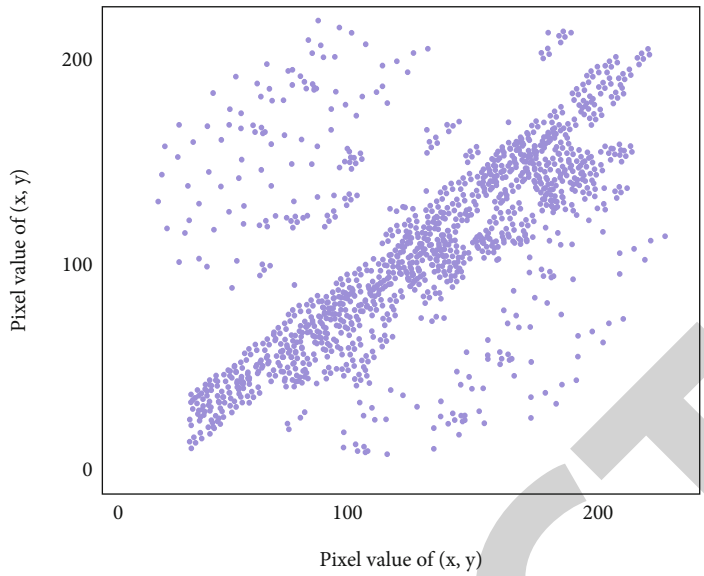

Figure 4: Lateral correlation distribution of Lena images.

and decoding, the key used is set as a: [0.698,0.376,0.976], b: [0.6,0.3,0.7], and $Cr = 0.5$. Other parameters are set as $d = 10$, $TS = 25$, etc. During decryption, OMP technology is used to reconstruct the sparse coefficient matrix. It is difficult to decrypt an image without knowing the keys $x0$ and P. We set the image size to 256×256, the length of the encrypted image $L = 65536$, and the number of possible encryption results is 28 L. This is a fairly high standard. In addition, in the third method of encrypting the chaotic neural network, the signal of Equation (5) is obtained. Based on the chaotic binary structure sequence, the large weights and thresholds of neural networks are specialized. In the signal transformation method, there are two characteristics: (1) a signal value can be transformed into different values; (2) different signal values can be converted into the same value. Therefore, by acquiring some original images and cipher patterns or acquiring some special images and corresponding cipher results, the cipher analyst cannot accurately decipher other cipher patterns.

There is a very clear numerical limit line in the Lyapunov exponent graph of the logistic map, as shown in Figure 2. Therefore, we can find that the exponent of Figure 3 is always equal to zero, indicating that the system is always in a nonchaotic state. With the continuous growth of time, the system has gradually moved to a chaotic state, and there are still some nonchaotic regions. Therefore, in this section, in order to avoid the periodic window phenomenon (3.9, 4), it is adopted in this article. The variation of Lyapunov exponent with time, within the range of 33.57.

4.2. Experimental Results and Analysis. In the calculation of this paper, the threshold will also have a corresponding effect on the quality of the decrypted image. Figure 3 is an action curve of the threshold *ts* on the decryption quality, and the three curves are all expressed as the peak signal-to-noise ratio *psnrdec* between the plaintext picture and the decrypted picture. It can be seen from Figure 3 that the effect of the threshold point on the quality of the decrypted image is inconsistent. When the threshold point is lower than 25, the quality of the decrypted image increases with the increase of the threshold point. But if it is higher than 25, the quality of the decrypted image decreases and continues to drop. Therefore, in order to achieve good decryption performance, the threshold TS must be set between 25. Of course, every valuable image must have a relatively large correlation. In order to increase the image, the correlation within the image should be as small as possible physically, so the correlation coefficient should also be as small as possible (see Table 2 for the measurement results).

Figure 4 shows the correlation distributions of the Lena image and the corresponding ciphertext image in horizontal, vertical, and diagonal directions. It can be seen from Figure 4 that there is a strong correlation between adjacent pixels in the Lena image and a positive correlation distribution. In the generated ciphertext image, the correlation between adjacent pixels is very low, showing a chaotic distribution. In this paper, the asynchronous encryption and decryption algorithm of chaotic neural network changes the explicit mapping of the Henon chaos into the implicit mapping of neural network. Under the input excitation of the same system initial value and control rate, the chaotic neural network of the sender and receiver can asynchronously generate a more hidden and unpredictable chaotic sequence key stream. Simulation results show that the algorithm in this paper can achieve effective convergence of chaotic neural network, can track chaotic sequence efficiently, and has good encryption and decryption effect on plaintext. The asynchronous encryption algorithm has high security and avoids many inconveniences in chaotic synchronous communication, such as requiring strict synchronization between the sending and receiving ends. As shown in Figure 5, when length is 0.25, the value of the Lyapunov exponent is continuously less than 0, with the increase of the value, the Lyapunov index starts to repeat up and down at 0, but the whole

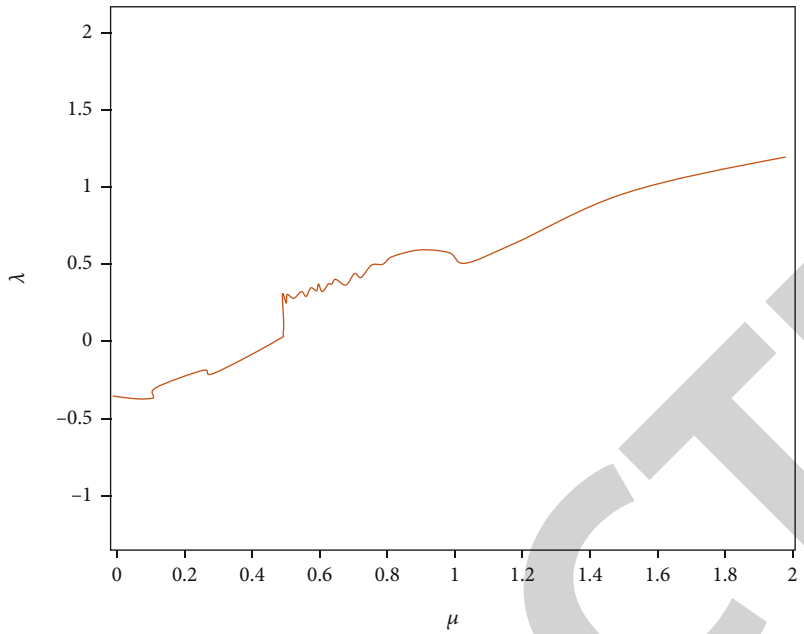

Figure 5: Lyapunov exponent plot of staged composite chaotic map.

Table 3: Random test result.

Type of test	p value	Through the situation
Frequency check (single bit)	0.707255	Pass
In-block frequency test	0.194782	Pass
Run test	0.453389	Pass
Longest run within block test	0.724014	Pass
Binary matrix rank test	0.535871	Pass
Discrete Fourier transform test	0.744492	Pass
Nonoverlapping module match test	0.436871	Pass
Overlapping module matching check	0.802471	Pass
Maurer's universal statistical test	0.850741	Pass
Linear complexity test	0.605880	Pass
Serial test ($P1$ value)	0.981279	Pass
Serial test ($P2$ value)	0.916700	Pass

process is extremely short, because the overall trend of the Lyapunov index is continuously rising, and its length is 0.25 to 0.33. Afterwards, when length is 0.33, the Lyapunov exponent remains greater than 0 and will not fall back.

Because ciphertext is a kind of stream cipher in this paper, it can be checked whether the ciphertext result has a random number sequence by the NIST randomization method. In order to test the randomness of the cryptographic information obtained by the encryption method, the National Institute of Information Technology (NIST) has developed a set of data verification kits, which are composed of 15 different methods. In each test, the p value was recorded, which represents the evaluation value of the random number sequence. If the p value of 15 tests exceeds 0.01, it means that the provided system has passed the randomness measurement with 99% confidence. By measuring the random number sequence of the cipher image obtained, the cipher signal can be measured through the NIST statistical test suite. The calculated p value is listed in Table 3.

The color information of a plaintext image can be interpreted by performing histogram statistics on its pixel values. The histogram is a function graph that counts the number of pixels with the same attribute value in the image. A good encryption process will mask this information, as if the distribution of pixels itself is just some random signal. The pixel value of the encrypted image should be as uniform as possible but not completely in line with the uniform distribution in its pixel range, that is, its ciphertext pixel histogram looks as random as possible. The pixel histogram of each image is different. This experiment analyzes and makes statistics of the pixel (brightness) distribution of the RGB three channels of the Lena map. The pixel value of the encrypted image

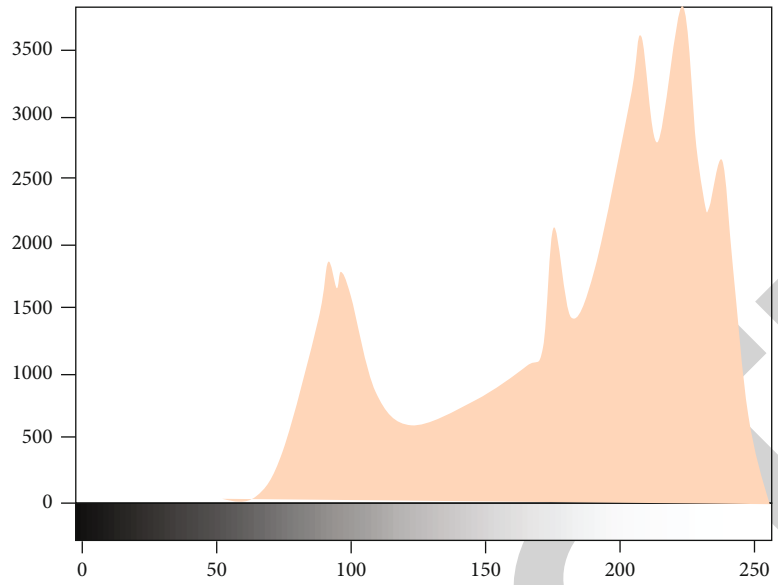

Figure 6: Lena graph R channel histogram.

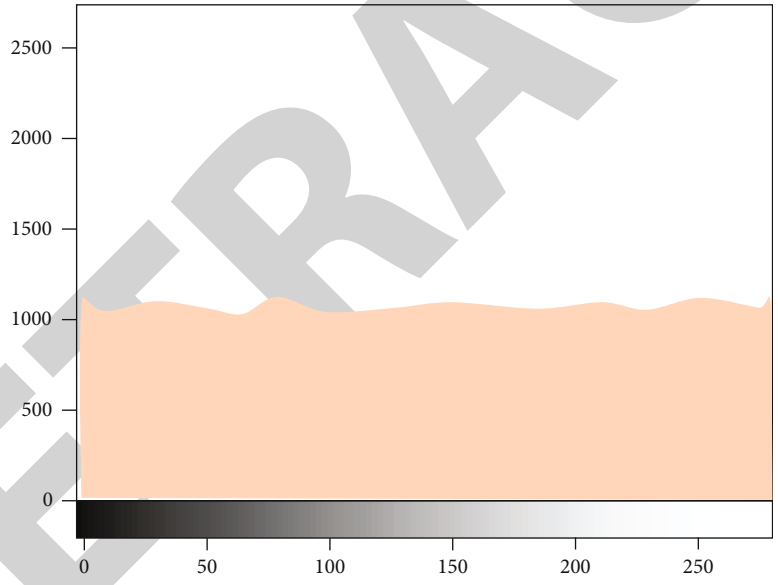

Figure 7: Histogram of ciphertext R channel.

should be as uniform as possible but not completely consistent with the uniform distribution in its pixel interval, that is, its ciphertext pixel histogram should look as random as possible. It can be seen from the results in Figures 6 and 7 that the pixel value distribution of the ciphertext image is obviously more uniform.

5. Conclusion

This paper presents a visual image encryption algorithm based on the Hopfield chaotic neural network and compressed sensing. Different from the existing visual image encryption algorithms, this method embeds the encrypted noise like information directly into the alpha channel of the carrier graphics, thus providing the visual stability of the algorithm. Finally, through simulation experiments and comparative studies, we will find that the image encryption algorithm provided in this paper has the advantages of large encryption space, small risk, good visual stability, high decryption efficiency, and good robustness. In the future research, this paper will also explore and study a variety of image embedding methods to further improve the image transmission quality and reduce the transmission cost. In this paper, the basic knowledge of chaos science is first expounded, and then the detailed method of constructing neural networks using Hopfield orthogonal integral coefficient polynomials is deduced. The asynchronous encryption and decryption method of Hopfield chaotic neural network

is applied to the control system. The simulation results show that this method can achieve the effective convergence of the Hopfield chaotic neural network and can also effectively track the chaotic sequence, which has a good effect on the plaintext encryption and decryption method.

Data Availability

The labeled data set used to support the findings of this study is available from the corresponding author upon request.

Conflicts of Interest

The author declares that there are no conflicts of interest.

Acknowledgments

This work is supported by the Jiangsu Vocational College of Business.

References

[1] Y. Chen, S. Xie, and J. Zhang, "A novel double image encryption algorithm based on coupled chaotic system," *Physica Scripta*, vol. 97, no. 6, article 065207, 2022.

[2] Z. Man, J. Li, and X. Di, "Double image encryption algorithm based on neural network and chaos," *Chaos Solitons & Fractals*, vol. 152, no. 24, article 111318, 2021.

[3] X. Y. Wang, H. H. Sun, and H. Gao, "An image encryption algorithm based on improved baker transformation and chaotic S-box," *Chinese Physics B*, vol. 30, no. 6, pp. 060507–060556, 2021.

[4] S. A. Mehdi, "Image encryption algorithm based on a novel 4D chaotic system," *International Journal of Information Security and Privacy (IJISP)*, vol. 15, no. 4, pp. 118–131, 2021.

[5] A. Baalaaji and R. Bevi, "Design of a novel chaotic neural network based encryption system for security applications," *Journal of the Chinese Institute of Engineers*, vol. 44, no. 5, pp. 424–439, 2021.

[6] J. Bi, S. Yin, and H. Li, "Research on medical image encryption method based on improved krill herb algorithm and chaotic systems," *International Journal of Network Security*, vol. 22, no. 3, pp. 486–491, 2020.

[7] U. A. Bhatti, L. Yuan, and Z. Yu, "Hybrid watermarking algorithm using Clifford algebra with Arnold scrambling and chaotic encryption," *Access*, vol. 8, pp. 76386–76398, 2020.

[8] S. A. Bhat and A. Singh, "A novel image encryption algorithm using multiple encryption techniques for mobile devices," *International Journal of Sensors Wireless Communications and Control*, vol. 81, no. 2, pp. 19–24, 2020.

[9] R. Kahalon, V. Klein, I. Ksenofontov, J. Ullrich, and S. C. Wright, "Mentioning the sample's country in the article's title leads to bias in research evaluation," *Social Psychologicaland PersonalityScience*, vol. 13, no. 2, pp. 352–361, 2022.

[10] F. Yang, J. Mou, Y. Cao, and R. Chu, "An image encryption algorithm based on BP neural network and hyperchaotic system," *China Communications*, vol. 17, no. 5, pp. 21–28, 2020.

[11] Z. Shen, W. Wang, D. Jiang, and X. Rong, "*Visual image encryption algorithm based on Hopfield chaotic neural network and compressive sensing*," *Journal of Computer Applications*, vol. 41, no. 10, p. 2893, 2021.

[12] E. Bashier and T. B. Jabeur, "An efficient secure image encryption algorithm based on total shuffling, integer chaotic maps and median filter," vol. 52, no. 4, pp. 33–38, 2021, https://www.researchgate.net/publication/352282860_An_efficient_secure_image_encryption_algorithm_based_on_total_shuffling_integer_chaotic_maps_and_median_filter.

[13] A. A. Karawia and Y. A. Elmasry, "New encryption algorithm using bit-level permutation and non-invertible chaotic map," *IEEE Access*, vol. 9, no. 4, pp. 1131–1135, 2021.

[14] O. M. Al-Hazaimeh, "A new speech encryption algorithm based on dual shuffling Hénon chaotic map," *Journal of Electrical and Computer Engineering*, vol. 11, no. 3, 2230 pages, 2021.

[15] S. Subashanthini and M. Pounambal, "A new venture to image encryption using combined chaotic system and integer wavelet transforms," *International Journal of Cloud Computing*, vol. 10, no. 1/2, pp. 43–55, 2021.

[16] H. Ora and M. R. Tür, "An effective image encryption algorithm using bit reversal permutation and a new chaotic map," *Gazi university journal of SCIENCE*, vol. 13, no. 1, pp. 1093–1105, 2021.

[17] I. Q. Abduljaleel, S. A. Abdul-Ghani, and H. Z. Naji, "An image of encryption algorithm using graph theory and speech signal key generation," *Journal of Physics: Conference Series*, vol. 1804, no. 1, p. 012005, 2021.

[18] G. Zou, Y. Luo, and Z. Feng, "Research on the extraction of image edge information in convolutional neural networks," *Journal of Physics: Conference Series*, vol. 2083, no. 3, pp. 032015–032026, 2021.

[19] Y. Hu and R. Tian, "Image encryption and decryption based on chaotic algorithm," *Journal of Applied Mathematics and Physics*, vol. 8, no. 9, pp. 1814–1825, 2020.

[20] L. Feng and X. Chen, "Image recognition and encryption algorithm based on artificial neural network and multidimensional chaotic sequence," *Computational Intelligence and Neuroscience*, vol. 2022, Article ID 9576184, 9 pages, 2022.