An image encryption algorithm based on neural network

Xuejun Li, Jiawu Yu*, Huizhen Yan
{yujiawu_dlpu@sina.com}

School of Information Science and Engineering, Dalian Polytechnic University, Dalian 116034, China

Abstract: Chaotic encryption provides a practical method for the confidentiality protection of today's digital images. Aiming at the problem of the secure transmission of image information in the network, an image encryption algorithm based on laser chaotic system and neural network is designed in this work. The phase diagram, Lyapunov exponential spectrum and bifurcation diagram analysis confirmed the chaotic characteristics of the single-mode laser power system. On this basis, the plaintext image is first compressed by the BP neural network, and then the compressed image is chaotically generated and diffused using the chaotic sequence obtained by the single-mode laser chaotic system to obtain the ciphertext image, and finally the histogram, Adjacent pixel correlation, anti-differential attack, information entropy and other aspects to test the security of the proposed encryption scheme. Simulation results show that the image encryption algorithm proposed in this work can not only save the channel bandwidth used in ciphertext transmission, but also have good encryption effect and high security performance.

Keywords: Laser chaotic system, Neural network, Arnold transform, Image encryption

1 Introduction

With the popularization of the digital images have been widely applied in military, medicine, industrial engineering, public security, trademark protection [1], and other fields. Images are stored and transmitted through multiple platforms or channels [2]. Because many images contain private or sensitive information, image security issues have received more and more attention in recent years [3].

Traditional image encryption methods usually treat digital images as binary data sequences, and then use traditional data encryption techniques (such as AES [4]) to encrypt the data sequences. For these reasons, traditional encryption schemes are actually not suitable for image encryption. Chaos has the characteristics of initial value sensitivity, unpredictability and ergodicity. These characteristics make the pseudo-random sequence very appropriate to image

EAI GreeNets 2021, June 06-07, Dalian, People's Republic of China

DOI 10.4108/eai.6-6-2021.2307843

encryption [6]. At present, a variety of image encryption algorithms have been designed by using memristor system [7], chaos theory [8-10], quantum theory [11,12], compressed sensing [13-15], DNA coding [16,17], and other technologies. For example, an adaptive medical image encryption algorithm based on improved chaotic mapping was proposed by Chen et al. [18], which used logistics chaotic mapping to scramble plane images, and at the same time uses a hyperchaotic system to adaptively encrypt sub-blocks. In Literature [19], a new encryption and decryption algorithm was proposed, which used projection transformation to improve the diffusion characteristics of the algorithm. Chai et al. proposed a highly adaptive medical image encryption algorithm, which is mainly based on the replacement of pure images and the Latin square matrix and two-way adaptive diffusion [20]. A new image encryption scheme based on the hidden attractor chaotic system was proposed in the literature [21]. Literature [22] proposed a new image encryption algorithm using chaotic cross-mapping to replace and diffuse the matrix of each image color channel. Niu et al. proposed a new color image encryption algorithm based on the anti-control of fractional-order chaotic system [23]. Literature [24] proposed a chaotic-based parallel encryption scheme, which makes full use of modern computer processors to encrypt images. Literature [25] proposed a three-dimensional fractional discrete Hopfield neural network based on left Caputo discrete increments, and at the same time studied the dynamic characteristics and synchronization characteristics of the neural network, and applied it to image encryption. Zhang et al. designed an image encryption scheme based on an integer domain-like perceptron network. It takes the perceptron network as the core to realize the information storage and dissemination of ordinary images [26]. Liu et al. studied an optical image encryption algorithm based on the hyperchaotic system and public-key cryptography theory by combining double random phase encoding of the Fresnel domain [27].

Compared with traditional chaotic systems, the dynamic characteristics of laser chaotic systems are more complex and more sensitive to system parameters. Therefore, the application of laser chaotic system in secure communication has a good application prospect. Therefore, in this work, a single-mode laser chaotic system is used to generate the pseudo-random sequence of pixel scrambling and diffusion. At the same time, a new digital image encryption scheme is designed by combining the neural network method, Arnold scrambling method, and the diffusion method of adding mode operation.

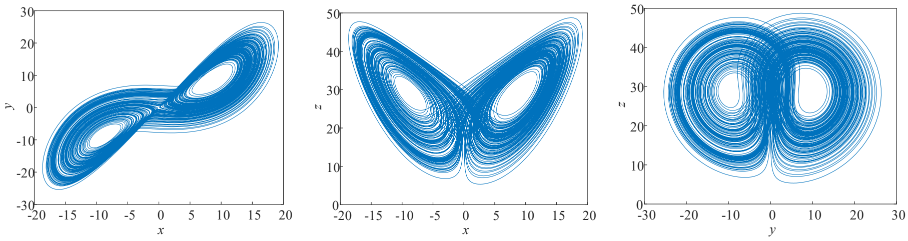
The rest of the paper is arranged as follows: The single-mode laser chaotic system is discussed in section 2. Section 3 introduces the proposed encryption algorithm and decryption algorithm in detail. The encryption and decryption test results and security performance are analyzed in section 4. The 5 section summarizes the work of this article and draws important conclusions.

2 Single-mode laser chaotic system

The equation of the single-mode laser Lorentz system can be described as follows:

$$\begin{cases} \dfrac{dx}{dt} = a(y-x) \\ \dfrac{dy}{dt} = (c-z)x-y \\ \dfrac{dz}{dt} = xy-bz \end{cases} , \tag{1}$$

where a, b and c are the system parameters. Let the system initial x_0=1, y_0=2, z_0=3, the system parameter a=10, b=8/3, c=30, and step length h=0.01. The calculated Lyapunov exponent of the system is (1, 0, -14.79). Among them, there is a positive Lyapunov exponent, and the sum of all values is negative. Therefore, the single-mode laser Lorenz system is a chaotic system. Fig.1 shows the system phase diagrams.

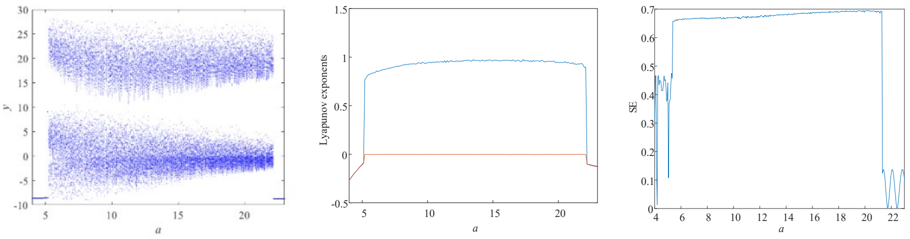


(a) x–y plane (b) x–z plane (c) y–z plane

Fig.1 Phase diagram of single-mode laser Lorenz system

2.1 Influence of different system parameters on dynamic performance

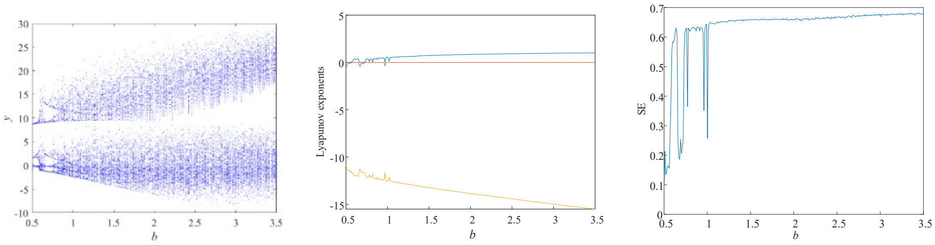
Let parameter b=8/3, c=30, step length h=0.01, initial value x_0=1, y_0=2, z_0=3. When $a \in$ [4, 23], the bifurcation graph, Lyapunov exponent and SE complexity of the system are shown in Fig.2. As can be seen from Fig.2(a, b), when $a \in (4, 5.2) \cup (22.18, 23)$, the system Lyapunov exponent is less than 0, so the system is in a stable state. When $a \in (5.2, 22.17)$, there is a positive Lyapunov exponent and the system is in a chaotic state. Fig.2(c) shows that the complexity of the system is large when it is in a chaotic state. When the system is in a chaotic state, the SE complexity of the system is very high. When the system is in equilibrium, the SE complexity of the system is very low.



(a) Bifurcation diagram (b) Lyapunov exponents (c) SE complexity

Fig.2 Dynamic characteristics of the system at parameter $a \in [4, 23]$

According to the parameters a=10,c=30, step size h=0.01, initial value x_0=1,y_0=2,z_0=3, and $b \in [0.5, 3.5]$, the dynamic characteristics of the system are shown in Fig.3. In Fig.3(a, b), when $b \in [0.5, 0.58) \cup (0.65, 0.73) \cup (0.96, 0.98)$, the maximum Lyapunov exponent is 0, and the system is in the form of periodic motion. The system has a period-doubling bifurcation at b=0.54 and 0.73. When $b \in (0.58, 0.65) \cup (0.73, 0.96) \cup (0.98, 3.5]$, there is a positive Lyapunov exponent, and the system is in a chaotic state. Fig.3(c) shows that the complexity is large in the range of chaotic states, which is in good agreement with the states of bifurcation diagram and Lyapunov exponential spectrum.



(a) Bifurcation diagram (b) Lyapunov exponents (c) SE complexity

Fig.3 Dynamic characteristics of the system at parameter $b \in [0.5, 3.5]$

3 Encryption and decryption algorithm design

3.1 Arnold transform

Arnold transform is also called "Cat transform". It is a chaotic mapping method that performs repeated folding and stretching transformations in a limited area [28]. The digital image can be regarded as a two-dimensional matrix, and the pixel position in the image can be regarded as the position of the corresponding coordinate in the two-dimensional matrix. After Arnold transform, the pixel positions of the image will be rearranged to achieve the effect of scrambling and encrypting the image. Arnold transformation algorithm is realized by formula (2) (positive transformation):

$$\begin{bmatrix}\alpha_{n+1}\\ \beta_{n+1}\end{bmatrix}=\begin{bmatrix}1 & b\\ a & ab+1\end{bmatrix}\begin{bmatrix}\alpha_{n}\\ \beta_{n}\end{bmatrix}\operatorname{mod}(N), \tag{2}$$

where α_n and β_n represent the positions of the image pixels before the transformation, α_{n+1} and β_{n+1} are the positions of the pixels after the transformation, a and b mean the number of current transformations, N is the length or width of the image.

The inverse transformation is shown in formula (3):

$$\begin{bmatrix}\alpha_{n+1}\\ \beta_{n+1}\end{bmatrix}=\begin{bmatrix}ab+1 & \text{-}b\\ -a & 1\end{bmatrix}\begin{bmatrix}\alpha_{n}\\ \beta_{n}\end{bmatrix}\operatorname{mod}(N), \tag{3}$$

The two transformation matrices are reciprocal matrices, and the inverse matrix is still an integer matrix.

3.2 BP neural network

The BP neural network model has three main components, which are layers (input layer, hidden layer, and output layer), neurons, and weights between neurons. The input layer neuron receives the input information and transmits it to each neuron in the hidden layer. The hidden layer neurons are responsible for processing and transforming the received information, and the output layer outputs the processing results. Neurons in each layer are only fully connected to neurons in the adjacent layer, and neurons in the same layer are not connected. The calculation process of each neuron in the BP neural network method is showed in Fig.4. The calculation process of the BP neural network model can be expressed as

$$\hat{Y}=f_{output}\sum_{j=1}^{H}w_{kj}\left(f_{hidden}\left(\sum_{i=1}^{I}w_{ji}X_i+b_j\right)+b_k\right), \tag{4}$$

where I and H mean the number of neurons in the input layer and the hidden layer, X_i is the input information, b_k and b_j mean output layer deviation and hidden layer deviation respectively, f_{output} and f_{hidden} represent the transfer functions of the neurons in the hidden layer and the output neuron respectively, w_{ji} is the weight that connects the input layer and the hidden layer, w_{kj} is the weight between the hidden layer and the output layer.

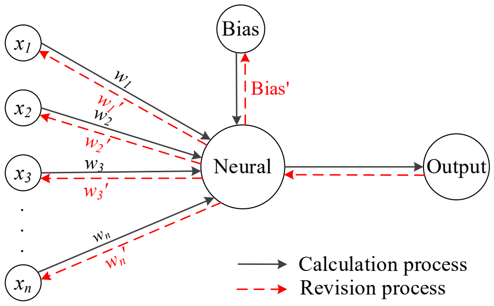


Fig.4 Principle of neuron calculation

The error between the output value and the actual value is measured by Equation (5). If the error exceeds the tolerance, the weight and deviation are corrected by the gradient descent method. The output value is retrained through the modified weight and deviation. The above process is repeated until the output is within the tolerance, which is expressed as

$$E=\frac{1}{N}\sum_{n=1}^{N}\left(Y'_{n}-Y_{n}\right)^{2} n=1,2,3,\cdots,N \ , \tag{5}$$

where $Y^{'}$,$_{n}$ and Y_n represent the predicted output and actual output of the training vector respectively, and N means the number of training samples.

3.3 Encryption algorithm

Assuming the input image size is W×H. Fig.5 shows the image encryption process proposed in this paper, and the specific encryption steps can be described as follows:

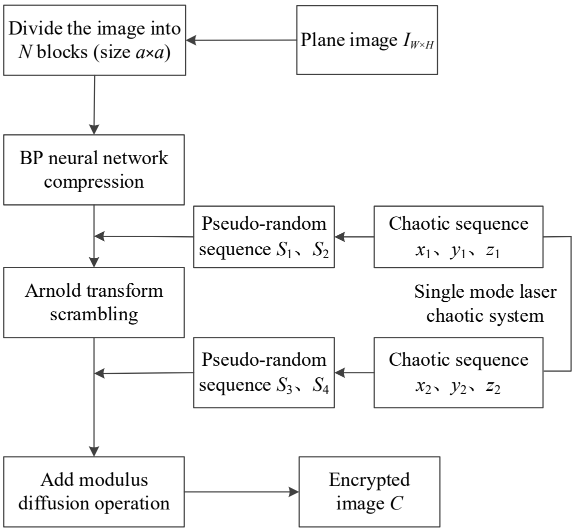

Divide the image into N blocks (size a×a)
Plane image $I_{W\times H}$
BP neural network compression
Pseudo-random sequence S_1、S_2
Chaotic sequence x_1、y_1、z_1
Arnold transform scrambling
Single mode laser chaotic system
Pseudo-random sequence S_3、S_4
Chaotic sequence x_2、y_2、z_2
Add modulus diffusion operation
Encrypted image C

Fig.5 Encryption process

Step 1: Input image $I_{W\times H}$ and divide the image into N sub-image blocks of size $a \times a$.

Step 2: The mean distribution preprocessing is used to normalize the generated sub-image block matrix. The grayscale range of the image to be processed is [x_{min}, x_{max}], and the transformation domain is [y_{min}, y_{max}]. Assuming that the pixel to be processed is x_{value}, then y_{value} can be obtained by the following formula:

$$y_{value} = \frac{\left(y_{\max} - y_{\min}\right)\left(x_{value} - x_{\min}\right)}{x_{\max} - x_{\min}} + x_{\min} \,. \tag{6}$$

Step 3: Use the newff function for training to get compressed data. The transfer function is as follows:

$$\log sig\left(n\right) = \frac{1}{1+e^{-n}} \,. \tag{7}$$

The characteristic of log*sig*(*n*) function is that the data in the range of (-∞, +∞) is mapped to the interval (0, 1), and *n* is the input of the number of neuron nodes.

$$\tan sig\left(n\right) = \frac{2}{1+e^{-2n}} - 1 \,. \tag{8}$$

In the tan*sig*(*n*) function, the output is limited to the interval (-1, 1).

Step 4: Setting the parameters and initial values of the chaotic system, and iterate the chaotic system (t+ $W\times H$) times. The first t values are discarded to avoid interference to the chaotic system. Combine three chaotic sequences x_1, x_2, x_3 to obtain a pseudo-random sequence S of floating-point number type.

Step 5: From the pseudo-random sequence S of floating-point number type, we get the pseudo-random number vector X of integer type length $2WH$, $X_i \in \{1, 2, ..., 10WH\}$. Then two pseudo-random sequences S_1 and S_2 are obtained from X.

Step 6: Convert the image matrix Q compressed by the neural network into a one-dimensional vector T. Pseudo random sequences S_1 and S_2 are used to scramble T. Then the one-dimensional vector is reduced to a $W\times H$ pixel matrix.

Step 7: Similarly, pseudo-random sequences S_3 and S_4 are obtained according to the fifth and sixth steps.

Step 8: pseudo-random sequences S3 and S4 are combined with diffusion algorithm $C_i=(C_{i-1}+S_i+P_i)\text{mod}(256)$ to diffuse pixel values. Among them, the scrambled image is expanded into P, S represents the cipher vector, and the corresponding ciphertext is C, i=1, 2, 3, ..., $W\times H$.

$C_i=(C_{i-1}+S_i+P_i)\text{mod}(256)$ expands as:

$$C_n = \left(C_0 + S_1 + S_2 + \cdots + S_n + P_1 + P_2 + \cdots + P_{\text{n}}\right)\text{mod}\left(256\right) \,. \tag{9}$$

The positive diffusion can be expressed as:

$$C_i = \left(C_{i-1} + S_i + P_i\right)\text{mod}\left(256\right). \tag{10}$$

The reverse diffusion can be expressed as:

$$P_i = \left(2\times 256 + C_i - C_{i-1} - S_i\right)\text{mod}\left(256\right). \tag{11}$$

Step 9: The ciphertext vector *C* can be obtained according to the above formula, and then it is restored to pixel moment. Then the encrypted image *C* is obtained.

3.4 Decryption algorithm

The image decryption process is the reverse process of image encryption. Fig.6 shows the decryption process, and the detailed decryption steps can be described as:

Step 1: Similarly, by the step 6 and 8 of the encryption processes, the pseudo-random sequences S_1, S_2, S_3 and S_4 of the reverse process are obtained.

Step 2: Restore the pixel value by formulas (12) and (13) to obtain the pixel matrix *E*.

The positive diffusion is:

$$C_i = \left(C_{i+1} + S_i + P_i\right)\text{mod}\left(256\right). \tag{12}$$

The reverse diffusion is:

$$P_i = \left(2\times 256 + C_i - C_{i+1} - S_i\right)\text{mod}\left(256\right). \tag{13}$$

Step 3: Combined with the Arnold inverse transform algorithm, the pixel position of the pixel matrix after inverse diffusion is restored to obtain a one-dimensional vector *F*.

Step 4: Restore the pixel value of the one-dimensional vector *F* from [0, 1] to [0, 255], and the vector is restored to $a\times a$ sub-image block.

Step 5: Finally, combine all the sub-images into a complete image to get the decrypted image.

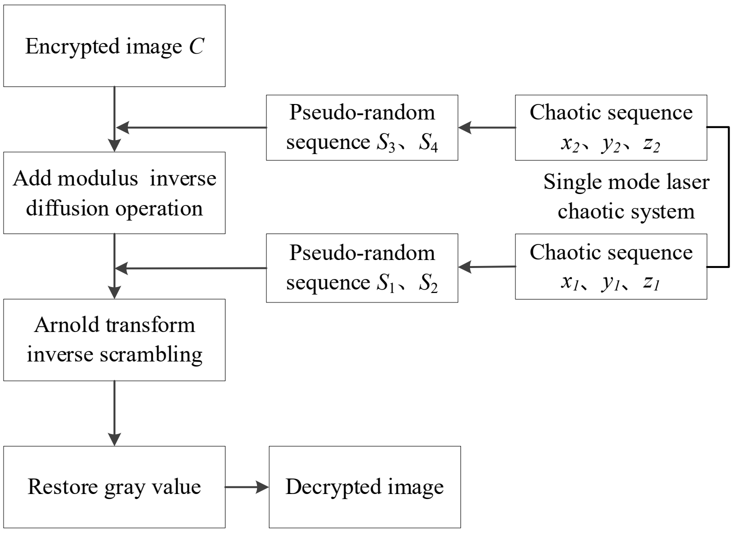
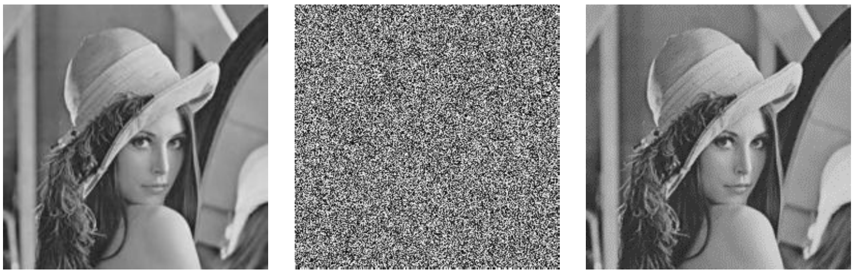

Encrypted image C
Pseudo-random sequence S_3、S_4
Chaotic sequence x_2、y_2、z_2
Add modulus inverse diffusion operation
Single mode laser chaotic system
Pseudo-random sequence S_1、S_2
Chaotic sequence x_1、y_1、z_1
Arnold transform inverse scrambling
Restore gray value
Decrypted image

Fig.6 Decryption process

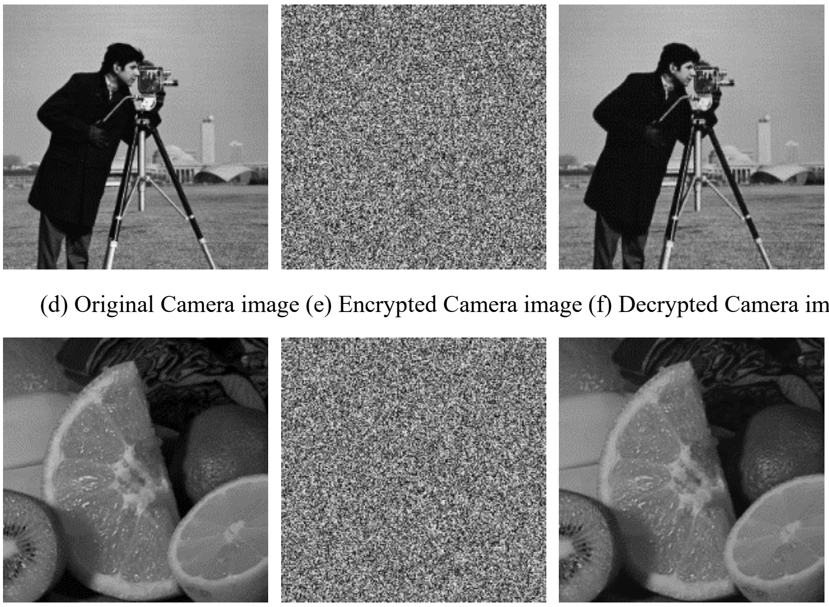
4 Algorithm test results and performance analysis

4.1 Algorithm test results

In this paper, 256×256 grayscale images are selected as the object to test the algorithm performance. The encryption and decryption results obtained by this scheme are shown in Fig.7. As can be seen from Figure 7, the encryption is effective and can effectively mask the information in the plaintext image. At the same time, the decryption algorithm can completely decrypt the ciphertext correctly. Since the security performance of image encryption determines whether the algorithm can effectively resist external attacks, it is necessary to analysis the performance of the encryption scheme through methods such as key sensitivity, histogram analysis, correlation analysis, and so on.



(a) Original Lena image (b) Encrypted Lena image (c) Decrypted Lena image



(d) Original Camera image (e) Encrypted Camera image (f) Decrypted Camera image

(g) Original Fruits image (h) Encrypted Fruits image (i) Decrypted Fruits image

Fig.7 Encryption and decryption test of plaintext image

4.2 Key space

The key space of the image cipher system should be large enough so that the encryption system can resist brute force attacks. The password length should be at least 128bit. In this algorithm, the key is about 292bit, so the key space is about 2^{292}. It can be seen from the comparison of Tab.1 with other encryption algorithms that the encryption system in this paper has a large key space, so it can withstand all kinds of brute force attacks.

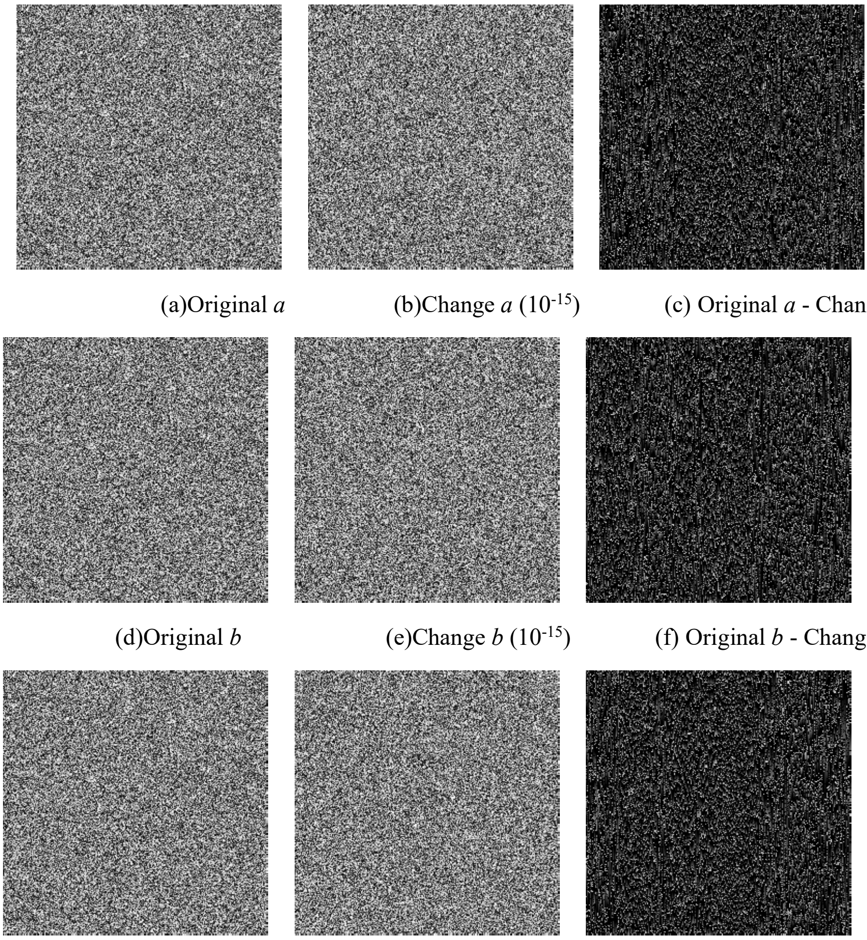
Tab.1 Key space comparison

Our	Ref.[19]	Ref.[21]	Ref.[22]
2^{292}	2^{128}	2^{128}	2^{213}

4.3 Key sensitivity analysis

Key sensitivity is an important characteristic of encryption algorithms. Due to the slight change of the key, the encryption effect will be very different. The degree of this difference can be evaluated by calculating the difference between two different ciphertexts. In this algorithm, sensitivity analysis is performed on keys *a*, *b*, and *c*. When the parameter has a slight change of 10^{-15}, the difference between the new ciphertext image and the original ciphertext image is shown in Fig.8. Fig.8 (c, f, i) shows that when the parameters change slightly, there is a difference between the obtained ciphertext image and the original ciphertext.

The experimental results indicate that the encryption system in this paper is very sensitive to the keys.



(a)Original *a* (b)Change *a* (10^{-15}) (c) Original *a* - Change *a*

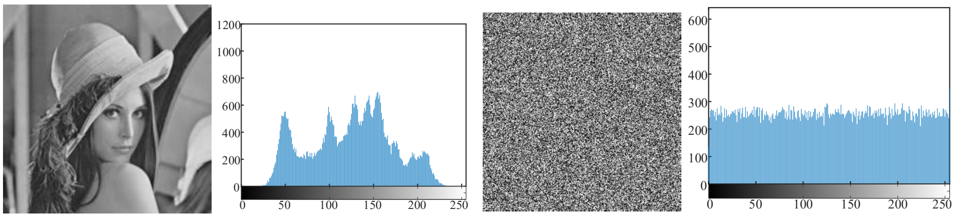
(d)Original *b* (e)Change *b* (10^{-15}) (f) Original *b* - Change *b*

(g)Original *c* (h)Change *c* (10^{-15}) (i) Original *c* - Change *c*

Figure.8 Sensitivity of secret keys

4.4 Histogram analysis

The distribution of image pixels can be expressed by a histogram. It can be seen from the simulation results of the “Lena” image in Fig.9 that the histogram of the plaintext image is not flat. In other words, the image contains the key information of the pixel, and the attacker can easily extract the key information of the image. The histogram distribution of the ciphertext image is relatively flat, which better hides the key information of the image. It indicates that the encryption scheme in this work can effectively resist statistical attacks.



(a)Plaintext of Lena (b) Histogram of plaintext (c) Ciphertext of Lena (d) Histogram of ciphertext

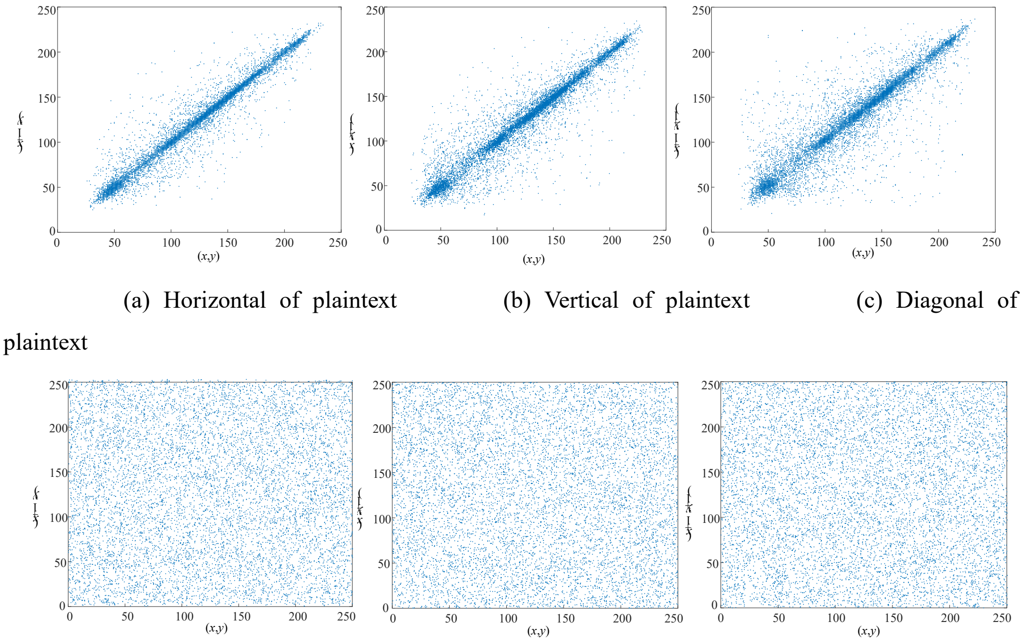
Fig.9 Histogram of original image and encrypted image

4.5 Correlation test

In general, the correlation between adjacent pixels of plaintext images in all directions is very high, so the ability to resist differential attack is weak. Equation (14) can be used to calculate the correlation of adjacent pixels in horizontal, vertical, and diagonal directions.

$$\begin{cases} E(u)=\dfrac{1}{N}\sum\limits_{i=1}^{N}u_i \\ D(u)=\dfrac{1}{N}\sum\limits_{i=1}^{N}\left(u_i-E(u)\right)^2 \\ Cov(u,v)=\dfrac{1}{N}\sum\limits_{i=1}^{N}\left(u_i-E(u)\right)\left(v_i-E(v)\right) \\ r_{uv}=\dfrac{\left|Cov(u,v)\right|}{\sqrt{D(u)}\sqrt{D(v)}} \end{cases}, \tag{14}$$

where u and v are the gray values of two adjacent pixels, $E(u)$ represents the mean value, $D(u)$ is the variance, $Cov(u,v)$ means the covariance, and r_{uv} is the correlation. It can be seen from the experimental results of "Lena" in Fig.10 that the correlation between adjacent pixels of plaintext images is very high, while that of ciphertext images is very low. To further demonstrate the characteristics of correlation coefficients, the comparison results of correlation coefficients are shown in Tab.2. According to Tab.3, it can be seen that the ciphertext image has low correlation. In other words, the encryption algorithm proposed in this article has better anti-attack performance.



(a) Horizontal of plaintext (b) Vertical of plaintext (c) Diagonal of plaintext

(d) Horizontal of ciphertext (e) Vertical of ciphertext (f) Diagonal of ciphertext

Fig.10 Adjacent pixel distribution of Lena image

Tab.2 Comparison of Lena correlation coefficients

Direction	Plaintext	Ours	Ref.[19]	Ref.[21]	Ref.[22]
Horizontal	0.9698	-0.0005	0.0070	0.0004	-0.0055
Vertical	0.9406	-0.0002	-0.0102	0.0013	0.0075
Diagonal	0.9152	-0.0018	0.0030	-0.0023	0.0187

4.6 Anti-differential attack analysis

Minor changes in image pixels are usually measured by NPCR(rate of change in pixel number) and UACI(uniform mean intensity of change). NPCR and UACI are defined as

$$\begin{cases} NPCR=\dfrac{\sum_{i,j} D(i,j)}{W\times H}\times 100\% \\ UACI=\dfrac{1}{W\times H}\left[\sum_{i,j}\dfrac{\left|c_1(i,j)-c_2(i,j)\right|}{255}\right]\times 100\% \end{cases}, \tag{15}$$

where c_1 and c_2 represent two images of size $W\times H$. When $c_1(i, j)\neq c_2(i, j)$, $D(i, j)$=1 can be obtained. On the contrary, if $c_1(i, j) = c_2(i, j)$, then $D(i, j)$=0. The expectations for NPCR and

UACI were 99.6094% and 33.4635%, respectively. Comparison with different algorithms is shown in Table 3. The comparison results in Table 3 indicate that the proposed encryption scheme has good resistance to differential attacks.

Tab.3. Mean values of UACI and NPCR

Algorithm	Ours	Ref.[19]	Ref.[21]	Ref.[22]
NPCR	99.62%	99.62%	99.59%	99.01%
UACI	33.44%	33.56%	33.50%	33.69%

4.7 Information entropy test

The randomness of image information can be reflected by information entropy. The information entropy can be described as:

$$H(s) = \sum_{i=0}^{2^{n-1}} p(s_i) \log_2 \frac{1}{p(s_i)}, \tag{16}$$

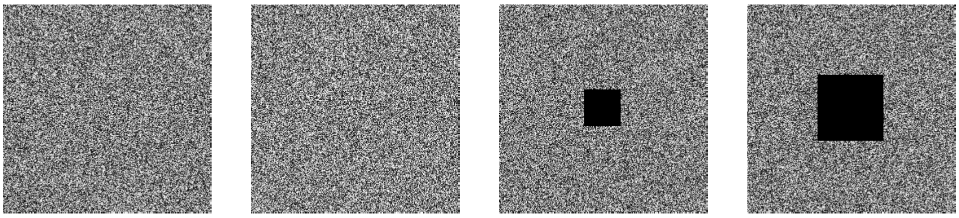
where $p(s_i)$ is the probability of s_i. The expected information entropy of 8-bit grayscale image is 8. According to the comparison of the "Lena" image test results in Tab.4 with the results of other algorithms, the information entropy of the encryption scheme in this work is very close to the ideal value of 8, which has high security.

Tab.4 Information entropy of different algorithms

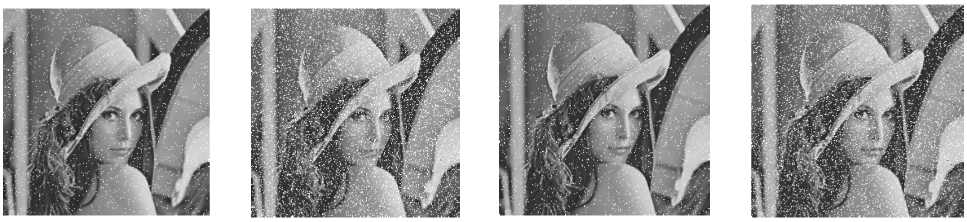
Image	Our algorithm	Ref.[19]	Ref.[21]	Ref.[22]
Lena	7.9960	7.9975	7.9978	7.9564

4.8 Robustness analysis

In the transmission and storage of digital images, different types of noise and data loss are prone to occur. Clipping attacks and noise attacks tests can be used as the evaluation methods of robustness analysis. Figures 11(a)-(d) show the salt and pepper noise attack and occlusion attack of the Lena encrypted image. Figure 11(e)-(h) show the decrypted images of the salt and pepper noise attack and occlusion attack. When the encrypted image loses some data or is blurred by noise, the decryption process can still restore the original image and has a high visual effect. The experimental results indicate that the encryption scheme proposed in this work has good anti-noise and anti-occlusion attack capabilities.



(a) S&P attack wih 1% (b) S&P attack wih 4% (c) data lost with 3% (d) data lost with 10%



(e) Decrypted image of (a) (f) Decrypted image of (b) (g) Decrypted image of (c) (h) Decrypted image of (d)

Fig.11 Robustness analysis

5 Conclusion

An image encryption algorithm based on a laser chaotic system and neural network is proposed in this work. The sensitivity of the laser chaotic system to initial conditions is used to enhance the secret key space and its sensitivity. At the same time, this work combines BP neural network and Arnold transform to effectively reduce the correlation between adjacent pixels of the image and improve the performance of resisting statistics and sensitive attacks. By comparing and analyzing the security with other encryption algorithms, it can be seen that the algorithm proposed in this work has high security. Therefore, this algorithm is suitable for secure communications to protect the secure transmission of digital image information on the Internet and has good practical significance and application prospects.

References

[1] Xu J, Sun B, Yang F, et al. A trademark graphic encryption algorithm based on discrete chaotic system [J]. Journal of Dalian Polytechnic University, 2019, (3).

[2] Mou J, Yang F, Chu R, et al. Image Compression and Encryption Algorithm Based on Hyper-chaotic Map[J]. Mobile Networks and Applications, 2019, (3): 1-13.

[3] Alawida M, Samsudin A, Sen Teh J, et al. A new hybrid digital chaotic system with applications in image encryption[J]. Signal processing, 2019, 160(JUL.): 45-58.

[4] Al. C P E. Understanding Cryptography[J]. Springer-Verlag Berlin Heidelberg 2010.

[5] Hua Z, Xu B, Jin F, et al. Image Encryption Using Josephus Problem and Filtering Diffusion[J]. IEEE Access, 2019, 7: 8660-8674.

[6] Zhu C, Sun K. Cryptanalyzing and Improving a Novel Color Image Encryption Algorithm Using RT-Enhanced Chaotic Tent Maps[J]. IEEE Access, 2018, 6.

[7] Yang F, Luo C, Mou J, et al. Analysis of memory chaotic synchronization based on driver-response synchronization algorithm and coupling synchronization algorithm [J]. Journal of Dalian Polytechnic University, 2019, (3): 229-234.

[8] Yang F, Mou J, Ma C, et al. Dynamic analysis of an improper fractional-order laser chaotic system and its image encryption application[J]. Optics and Lasers in Engineering, 2020, 129.

[9] Wang X, Wang Q, Zhang Y. A fast image algorithm based on rows and columns switch[J]. Nonlinear Dynamics, 2015, 79(2): 1141-1149.

[10] Haibo L, Bin G. Image encryption based on Henon chaotic system with nonlinear term[J]. Multimedia Tools and Applications, 2019, Vol.78 (24): 34323-34352.

[11] Jiang D, Chen Y, Gu X, et al. Efficient and universal quantum key distribution based on chaos and middleware[J]. International Journal of Modern Physics B, 2017, 31(02): 1650264.

[12] Zhou N, Hu Y, Gong L, et al. Quantum image encryption scheme with iterative generalized Arnold transforms and quantum image cycle shift operations[J]. Quantum Information Processing, 2017, 16(6): 164.

[13] Shen Q, Liu W, Lin Y, et al. Designing an Image Encryption Scheme Based on Compressive Sensing and Non-Uniform Quantization for Wireless Visual Sensor Networks[J]. Sensors (Basel), 2019, 19(14).

[14] Yang X, Wu H, Yin Y, et al. Multiple-image encryption base on compressed coded aperture imaging[J]. Optics and Lasers in Engineering, 2020, 127.

[15] Ye G, Pan C, Dong Y, et al. Image encryption and hiding algorithm based on compressive sensing and random numbers insertion[J]. Signal Processing, 2020.

[16] Zhang X, Han F, Niu Y. Chaotic Image Encryption Algorithm Based on Bit Permutation and Dynamic DNA Encoding[J]. Comput Intell Neurosci, 2017, 2017: 6919675.

[17] Wang X, Wang Y, Zhu X, et al. A novel chaotic algorithm for image encryption utilizing one-time pad based on pixel level and DNA level[J]. Optics and Lasers in Engineering, 2020.

[18] Chen X, Hu C J. Adaptive medical image encryption algorithm based on multiple chaotic mapping[J]. Saudi J Biol Sci, 2017, 24(8): 1821-1827.

[19] Li B, Liao X, Jiang Y. A novel image encryption scheme based on logistic map and dynatomic modular curve[J]. Multimedia Tools and Applications, 2017, 77(7): 8911-8938.

[20] Chai X, Zhang J, Gan Z, et al. Medical image encryption algorithm based on Latin square and memristive chaotic system[J]. Multimedia Tools & Applications, 2019, 21.

[21] Wang S, Wang C, Xu C. An image encryption algorithm based on a hidden attractor chaos system and the Knuth–Durstenfeld algorithm[J]. Optics and Lasers in Engineering, 2020.

[22] Abbas A E, Abdulbaqi M A, H. L S. Block image encryption based on modified playfair and chaotic system[J]. Journal of Information Security and Applications, 2020.

[23] Niu Y, Sun X, Zhang C, et al. Anticontrol of a Fractional-Order Chaotic System and Its Application in Color Image Encryption[J]. Mathematical Problems in Engineering, 2020, 2020: 1-12.

[24] Song W, Zheng Y, Fu C, et al. A Novel Batch Image Encryption Algorithm Using Parallel Computing[J]. Information Sciences, 2020: 211-224.

[25] Chen L, Yin H, Huang T, et al. Chaos in fractional-order discrete neural networks with application to image encryption[J]. Neural Netw, 2020, 125: 174-184.

[26] Zhang Y, Chen A, Tang Y, et al. Plaintext-related image encryption algorithm based on perceptron-like network[J]. Information Sciences, 2020, 526: 180-202.

[27] Liu Y, Jiang Z, Xu X, et al. Optical image encryption algorithm based on hyper-chaos and public-key cryptography[J]. Optics and Laser Technology, 2020.

[28] Zhou N, Hu Y, Gong L, et al. Quantum image encryption scheme with iterative generalized Arnold transforms and quantum image cycle shift operations[J]. Quantum Information Processing, 2017, 16(6):164.