IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 28 September 2022, accepted 3 November 2022, date of publication 14 November 2022,
date of current version 12 December 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3221804

RESEARCH ARTICLE

Color Image Encryption Algorithm Using DNA Encoding and Fuzzy Single Neurons

YAOQUN XU[1,2] AND MENG TANG[2]
[1]School of Systems Engineering, Harbin University of Commerce, Harbin 150028, China
[2]School of Computer and Information Engineering, Harbin University of Commerce, Harbin 150028, China

Corresponding author: Meng Tang (tm@s.hrbcu.edu.cn)

The work of Yaoqun Xu was supported by the Natural Science Foundation of Heilongjiang Province through the Project "Chaotic Neural Network Based on Self-feedback Delay and its application" under Grant LH2021F035.

ABSTRACT In order to hide image information more efficaciously, improve the radio of workpiece and quality of encryption, this paper proposes delayed chaotic neuron dynamical system, extracts a single neuron research model to determine its dynamic properties, analyzes the model's sensitivity, stability and the randomness of the chaotic sequence, and verifies its dynamics feasibility of combining the system with DNA encoding. The single delay neuron can simulate the unknown dynamic behavior and capability in the model in a certain sense which can effectively improve optimization ability and con-vergence speed of the neural to make the network more practical. DNA encoding also offers new train of thoughts and directions for the study of cryptography. In addition, by introducing the functional form of fuzzy number can further enhance the stability and adaptability of chaotic system in un-certain environment, and get more distinct chaotic phenomena. The experimental simulation and comprehensive data analysis of the algorithm are carried out in this paper. The data manifest that the system has a large chaotic range, can pass the randomness test of NIST and TestU01, has high complexity and sensitivity which could effectively avoid noise attacks. The encrypted information entropy of classical images can reach 7.9998, which confirms that it can effectively and safely realize the encryption of digital images.

INDEX TERMS Self-feedback delayed chaos, single neuron dynamical system, fuzzy numbers, DNA encoding, image encryption algorithm.

I. INTRODUCTION

Chaos represents simple confusion and disorder in the sense of life, while in the sense of science [1] it is an intricate dynamic action in a deterministic system without rules. Theoretically speaking [2], chaos represents the simple and refined natural rules that actually exist in random phenomena. It displays a nonlinear dynamic behavior, which represents the widely existing cooperative and consistent laws in the same category of problems. American meteorologist Lorenz first proposed the existence of chaotic systems in 1963; American mathematician and founder of information theory Shannon pointed out in 1994 in "Communication Theory of Social Systems" [3] that a chaotic system obtained by specific means the random sequence related to the key, if the initial value is given an extremely small difference, the random sequence will inevitably become very different, and this sequence can be used in the image encryption process. As a nonlinear dynamical system, the chaotic system [4] can fully reflect the randomness existing in the deterministic dynamic system, which is highly susceptible to the initial factors. It has sequence randomness, ergodicity, and determination of non-deterministic systems. This feature makes it natural to have similarities with cryptography, so there are many articles using it to combine with the field of cryptography.

Since the 1990s, the existence of biological chaotic properties of real neurons has led to new thinking, the chaotic dynamics made use of the Hopfield neural network. Aihara and Chen et al. proposed novel chaotic neural network model [5] can continuously and effectively avoid the situation that the neural network drops into a local minimum point. In the literature [6], the simulated annealing algorithm is imported for the model of chaotic network, so that the self-feedback varies from linear to the nonlinear term, which shows a better

The associate editor coordinating the review of this manuscript and approving it for publication was Jun Wang.

state of chaos. Similarly, self-feedback, as the key to the evolution of chaotic neural network, is also an important aspect of research, and its different forms will lead to different chaotic dynamic evolution behaviors. The Bessel function has high nonlinearity and good function approximation ability which presents a non-monotonic but overall increasing form after being combined with the sigmoid function and meanwhile compared with the monotonous increase, the degree and state of chaos are more complex and unpredictable. Therefore, we choose this combination to build a new chaotic neuron model.

After Chen Zhisheng et al. proposed the drive-response synchronization method in 2005, Zhang Tingfang et al. proposed the linear and nonlinear feedback control method in 2006, and Chen Baoying et al. proposed the adaptive control method [7], delay and synchronization are hot spots in the debate on nonlinear dynamics. At pre-sent, most domestic and foreign researchers just stop at improving the self-feedback model with no delay. There are few studies that incorporate both self-feedback and delay into chaotic neural networks also lack of effective neuron dynamics analysis mechanisms. Simulation experiments found that in a chaotic neural network with lag, a single delay neuron can simulate the unknown dynamic behavior and capability in the model in a certain sense by delaying the dynamics and speeding up the neuron reaching the saturation state, which can effectively improve optimization ability and convergence speed of the neural to make the network more practical. Therefore, this paper put forward to combine the time delay neural network with the Bessel self-feedback function, and blur the neurons will lead to more distinct chaotic phenomena to make more full use of the dynamic information units in the time delay and its self-learning ability. Fuzzy refers to indistinctness and dialectics in an intermediate transition state, while fuzzy numbers combine the rigor of mathematics with the reality of life, which can validly on behalf of the information which is difficult to be represented by exact numerical values, and can also agilely converted to another fuzzy number, so as to settle the issues in many areas. The extensive research of fuzzy numbers in various fields also promotes its development in dynamical systems.

In cryptography, DNA can not only be used to store and transmit information, but also can be used for algebraic calculations. Therefore, these few years, DNA-based encryption methods have been gradually applied in the literature of image encryption algorithms [8]. Deoxyribonucleic Acid (DNA) is a nucleic acid in biological cells that has genetic instructions acting on cellular functions, biological organisms and virus growth and development, which is used to guide development of biology and the operation of life functions. DNA is made up of four types of ''nucleotide'' molecules, A (adenine), T (thymine), C (cytosine) and G (guanine), the bases in these four types of nucleotides are complementary and together can create chemical bonds. Subject to the high-quality experimental requirements and precise computing power of DNA cryptography, this paper does not use real biological DNA molecules to perform the encryption process, but instead chooses a pseudo-DNA cryptographic method that relies on the basic central dogma of biomolecules. This method is experimentally simulated for the main process, and follows the basic central dogma of the transfer of biological genetic information between macromolecular cells. After theoretical analysis and experimental simulation, it is determined that it has high efficiency in three basic aspects of calculation, storage and transmission, strong resistance to noise attack methods of digital images. Liu and Liu et al. [9] began to use DNA sequences and low-dimensional chaotic systems to operate and encrypt digital pictures, but the key stream was difficult to achieve the required randomness. In 2020, on the basis of DNA encoding, an encryption algorithm combined with the spatiotemporal chaotic system is proposed by Kang and Guo [10], but the information entropy in the encryption effect only reaches 7.9980. Although this method can be used in cryptography to in-crease its security and speed, it also needs to be enhanced expansion and changed on the basis to improve its security, stability, feasibility and practical application.

In this paper, a discrete representation method of single-neuron dynamic system is extracted from fuzzy time delayed self-feedback neural network and incorporated into the enhanced single-neuron dynamic system. Based on DNA encoding and fuzzy delayed self-feedback chaotic neurons, a new encryption algorithm of color image is simulated and the effect of the algorithm is analyzed. The randomness of the key stream can pass the NIST and TestU01 test, and the information entropy of the encrypted graph reaches 7.9998, other simulation results can also meet the corresponding requirements after analysis.

The remaining work of the paper is constituted as follows: Second section proposes preliminary model of neuron and seeks improvements and enhancements on the model. In Section 3, on the basis of the second section, an image encryption algorithm combined with DNA encoding is proposed. Section 4 analyzes the effect of encryption algorithm in various evaluation indexes. In the end, Section 5 concludes this paper and discuss on future work.

II. PRELIMINARY OF NETWORK

A. THE MODEL OF NETWORK

There are a lot of HD chaos is applied to image encryption scheme, but the password system has also been password analysis, so as to enhance the security of the cryptosystem, overcomes the defects that exist in the chaotic system, put forward a lot of remedial measures, or more mapping to expectations by raising the precision coupling chaos way to reduce the influence of degradation. In this paper, it is proposed that the model of chaotic network with Bessel function and delay can be expressed as:

$$x_i(t) = \frac{1}{1 + \exp(-y_i(t-1)/\varepsilon_0)} \tag{1}$$

$$y_i(t) = ky_i(t+1) + \alpha \cdot \left[\sum_{j=1, j\neq i}^{n} w_{ij} x_j(t-1) + I_i \right] - Z(t) \tag{2}$$

$$Z(t) = z_i(t) - f(x_i(t-1) - I_0) \tag{3}$$

$$f(u) = \lambda V_0(au) \tag{4}$$

$$V_0(au) = \sum_{k=0}^{\infty} (-1)^k \frac{1}{k!\Gamma(k+1)} \left(\frac{au}{2}\right)^{2k} \tag{5}$$

$$z_i(t) = (1-\beta) z_i(t-1) \tag{6}$$

Among them, $x_i(t)$ and $y_i(t)$ are the input and output of the neuron i at the moment t. Due to the time delay, the input and output of the neuron i at the previous moment $t-1$ is expressed as $x_i(t-1)$ and $y_i(t-1)$. $f(u)$ is the term for self-feedback which introduces the Bessel function, $V_0(au)$ is Bessel function, a is the expansion factor of $V_0(au)$, λ is the combination coefficient of the feedback function.

Compared with the self-feedback term with linear, the self-feedback term introduced by the nonlinear Bessel function enables the system show new kinetic characteristics. The self-feedback function curve is shown in Fig. 1.

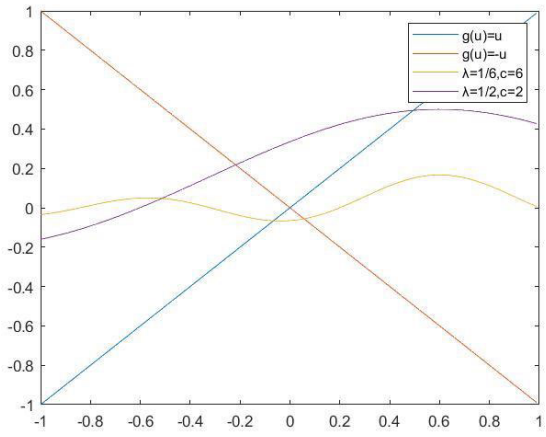


FIGURE 1. Curve of different Self-feedback terms.

B. NEURON MODEL

Extract a single neuron model from the network model, which can be expressed as:

$$x_i(t) = \frac{1}{1 + \exp(-y_i(t-1)/\varepsilon_0)} \tag{7}$$

$$y_i(t) = ky_i(t+1) - Z(t) \tag{8}$$

$$Z(t) = z_i(t) - f(x_i(t-1) - I_0) \tag{9}$$

$$f(u) = \lambda V_0(au) \tag{10}$$

$$V_0(au) = \sum_{k=0}^{\infty} (-1)^k \frac{1}{k!\Gamma(k+1)} \left(\frac{au}{2}\right)^{2k} \tag{11}$$

$$z_i(t) = (1-\beta) z_i(t-1) \tag{12}$$

The single neuron model is simulated, and the single neuron dynamical system dynamic behavior [11] is analyzed,

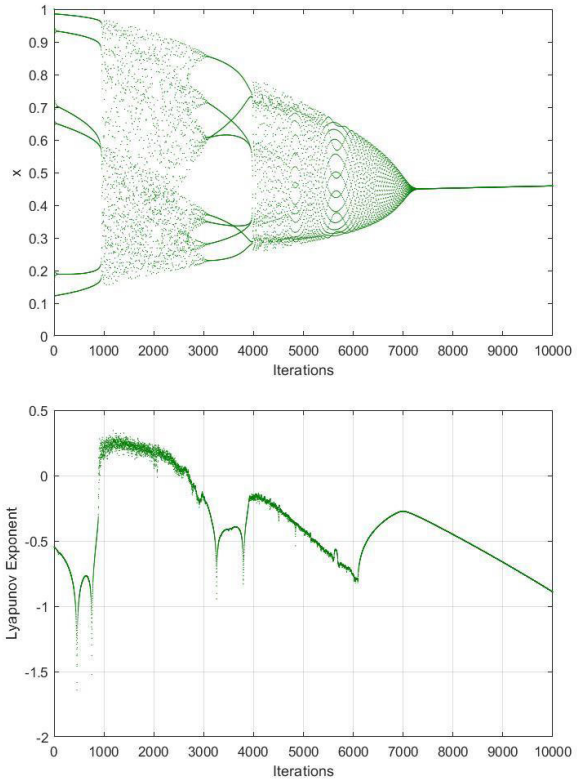


FIGURE 2. Time evolution diagram of single neuron model.

and the parameter values k=0.2, $z = 0.1$, $\varepsilon_0 = 0.004$, $I_0 = -0.1$, $\mu = 0.1$ are taken respectively. The parameter λ is a constant value of 1/6, and the parameter a is a constant value of 6, and the time evolution graph after 10,000 iterations of single neuron and enhanced single neuron is shown in Fig. 2.

The above time evolution diagram can reflect that the model has momentary chaotic dynamic behavior of chaotic network, which reflects its chaotic search capability to a certain extent. When three of the four parameters are kept constant, the influence of the parameter on the dynamic behavior of system can be observed by changing one of the parameters, and the corresponding the evolution of the Lyapunov exponent can be drawn. to analyze its dynamic characteristics. The influence of parameters k, z, ε_0, I_0 on the pattern is shown in Fig. 3.

C. IMPROVING THE SYSTEM

Embedding into the framework proposed by Abd El-Latif et al. [12], enables the realization of enhanced single-neuron dynamical systems (ESNDS), the value of $x_i'(t)$ can be obtained by calculating an intermediate value on the value of the parameter $x_i(t)$. For the article, the parameter n is a constant value of 16. The above system is expressed as the following formula:

$$\begin{cases} x_i(t) = \dfrac{1}{1 + \exp(-y_i(t-1)/\varepsilon_0)} \\ x_i'(t) = 2^n \cdot x_i(t) - floor(2^n \cdot x_i(t)) \\ y_i(t) = ky_i(t-1) - Z(t) \end{cases} \tag{13}$$

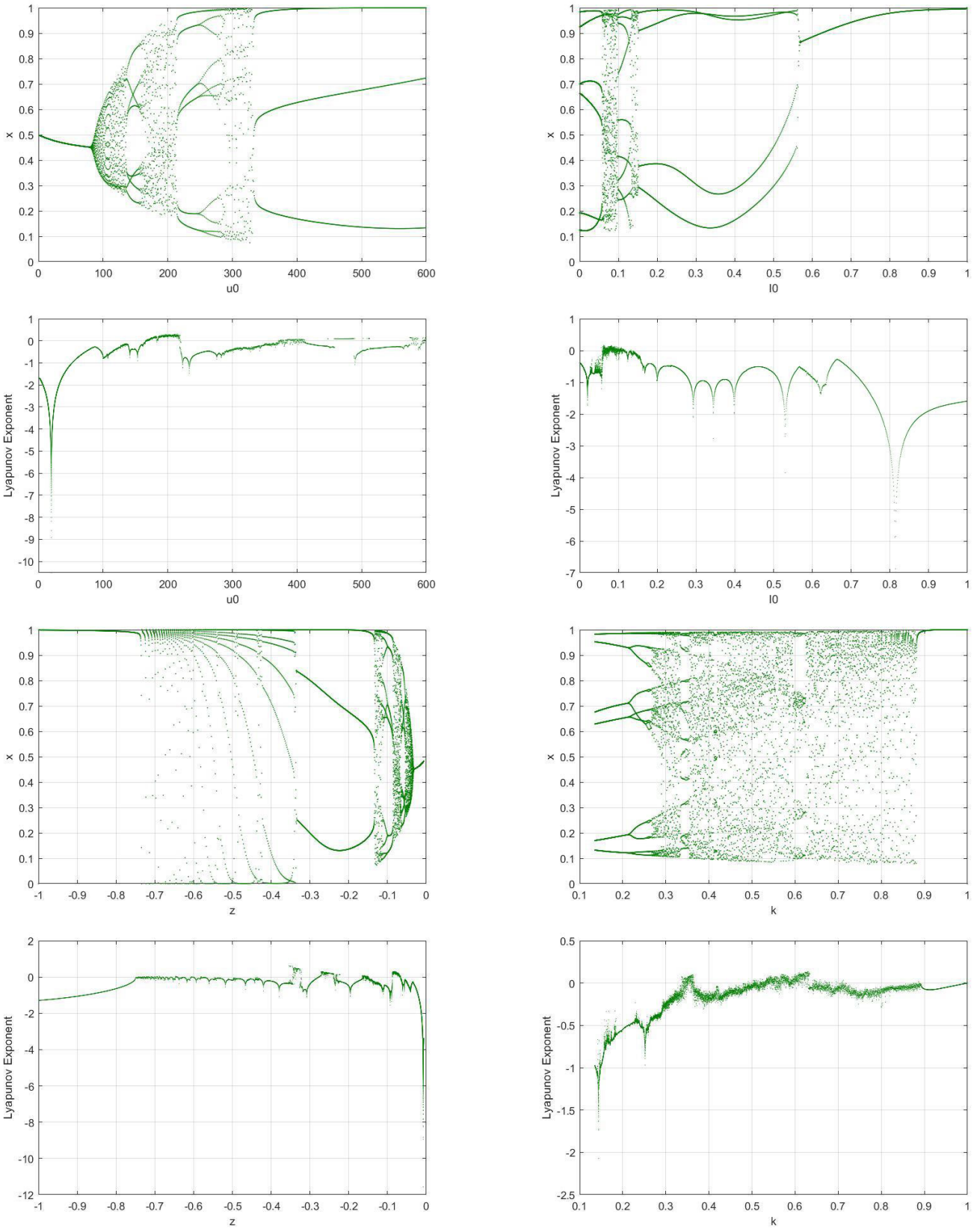


FIGURE 3. Evolution diagram of function x by fix three of four parameters k=0.2, $z = 0.1$, $\varepsilon_0 = 0.004$ and $I_0 = -0.1$ when $\mu = 0.1$.

The concept of fuzzy number is introduced in the above system, and the triangular fuzzy function with relatively few parameters is selected in the trapezoidal approximation and triangular approximation to combine with the single-neuron dynamical system, which further improves its applicability and stability, and shows more complex and distinct chaotic phenomena., and the equation is expressed as follows:

$$g(x) = \begin{cases} \dfrac{x_n}{\mu}, & 0 \le x_n < \mu \\ \dfrac{1 - x_n}{1 - \mu}, & \mu \le x_n < 1 \end{cases} \tag{14}$$

The enhanced expression of the above neurons is combined with the fuzzy function to simplify its expression as follows:

$$\begin{cases} x_i(t) = g\left(\dfrac{1}{1 + \exp(-y_i(t-1)/\varepsilon_0)}\right) \\ x_i'(t) = 2^n \cdot x_i(t) - floor(2^n \cdot x_i(t)) \\ y_i(t) = k y_i(t-1) - Z(t) \end{cases} \tag{15}$$

The dynamics of the improved system is analyzed, from the Lyapunov exponent, it is obvious that the chaotic state is not continuous, and there may be moments of entering and exiting the chaotic state.

D. TEST FOR RANDOMNESS

1) NIST TEST

According to the literature [13], the randomness of the chaotic sequence can have a great impact on the efficiency and effect of image encryption. So as to prove the robustness of the network and its development prospect in image encryption Randomness of random sequences, using the NIST SP800-22 test standard [14], utilizing the 15 statistical packages in the NIST test, which focuses primarily on existing non-random sequences of various types. Some experiments can be sprained into seed experiments, produced by the value of the parameter the binary number used for testing in (15), the first 10 decimal places are removed, and then compared with 0.5, the process is as (16) and (17) as shown:

$$q_i = (10^{10} \times x_i') \bmod 1 \tag{16}$$

$$p_i = \begin{cases} 0, 0 \le q_i \le 0.5 \\ 1, 0.5 \le q_i \le 1 \end{cases} \tag{17}$$

In testing, 15 subsets are considered, each of which will output a p-value. In case of the value is greater than 0.01 as expected value, the series is thought to be evenly distributed. We prepared one hundred sets of 1,000,000-bit binary sequences for testing, during which the parameter original value was a constant value: $k = 0.2, I_0 = -0.1, z = 0.1, \varepsilon_0 = 0.004$. Because the p-values of the 15 subsets are all greater than 0.01, this sequence is considered to meet the required randomness, and the randomness are listed in Table 1.

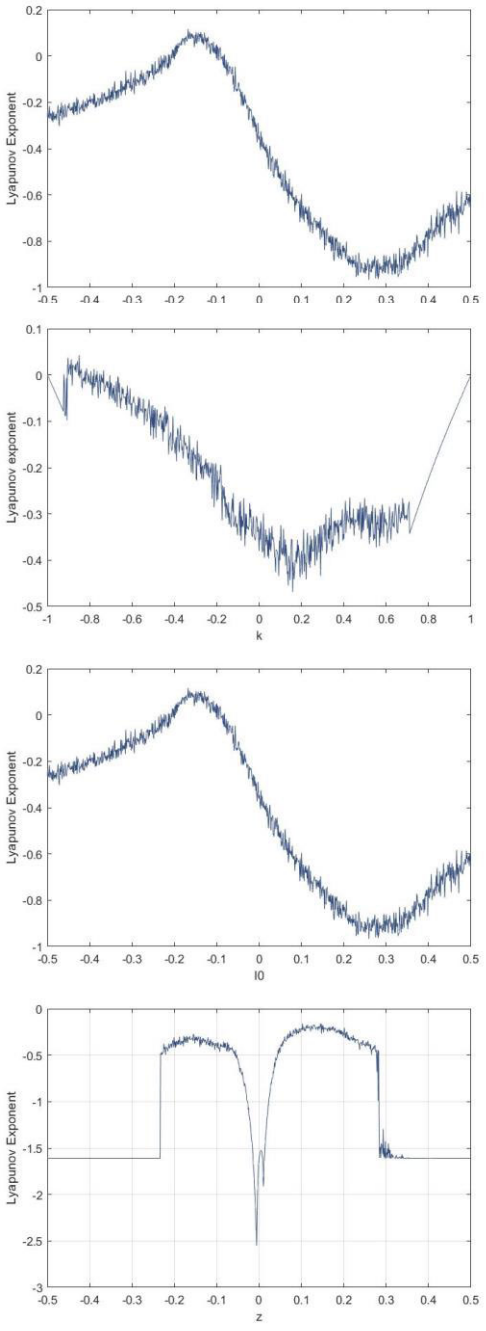


FIGURE 4. Evolution diagram of function x by fix three of parameters k=0.2, $z = 0.1$, $\varepsilon_0 = 0.004$ and $I_0 = -0.1$ when $\mu = 0.1$, $n = 16$.

2) TESTU01

To further verify the randomness of the sequences, we chose TestU01 to examine the sequences generated by ESNDS. As an empirical statistical test set, TestU01 can effectively evaluate the randomness of sequences. It is common that the length of binary sequences, used of the test, is close to 3×10^7 bits. We chose four predefined batteries to verify the bitstream of the sequences in the experiment and the results is shown as Table 2. It proves that bits have fairly strong randomness the dynamical system is relatively effective.

TABLE 1. Analysis of NIST test.

No.	Subset	p-Value	Proportion	Result
1	Freq.	0.678686	99/100	Random
2	Block Freq.	0.678686	99/100	Random
3	Cumulative Sums.	0.115387	100/100	Random
4	Runs	0.334538	100/100	Random
5	Lon. Run	0.554420	99/100	Random
6	Rank	0.514124	100/100	Random
7	FFT	0.474986	98/100	Random
8	Non-Over. Temp.	0.987896	100/100	Random
9	Over. Temp.	0.162606	100/100	Random
10	Universal	0.129620	100/100	Random
11	Appr. Entropy	0.045675	100/100	Random
12	Ran. Exc.	0.900104	100/100	Random
13	Ran. Exc. Var.	0.900104	99/100	Random
14	Serial	0.637119	100/100	Random
15	Linear Complexity	0.897763	99/100	Random

TABLE 2. Analysis of TestU01.

Battery	Length	Consequence
FIPS_140_2	10^9	Passed
Rabbit	2^{20}	Passed
Alphabit	10^9	Passed

III. DNA ENCODING RULES

There are four varieties of molecules constitute DNA: A (adenine), T (thymine), C (cytosine), G (guanine), which is called ''nucleotides''. According to the principle of base pairing [15], A and T are supplementary bases, C and G are also supplementary bases. Corresponding to the complementary principle of 0 and 1 in the binary system, it can be known that 00 and 11, 10 and 01 are also supplementary binary numbers respectively. If we use the four basic nucleotides (A, C, G, T) to represent the four binary numbers 00, 01, 10, 11, there are 4 in total! = 24 encoding regulations. But there are only 8 regulations listed in Table 3 can satisfy the Watson-Crick complementarity demand and be valid. Based on these rules, we can read the pixel value of the image, convert it to 8-bit binary number, and then DNA-encode it to get four 2-bit DNA sequences. The opposite approach of the encoding can be used to DNA decoding rules. According to the above regulations, some biological and algebraic calculations (addition, sub-traction and XOR operations, for instance) could apply to DNA sequences. Table 4 lists the results of three kinds of operations performed on DNA sequences according to Rule 1 in Table 3 respectively.

IV. IMAGE ENCRYPTION PROCESS

Step 1: The original color image of size M×N×O is read into a matrix A (M, N, O), all elements in matrix A (M, N, O) are consistent to pixel value of the graphic dot.

Step 2: Encrypt the chaotic sequences received by the above-mentioned enhanced neural network iteratively, and the security key consists of four parameters of the neural network model. We can do (M×N+M+N+H) number of iterations, then drop the previous H data, ultimately, we get a new sequence L of length (M×N+M+N).

TABLE 3. DNA encoding rules.

Regulations	No. 1	No. 2	No. 3	No. 4	No. 5	No. 6	No. 7	No. 8
00	A	A	T	T	G	C	C	C
01	G	C	G	C	A	A	A	T
10	C	G	C	G	T	T	T	A
11	T	T	A	A	C	G	G	G

TABLE 4. DNA algorithm rules.

1)DNA addition					2)DNA subtraction					3)DNA XOR				
+	A	T	C	G	-	A	T	C	G	⊕	A	T	C	G
A	A	T	C	G	A	A	G	C	T	A	A	T	C	G
T	T	C	G	A	T	T	A	G	C	T	T	A	G	C
C	C	G	A	T	C	C	T	A	G	C	C	G	A	T
G	G	A	T	C	G	G	C	T	A	G	G	C	T	A

Step 3: Original matrix is encoded by DNA to obtain a pseudo-DNA sequence made up by four bases (A, T, C, G) with a length of (M×N×O), and the pseudo-DNA generated by encoding after iteration with the network model. The sequence is XORed to obtain a new pseudo-DNA sequence A of the same length. There are eight rules for DNA encoding, which are represented by numbers 1-8. The random rules are generated by the following formula:

$$r(i) = (L(i) \times 255) \bmod 8 \tag{18}$$

Step 4: Given key P is mapped to a chaotic random sequence by the model. The generative sequence from the chaotic neural network model with the given initial value and parameters, and is encoded as a pseudo-DNA sequence B by DNA.

Step 5: performing DNA addition operation on the pseudo-DNA sequence A obtained by XOR and the pseudo-DNA sequence B after mapping and encoding to obtain pseudo-DNA sequence C.

Step 6: After the pseudo-DNA sequence C is decoded by the same random rules of DNA, it is converted from an 8-bit binary number to a decimal number, and is output as a final encrypted image through a public channel.

The above process is shown in Fig. 5. The decryption process of ciphertext image is the reverse process of encryption.

V. EXPERIMENTAL SIMULATION AND RESULT ANALYSIS

A. SIMULATION EFFECT OF IMAGE ENCRYPTION ALGORITHM

Three different color images are used for simulate test of the image encryption algorithm constructed by the enhanced single neuron, and the practical impact of the encryption method is verified in the encryption process. In the proof, we take $k = 0.2, I_0 = -0.1, z = 0.1, \varepsilon_0 = 0.004$ as fixed initial values. The original and encrypted images are shown in Fig. 6.

B. ANALYSIS OF INFORMATION ENTROPY

Information entropy [16] of color or grayscale image mirrors the average information measurement, which represents a

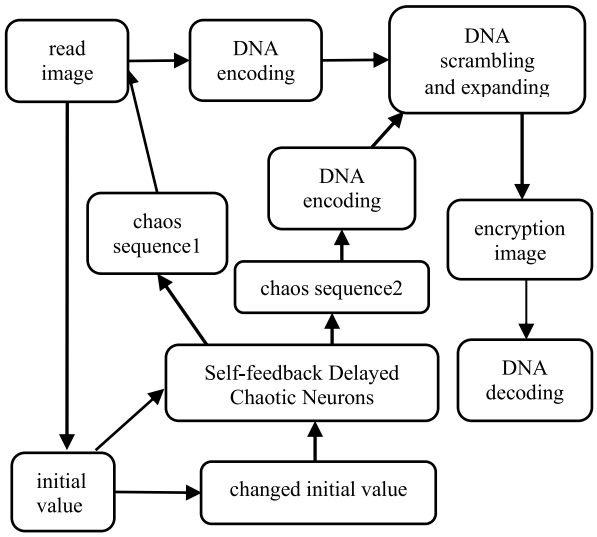


FIGURE 5. Image encryption process diagram.

statistical feature of $R(x_i)$. The numeration equation is:

$$Q(x) = -\sum_{i=0}^{n} R(x_i) \log_2 R(x_i) \tag{19}$$

$R(x_i)$ indicates the proportion of grayscale symbols, indicating the grayscale of the image, and image information vary from order into disorder though the encryption. Theoretically, the closer the value gets to 8, the messier the message, as shown in Table 5

C. ANALYSIS OF HISTOGRAM

The color image grayscale histogram value [19] mirrors the number of occurrences of each grayscale value. Fig. 7 accurately and sharply compares the pixel value distribution before and after encryption enforcement. The more balanced the distribution of encrypted graphic pixel values, the better the capacity to confront miscellaneous statistical attacks. The gray histogram of image Lena, airplane and peppers before and after encryption is shown below. We can clearly observe that the gray pixels of the encrypted pictures exist in a more uniform and orderly form.

D. GRAY LEVEL DIFFERENCE

Another statistical complexity measure is used to assess the performance of the algorithm is gray difference which could contrast the randomness of the graph. It can be described as the following definition: KaTeX parse error: No such environment: equation at position 8: \begin{equation} HN(x, y) = \frac... Where H(x, y) represents the gray value at position (x, y). The mean of neighborhood gray difference of the whole image can be figured by the mathematical formula:

$$GVD = \frac{KN'[HN(x,y)] - KN[HN(x,y)]}{KN'[HN(x,y)] + KN[HN(x,y)]} \tag{20}$$

$$KN[HN(x,y)] = \frac{\sum_{x=2}^{M-1}\sum_{y=2}^{N-1} HN(x,y)}{(M-2)(N-2)} \tag{21}$$

KN and KN′ on behalf of the average neighborhood gray value, but the previous value means before encryption, and the latter means after encryption process. The end value of the above mathematical formulas is called the GVD, which is 1 when the original graph is the same as encrypted exactly and 0 otherwise.

E. CORRELATION ANALYSIS

Correlation [20] means to disappear fortuitous factors influence via the observation of quantitative numeral data, and the correlation coefficient can objectively show the correlation level between adjacent pixels in the image up and down, left and right, and even in the diagonal direction. The closer the value of correlation coefficient is to 1, the higher the level of correlation between adjacent pixels and the calculation equation are as follows:

$$E(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i) \tag{22}$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x_i))^2 \tag{23}$$

$$cov(x,y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x_i))(y_i - E(y_i)) \tag{24}$$

$$r_{xy} = \frac{cov(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \tag{25}$$

There are strong correlation pixels in adjacent positions in the original image, and the adjacent pixels should be close to zero in the encrypted image to reduce the likelihood of image statistical attacks. Fig. 8 is the correlation image between the initial the encrypted image in three different directions.

As can be seen from the above chart analysis, the value of pixel correlation analysis of all encrypted images is close to zero, so the algorithm we put forward has remarkable capability to resist correlation analysis. Table 7 shows the comparison of the three-way correlation data between the algorithm we proposed and else in reference.

F. IMAGE ENCRYPTION QUALITY

Image encryption quality can be determined by the following formula:

$$G = \sum_{L=0}^{255}\frac{(H_L(P) - H_L(Q))^2}{256} \tag{26}$$

where $P(i,j)$ and $Q(i,j)$ are the pixel gray values at (i,j) of the ciphertext and plaintext images of $M \times N \times O$ pixel L gray level, respectively. $H_L(P)$ and $H_L(Q)$ are defined as the occurrence times of all gray levels L in the plaintext graph and the cipher graph separately and G shows the average change times for all gray level L. The bigger the encryption quality value is, the greater security will be in the encryption. Table 8 is the encryption quality analysis after encryption corresponding to before.

FIGURE 6. Encryption algorithm in the classic picture simulation renderings: (a)original graph; (b)encrypted graph; (c) decrypted graph.

TABLE 5. Analysis of TestU01.

Methods	Images	Entropy		
This paper	Lena	7.9998		
	Airplane	7.9998		
	Peppers	7.9998		
Ref. [17]	Lena	7.9993		
Ref. [10]		R	G	B
	Lena	7.9980	7.9979	7.9978
	Peppers	7.9979	7.9979	7.9979
Ref. [18]	Lena	7.9974	7.9970	7.9971

TABLE 6. Analysis of TestU01.

GVD	R	G	B
Lena	0.9834	0.9790	0.9838
Airplane	0.9770	0.0675	0.9831
Peppers	0.9752	0.0658	0.9772

G. KEY SENSITIVITY AND KEY SPACE ANALYSIS

Encryption keys are usually calculated by the effective number of bits. The lengthier the binary number in sequences, the larger the key space, which can clearly demonstrate the robustness, security and effectiveness of the encryption algorithm. For this essay, there are an initial value and four parameters was chosen as the key in the encryption algorithm. When there is a slight difference in the initial key value, the corresponding sequence generator for key or iterative function key is generated in the encryption process [1], [21], as shown in Fig. 9. The sequence shows obvious differences in about ten iterations, indicating that the system is extremely susceptive to the initial value of the key.

Similarly, when the key space is not large enough, other parameters can also be applied to strengthen the key space to satisfy the needs of encryption. So as to make sure that the safety of the algorithm, the correct decryption process cannot be given after minor modifications to the entire encrypted image. NPCR and UACI can compare the value of changed pixels and the average intensity of their variation between encrypted images with slightly different initial values. When pixel changes occur in the initial plaintext image, there must have a large change in the ciphertext image to resist differential attack effectively, otherwise the capability will be weaker. The several perfect values of NPCR and UACI should be infinitely reach to 99.6094% and 33.4635%. When the calculation results of the algorithm are more approximate

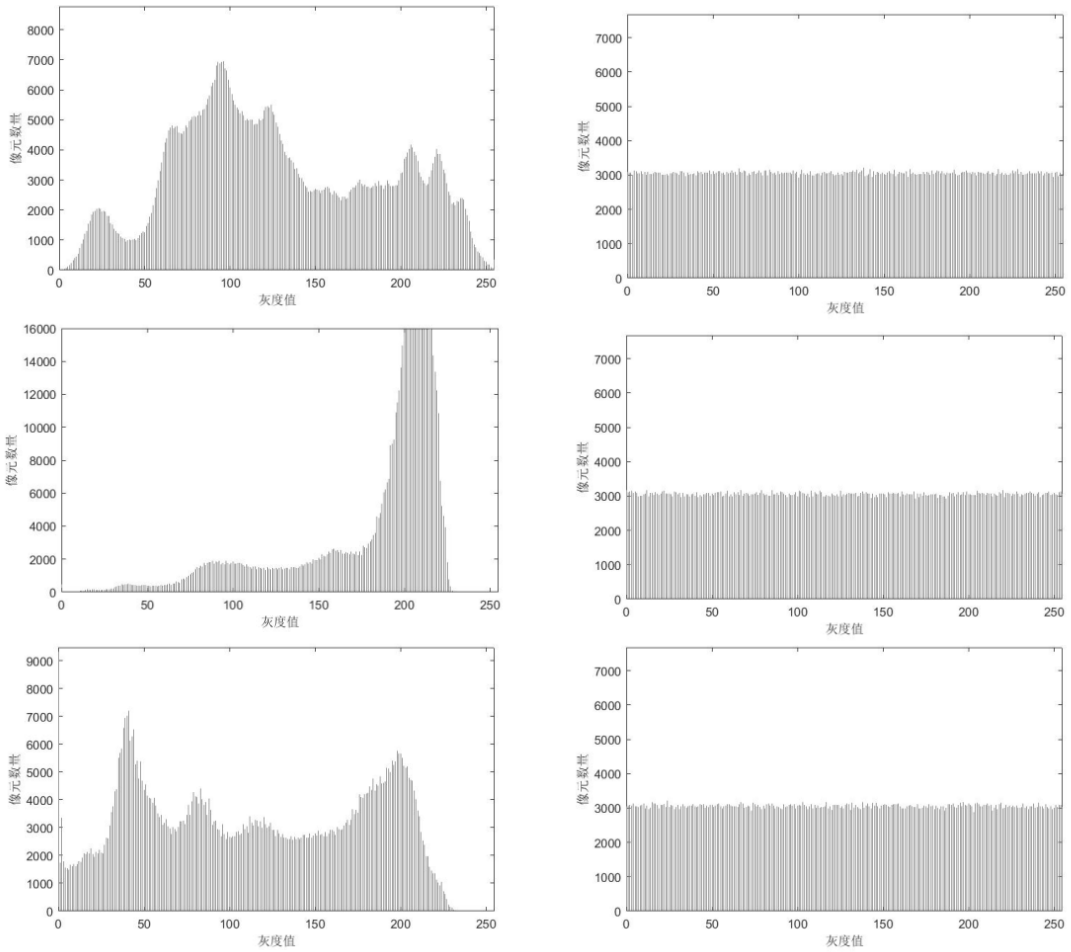


FIGURE 7. Histogram of image Lena, airplane and peppers: (a)original graph; (b)encrypted graph.

TABLE 7. Correlation analysis of original image.

Image	Channel	Original			Encrypted		
		Horizontal	Vertical	Diagonal	Horizontal	Vertical	Diagonal
Lena	R	0.9746	0.9872	0.9653	-0.0367	-0.0059	0.0182
	G	0.9751	0.9849	0.9619	0.0030	0.0587	-0.0123
	B	0.9551	0.9745	0.9333	-0.0037	-0.0227	-0.0134
Airplane	R	0.9713	0.9554	0.9309	-0.0141	0.0112	0.0044
	G	0.9608	0.9668	0.9349	-0.0137	0.0105	0.0351
	B	0.9577	0.9338	0.9117	-0.0134	-0.0091	-0.0079
Peppers	R	0.9618	0.9685	0.9552	0.0056	0.0019	0.0155
	G	0.9761	0.9838	0.9662	0.0064	-0.0019	0.0162
	B	0.9688	0.9681	0.9568	-0.0165	0.0245	-0.0056

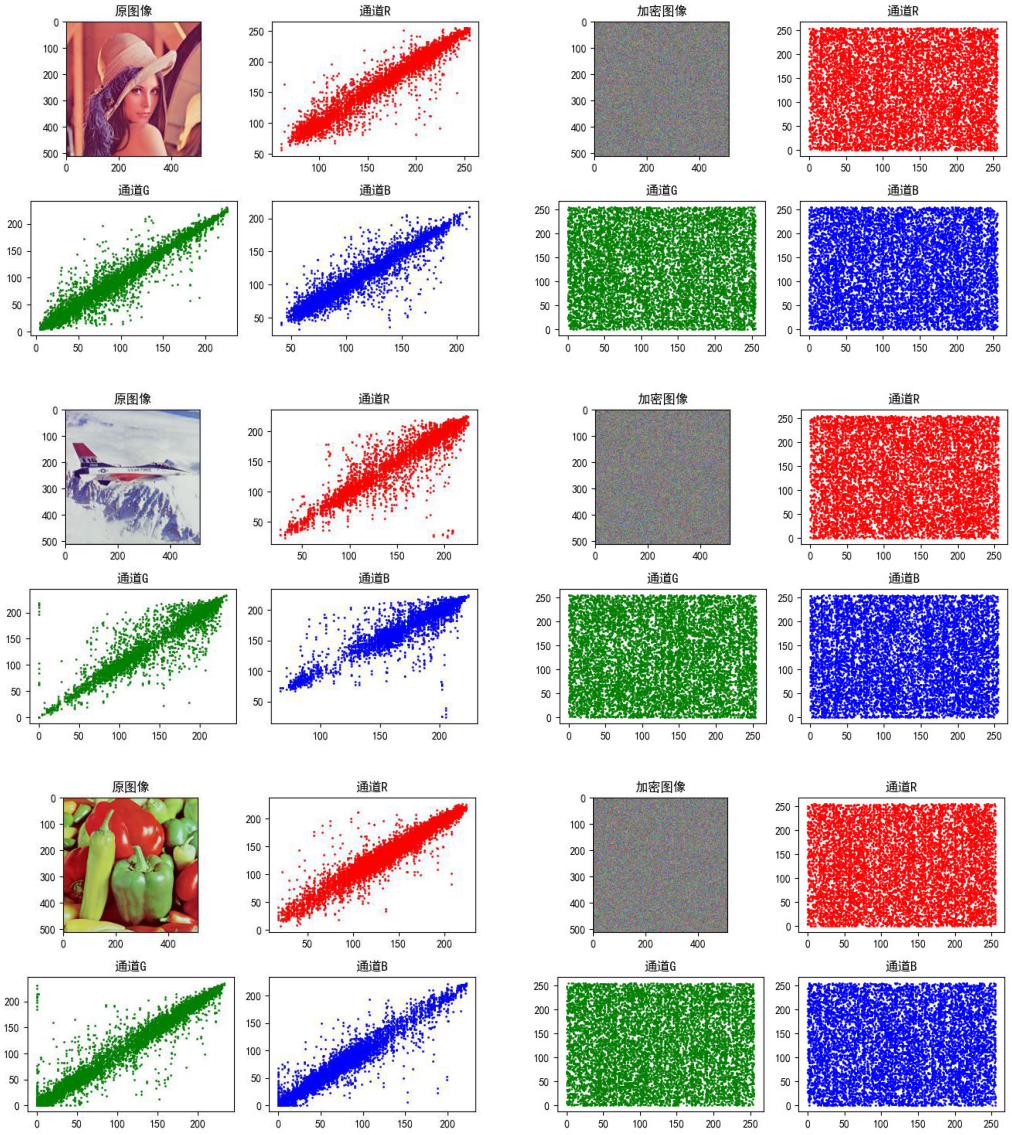
to the ideal value, it indicates that the algorithm has better resistance competence and safety. The concerned results and comparisons are represented in Table 9.

VI. ROBUSTNESS ANALYSIS OF THE ALGORITHM

In this part, image Lena of 512×512 was selected to compare the original, encrypted and reconstructed image under different attacks or losses, and peak signal-to-noise ratio (PSNR) was used to measure the quality of reconstructed image which mainly examines the errors between corresponding pixel points. The smaller the PSNR value, the larger the distortion, the larger the gap between two pictures, and the poorer the image quality. The formula is as follows:

$$PSNR = 10 \times \log_{10} \frac{(2^n - 1)^2}{MSE} \tag{27}$$

where, on behalf of the mean square error of the original image and the reconstructed image, MSE can be represented as this equation when given size M×N of the encrypted image



(a) (b)

FIGURE 8. Correlation coefficients of adjacent pixels of each channel in different images: (a)original graph; (b)encrypted graph.

TABLE 8. EQ analysis.

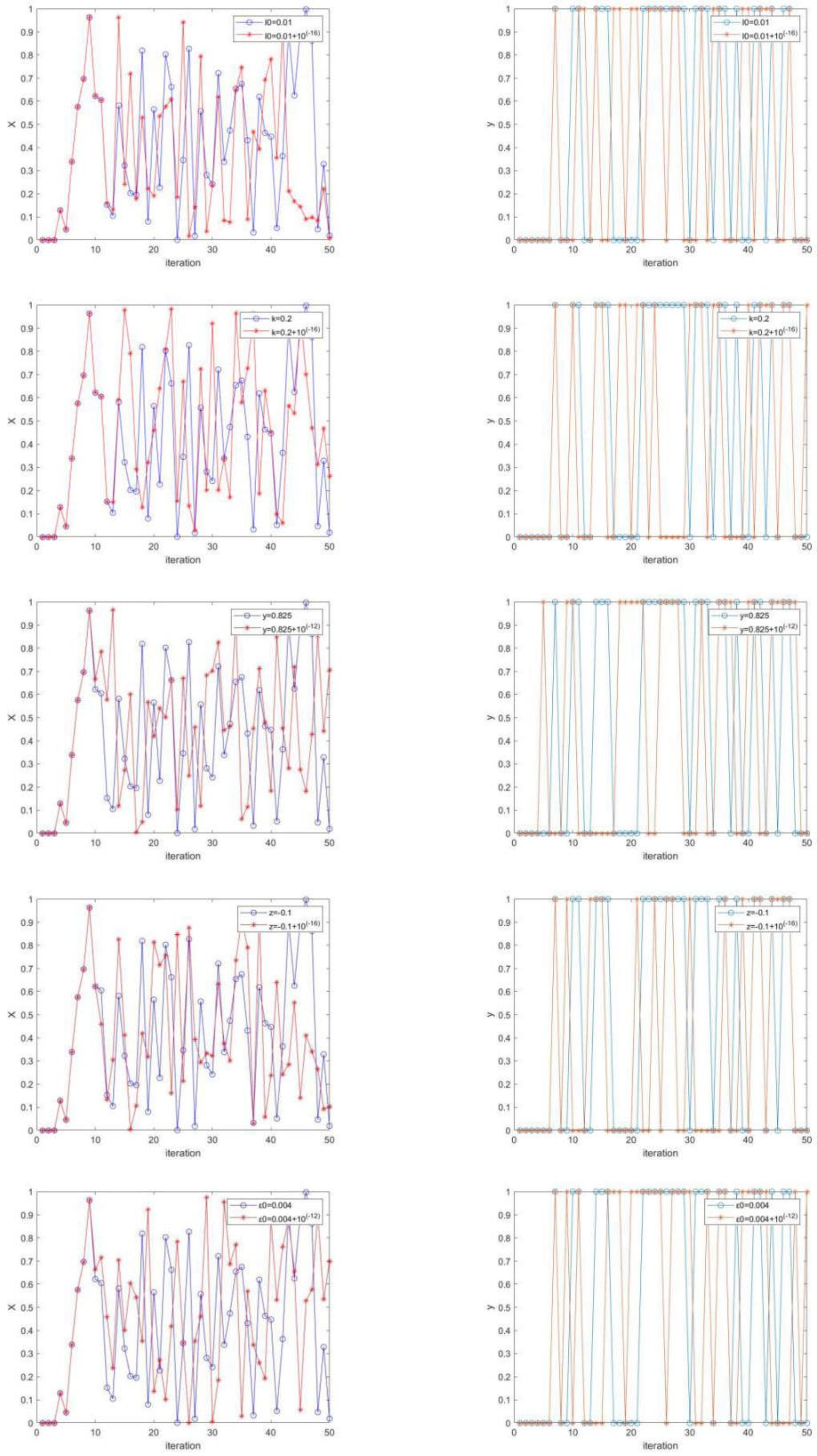
EQ	R	G	B
Lena-encryption	808	578	1020
Airplane- encryption	1074	1056	1254
Peppers- encryption	820	611	946

X and the original image Y:

$$MSE = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} (X(i,j) - Y(i,j))^2 \qquad (28)$$

A. ATTACK BY NOISE

Images are inevitably suffered influence by various factors in the actual process of Internet transmission, among which the more common ones are noise, communication noise caused by distortion, degradation and pollution is very common, all these elements will produce certain effect on the decryption of terminal images, which is in difficulty to restore images from noisy ciphertext. In this paper, gauss and salt and pepper noise are used for simulation experiments. We choose to add zero mean and 0.0005 variance of gauss noise and 5% salt and pepper noise to the encrypted image respectively, and the recover results are compared as exhibited in the Fig.10. The experiment shows that the PSNR value of reconstructed image performs well when we add noise into the encrypted images, indicating that the image still maintains the main information of the original image and is visually acceptable. Therefore, this algorithm has certain robustness against noise attacks.



(a) (b)

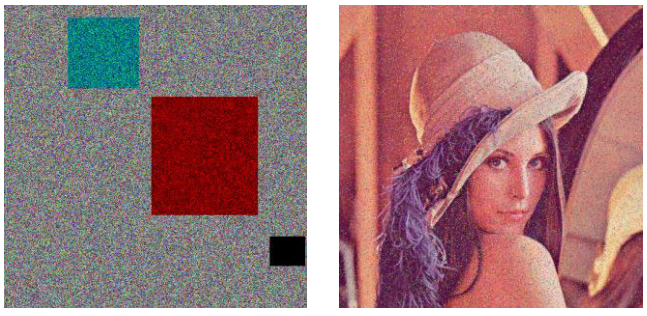
FIGURE 9. Sensitivity analysis of five parameters $l_0, k, y, z, \varepsilon_0$ to initial values: (a)for function x; (b)for function y.

TABLE 9. Comparison of NPCR and UACI parameters.

Methods	Images	NPCR (%)			UACI (%)		
		R	G	B	R	G	B
Proposed	Lena	99.5926	99.6040	99.6098	33.4832	33.5112	33.4032
	Airplane	99.5979	99.6021	99.6162	33.3954	33.5556	33.4386
Ref. [10]	Lena	99.6531	99.66522	99.6518	33.4572	33.4715	33.4384
	Airplane	99.6387	99.6291	99.6283	33.4511	33.4627	33.4416
Ref. [18]	Lena	99.6124	99.6134	99.6192	33.4438	33.5232	33.5010
	Airplane	99.6200	99.6105	99.6164	33.4451	33.3776	33.4782

(a) (b)

FIGURE 10. Add noise in encrypted image and decrypt: (a)gauss noise; (b)salt noise.



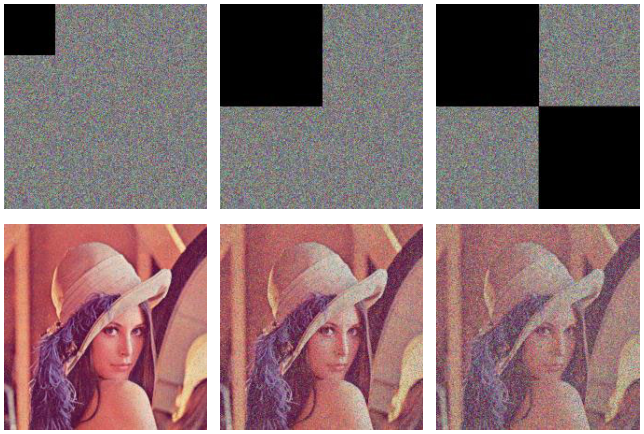
(a) (b)

FIGURE 11. Block attack: (a)loss image; (b)decryption image.

B. LOSS OF DATA

1) ATTACK BY BLOCK

In the face of blocking attacks, an image may lose the data information of one or two or all three channels. Fig. 11 is taken as an example for decryption. After decryption, the original information is retained and can be visualized, so the algorithm can resist blocking attacks.



(a) (b) (c)

FIGURE 12. Add noise in encrypted image and decrypt: (a)6.25% data loss; (b)25% data loss; (c)50% data loss.

TABLE 10. PSNR for robustness analysis of the algorithm.

Lena	Attack	PSNR		
		R	G	B
Noise Attack	Gauss	18.03	18.45	19.27
	Salt	20.99	21.64	22.77
Block Attack		17.39	17.26	19.07
Shearing	6.25%	18.60	21.08	22.91
Attack	25%	13.05	14.86	16.36
	50%	10.87	11.56	12.61

2) ATTACK BY SHEARING

In the process of Internet communication, some parts of the image may be cropped or even lost, so the proposed algorithm must be able to handle the encryption and decryption of the possible loss of the image in an appropriate way. In the simulation experiment, it is assumed that a part of the ciphertext image is lost, taking 6.25%, 25% and 50% data loss of encrypted image as an example, and decrypted the loss images with the correct parameters. The loss image and decrypted image are shown in Fig. 12.

As can be seen from the figure above, when the shearing size reaches 50%, the reconstructed image is obviously fuzzy, but most of the information of the image is still retained and visually acceptable, which indicates that the algorithm is robust against data loss or shearing attacks.

The PSNR values of above decrypted images of ciphertext used original key which subjected to different noise, channel

loss and clip attack is shown in Table 10. It can be seen that the algorithm itself has robust security.

VII. CONCLUSION

In this essay, the time delay and the Bessel function are introduced into the chaotic neural network as self-feedback terms, and the fuzzy number is combined to enhance chaos, so that network constructed reflects different dynamic behaviors for different parameters, and a certain parameter value is selected to propose the model and analysis its dynamic behavior. On this basis, the network model is combined with DNA encoding, and an image encryption algorithm combining pseudo-DNA sequence and chaotic random sequence is proposed. Through the randomness test of sequence, algorithm simulation experiment, information entropy, histogram, gray difference, correlation, encryption quality, key sensitivity, noise attack and other aspects to evaluate the algorithm, it is proved that the encryption scheme is effective and feasible. The method of improving the characteristics of simple chaotic systems combined with our system has broad application prospects, and this feasibility consideration can be used in more operation fields.

ACKNOWLEDGMENT

The authors would like to thank the anonymous reviewers for their constructive remarks that will help them to modify the manuscripts a lot.

REFERENCES

[1] Y. C. Li, "Existence of chaos in weakly quasilinear systems," *Commun. Pure Appl. Anal.*, vol. 10, no. 5, pp. 1331–1344, 2011.
[2] W. H. Yu, "Research on chaos dynamics of several nonlinear systems," M.E. dissertation, Xihua Univ., Chengdu, SC, China, 2020.
[3] C. E. Shannon, "Communication theory of secrecy systems," *Bell Labs Tech. J.*, vol. 28, no. 4, pp. 656–715, Oct. 1949.
[4] R. Guesmi, M. A. B. Farah, A. Kachouri, and M. Samet, "A novel chaos-based image encryption using DNA sequence operation and secure hash algorithm SHA-2," *Nonlinear Dyn.*, vol. 83, no. 3, pp. 1123–1136, Feb. 2016.
[5] L. Chen and K. Aihara, "Chaos and asymptotical stability in discrete-time neural networks," *Phys. D, Nonlinear Phenomena*, vol. 104, nos. 3–4, pp. 286–325, Jun. 1997.
[6] Y. Xu, M. Tang, and J. Fan, "An algorithm of image encryption based on Bessel self-feedback chaotic neural network," in *Proc. Int. Conf. Bus. Intell. Inf. Technol.* Cham, Switzerland: Springer, 2021, pp. 257–266.
[7] F. Masood, W. Boulila, J. Ahmad, Arshad, S. Sankar, S. Rubaiee, and W. J. Buchanan, "A novel privacy approach of digital aerial images based on Mersenne twister method with DNA genetic encoding and chaos," *Remote Sens.*, vol. 12, no. 11, p. 1893, Jun. 2020.
[8] S. C. Su, J. Pang, G. Y. Zhang, H. Z. Hu, and H. T. Chai, "Chaotic synchronization method for unified chaotic system," *J. BeiHua Inst. Aerosp. Technol.*, vol. 24, no. 6, pp. 15–17+42, 2014.
[9] L. Liu, Q. Zhang, and X. Wei, "A RGB image encryption algorithm based on DNA encoding and chaos map," *Comput. Electr. Eng.*, vol. 38, no. 5, pp. 1240–1248, Sep. 2012.
[10] K. Xuejing and G. Zihui, "A new color image encryption scheme based on DNA encoding and spatiotemporal chaotic system," *Signal Process., Image Commun.*, vol. 80, Feb. 2020, Art. no. 115670.
[11] X. Xu and S. Chen, "Single neuronal dynamical system in self-feedbacked Hopfield networks and its application in image encryption," *Entropy*, vol. 23, no. 4, p. 456, Apr. 2021.
[12] A. A. A. El-Latif and X. Niu, "A hybrid chaotic system and cyclic elliptic curve for image encryption," *AEU Int. J. Electron. Commun.*, vol. 67, no. 2, pp. 136–143, 2013.
[13] S. Chen and W. Xue, "Image encryption algorithm based on chaotic system and artificial neural network," *Appl. Comput. Syst.*, vol. 29, no. 8, pp. 236–241, 2020.
[14] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, and E. Barker, "A statistical test suite for random and pseudorandom number generators for cryptographic applications," Booz Allen Hamilton Inc, McLean, VA, USA, Tech. Rep. Special Publication (NIST SP)—800-22 Rev 1a, May 2001.
[15] L. Moysis, C. Volos, S. Jafari, J. M. Munoz-Pacheco, J. Kengne, K. Rajagopal, and I. Stouboulos, "Modification of the logistic map using fuzzy numbers with application to pseudorandom number generation and image encryption," *Entropy*, vol. 22, no. 4, p. 474, Apr. 2020.
[16] P. Rakheja, P. Singh, and R. Vig, "An asymmetric image encryption mechanism using QR decomposition in hybrid multi-resolution wavelet domain," *Opt. Lasers Eng.*, vol. 134, Nov. 2020, Art. no. 106177.
[17] Y.-Q. Zhang, X.-Y. Wang, J. Liu, and Z.-L. Chi, "An image encryption scheme based on the MLNCML system using DNA sequences," *Opt. Lasers Eng.*, vol. 82, pp. 95–103, Jul. 2016.
[18] X. Wang and H.-L. Zhang, "A color image encryption with heterogeneous bit-permutation and correlated chaos," *Opt. Commun.*, vol. 342, pp. 51–60, May 2015.
[19] Y. N. Wang, Z. Y. Song, Y. L. Ma, N. Hua, and H. Y. Ma, "Color image encryption algorithm based on DNA code and alternating quantum random walk," *Acta Phys. Sinica*, vol. 70, no. 23, 2021, Art. no. 230302.
[20] H. Liu, X. Wang, and A. Kadir, "Image encryption using DNA complementary rule and chaotic maps," *Appl. Soft. Comput.*, vol. 12, no. 5, pp. 1457–1466, 2012.
[21] X. T. Xu, S. B. Chen, and Y. Yan, "Remote sensing image encryption combining wavelet packet transform and chaotic neuron," *Remote Sens.*, vol. 36, no. 76, pp. 1–16, 2021.

YAOQUN XU received the B.S. degree in mathematics from Jilin University, Changchun, China, in 1993, the M.S. degree in mathematics from the Harbin Institute of Technology, Harbin, China, in 1997, and the Ph.D. degree in navigation, guidance, and control from Harbin Engineering University, Harbin, in 2002.

He is currently a Professor with the College of Computer and Information Engineering, Harbin University of Commerce. His current research interests include chaotic dynamics, neural networks, and intelligent optimization and decision.

MENG TANG was born in Shandong, China, in 1999. She received the B.E. degree in computer science and technology from Jining University, in 2019. She is currently pursuing the master's degree with the Harbin University of Commerce.