Dynamic behavior analysis, color image encryption and circuit implementation of a novel complex memristive system*

XIONG Li[1], WANG Xuan[2], ZHANG Xinguo[3], and HE Tongdi[1]**

1. School of Physics and Electromechanical Engineering, Hexi University, Zhangye 734000, China

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

3. School of Information Science and Engineering, Lanzhou University, Lanzhou 730000, China

(Received 30 May 2023; Revised 15 August 2023)

This paper is devoted to introduce a novel four-dimensional memristor-involved system and its applications in image encryption and chaotic circuit. The typical dynamical behaviors of the memristor-involved system are explored, such as chaotic phase potraits, Lyapunov exponent spectrum (LES), bifurcation diagram (BD) and complexity analysis. Then a color image encryption algorithm is designed. In this algorithm, the sequences generated by the four-dimensional memristor-involved system are used in scrambling and diffusion algorithm for three channels. The algorithm analysis results based on key space, key sensitivity, information entropy, histogram distribution, correlation coefficients, data loss and noise attacks indicate that the proposed algorithm can improve the security of the color image encryption algorithm. Finally, the memristor-involved chaotic circuit is implemented by using some discrete components. The experimental results of hardware circuit are consistent with the Multisim simulation results and the numerical simulation results. The research results have certain universality and portability, and can provide technical support for the subsequent analysis of other nonlinear circuits and the application of chaotic secure communication.

Document code: A **Article ID:** 1673-1905(2024)03-0183-10

DOI https://doi.org/10.1007/s11801-024-3096-3

As the fourth basic circuit element discovered, memristor is a non-linear passive device, which is different from resistance, capacitance and inductance. It was proposed by CHUA in 1971[1], and it was not until 2008 that HP Labs announced its successful development[2]. Due to the fundamental position of memristor in circuit theory, and its important prospects in computer information storage, large amount of data processing, artificial neural network, new switching model and other application fields, memristor has become a research hotspot at home and abroad[3-5]. This will lead to chaotic behavior in circuits containing memristor. Therefore, the study of memristive chaotic system is of great significance for understanding memristor characteristics and mastering memristor functions.

Memristor consumes energy but does not generate energy. It does not generate power gain in the circuit. It remembers the total amount of charge flowing through it in a nonvolatile manner. It is predicted that there will be the following three important applications in the future computer field based on memristors[6,7]. Firstly, in view of the low energy consumption and memory characteristics of memristor, the computer based on memristor does not need to waste time and energy[8] during startup. Therefore, it is different from the traditional DRAM based computer, which can not save information once the power is cut off. The second application is the huge energy storage of memristor, which will play an important role in cloud computing applications. The third application is that memristor has the function of simulating human memory behavior, so the computer system based on memristor can simulate the memory and association mode of human brain. At present, although the research on memristor in the application field is still in the development stage, the above assumption is expected to be realized in the next few years.

In addition, as the fourth circuit element, memristor has its own nonlinear characteristics, which also provides a new development space for circuit design and circuit application. At present, there are three types of memristor circuits in the literature: memristive basic circuit, memristive equivalent circuit and memristive chaotic oscillation circuit. Compared with conventional chaotic systems, memristive chaotic systems have special and

* This work has been supported by the National Natural Science Foundation of China (No.62061014), the Natural Science Foundation of Gansu Province (No.22JR11RG223), and the President Fund Innovation Team Project of Hexi University (No.CXTD2022003).

** E-mail: xl-427814@163.com

diverse nonlinear dynamic behaviors. With the deepening of research, researchers have found and defined some unique nonlinear behaviors of memristive circuits, such as hidden dynamics[9], coexisting attractorss[10] and asymmetric multistability properties[11]. The circuit with memristor has complex dynamic behavior, so scholars begin to explore its value in engineering applications[12,13]. Especially since the occurrence of Bitcoin virus in 2017, information security has become more and more important, and improving communication security with image encryption algorithm has become a hot topic[14,15]. Compared with text data, image data has the characteristics of large amount of data, strong data correlation and large amount of redundant information, which makes digital image encryption/decryption need a lot of password support. CHAI et al[16] designed an efficient visually meaningful image compression and encryption scheme based on compressive sensing and dynamic LSB embedding. MOU et al[17] constructed a fractional four-dimensional hyper-chaotic memristive model, and combined with DNA sequences[18] to encrypt color images. These experimental schemes show better encryption effect and higher security. In a word, because memristive chaotic signal has high randomness and larger key space, it becomes another good choice to generate image encryption cipher, which can provide a new development idea for chaotic cryptography[19,20]. Based on the newly constructed memristor system, this paper will optimize the existing algorithms and design a new memristive chaotic digital image cryptosystem.

Moreover, the hardware implementation of memristive circuit is also a key problem in the application of memristive chaotic system. It can not only prove the physical realizability and the correctness of theoretical analysis of the memristive circuit, but also provide basic circuit schemes and theoretical guidance for various engineering practices. Therefore, the hardware implementation of the schemed memristive circuit is verified and discussed in this paper.

The following expression is quoted in this paper for the equation of derivative function:

$$W(\varphi) = \mathrm{d}q(\varphi)/\mathrm{d}\varphi = a + 3b\varphi^2 . \tag{1}$$

The equilibrium point of the whole system only depends on the state variables except φ. Thus, φ is a constant in the equilibrium point, so this equilibrium point set is not an isolated equilibrium point, but a series of non-zero dimensional equilibrium point sets, whose dimension is not less than the number of memristor. Therefore, it is more difficult to study memristive systems than ordinary chaotic systems with only one equilibrium point.

Next, we will add a memristor into the ordinary chaotic system to form a new four-dimensional memristor-involved system. Consider a three-dimensional chaotic circuit system with the following equation:

$$\begin{cases} \dot{x} = -\alpha(x + y + yz) \\ \dot{y} = -\beta(x - xz) \\ \dot{z} = -z - \gamma xy \end{cases} . \tag{2}$$

According to Eq.(1), we use y to represent the input voltage of memristor in the new system, and use a positive constant ε to represent the increment of memristor, so Eq.(2) can be changed to the following system:

$$\begin{cases} \dot{x} = -\alpha(x + y + yz) \\ \dot{y} = -\beta(x - xz) + \varepsilon y W(w) \\ \dot{z} = -z - \gamma xy \\ \dot{w} = -y - w \end{cases} , \tag{3}$$

where $W(w)$ is the same as Eq.(1). Obviously, when ε=0, the previous three equations of Eq.(3) are the same as Eq.(2). We are very interested in the dynamic behavior of this nonlinear dynamic system with memristor. In the paper, we consider the case when ε>0. Thus, Eq.(3) can be changed to the following system:

$$\begin{cases} \dot{x} = -\alpha(x + y + yz) \\ \dot{y} = -\beta(x - xz) + \varepsilon y(c + dw^2) \\ \dot{z} = -z - \gamma xy \\ \dot{w} = -y - w \end{cases} . \tag{4}$$

When the system parameters of memristor-involved system (4) are chosen as α=10, β=5, γ=50, c=0.1, d=0.5 (d=5), ε=1, the four-dimensional memristor-involved system (4) is chaotic. After the specific parameter values are substituted, the four-dimensional memristor-involved system (4) changes to

$$\begin{cases} \dot{x} = -10(x + y + yz) \\ \dot{y} = -5x + 5xz + y(0.1 + 0.5w^2) \\ \dot{z} = -z - 50xy \\ \dot{w} = -y - w \end{cases} , \tag{5}$$

or

$$\begin{cases} \dot{x} = -10(x + y + yz) \\ \dot{y} = -5x + 5xz + y(0.1 + 5w^2) \\ \dot{z} = -z - 50xy \\ \dot{w} = -y - w \end{cases} . \tag{6}$$

When the initial values of the four-dimensional memristor-involved system (5) are selected as (1, 3, −7, −1), the phase portraits of chaotic attractors in different phase planes for system (5) are shown in Fig.1.

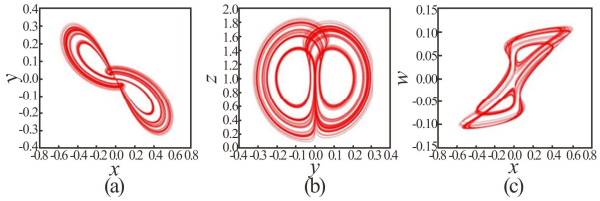


Fig.1 Phase portraits of the four-dimensional memristor-involved system (5): (a) *x*-*y* plane; (b) *y*-*z* plane; (c) *x*-*w* plane

When the system parameters are chosen as α=10, β=5, γ=50, c=0.1, d=5, ε=1, and the initial values of the four-dimensional memristor-involved system (6) are also selected as (1, 3, −7, −1), the phase portraits of chaotic attractors in different phase planes for system (4) are shown in Fig.2.

Comparing Fig.1 and Fig.2, it can be found that when the initial conditions are not changed, but only one of the system parameter values is changed, the chaotic phase portrait trajectory of memristor-involved system (6) is greatly changed. This shows that memristor-involved chaotic system is also very sensitive to system parameters.

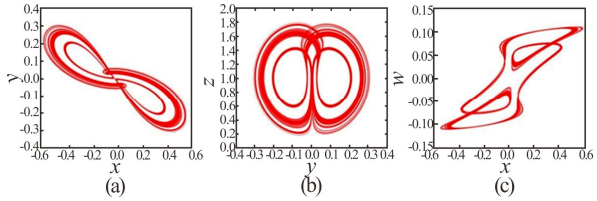


Fig.2 Phase portraits of the four-dimensional memristor-involved system (6): (a) *x*-*y* plane; (b) *y*-*z* plane; (c) *x*-*w* plane

By combining the bifurcation diagram (BD) with the Lyapunov exponent spectrum (LES), the chaotic state of the four-dimensional memristor-involved system under different parameters can be obtained. In the following, set system parameters α and β as variables, and the initial values are also chosen as (1, 3, −7, −1). Then take the step size as h=0.01, and fix the remaining parameters of the four-dimensional memristor-involved system. Next, the different states of the four-dimensional memristor-involved system (4) are observed by changing the system parameters α and β.

(1) For the memristor-involved system (5), take parameter $\alpha\in$[8, 15], order β=5, γ=50, c=0.1, d=0.5, ε=1, and the initial values are chosen as (1, 3, −7, −1), then the LES and BD of memristor-involved system (5) are shown in Fig.3. With the change of system parameter α, complex dynamic characteristics such as chaos and period appear in the memristor-involved system.

Through the LES shown in Fig.3, we can clearly see the state change of the memristor-involved system (5) when the parameter α changes. Through the BD, we can see the change of the memristor-involved system from chaos to period and then into chaos. The analysis shows that the BD is completely corresponding to the LES.

(2) Then, take parameter $\varepsilon\in$[0, 2], order α=10, β=5, γ=50, c=0.1, d=0.5, and the initial values are also selected as (1, 3, −7, −1). Under this condition, the LES and BD of memristor-involved system (5) are shown in Fig.4. With the change of parameter ε, there are obvious periodic and chaotic regions in system (5).

(3) For the memristive system (6), take parameters $\alpha\in$[8, 15], order β=5, γ=50, c=0.1, d=5, ε=1, and the initial values are chosen as (1, 3, −7, −1), then the LES and BD of memristor-involved system (6) are shown in Fig.5. Compared with the memristive system (5), the memristor-involved system (6) is 0.2 units ahead of this parameter.

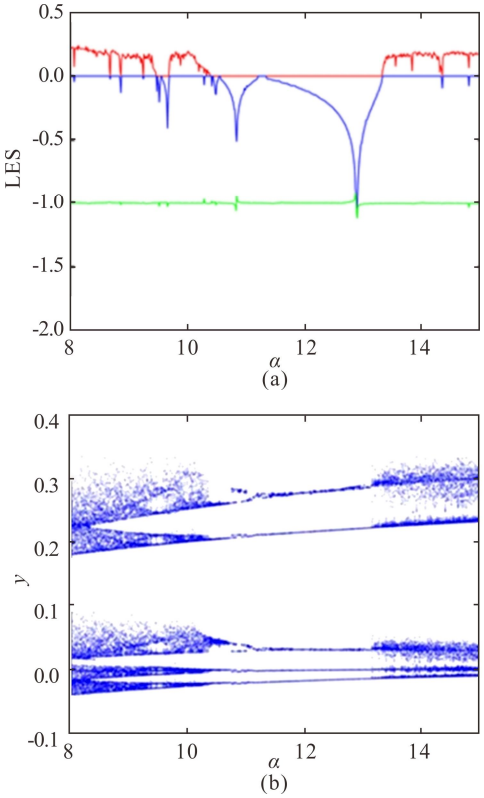


Fig.3 LES and BD of system (5) varying with α: (a) LES; (b) BD

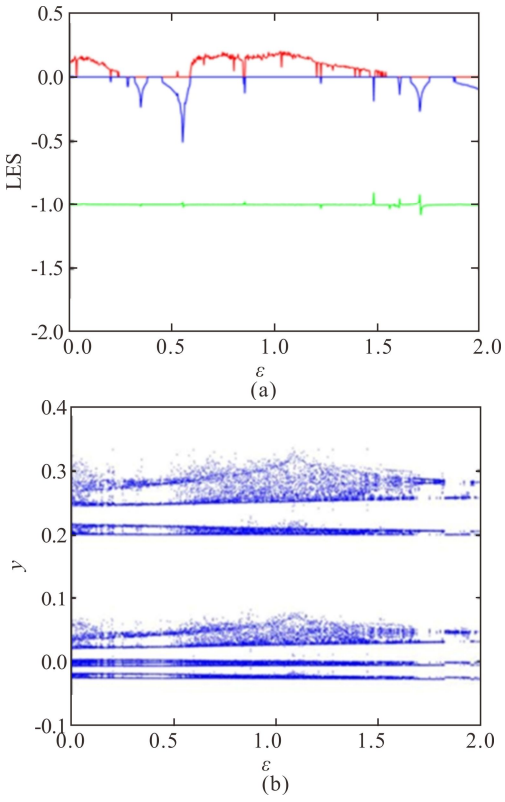


Fig.4 LES and BD of system (5) varying with ε: (a) LES; (b) BD

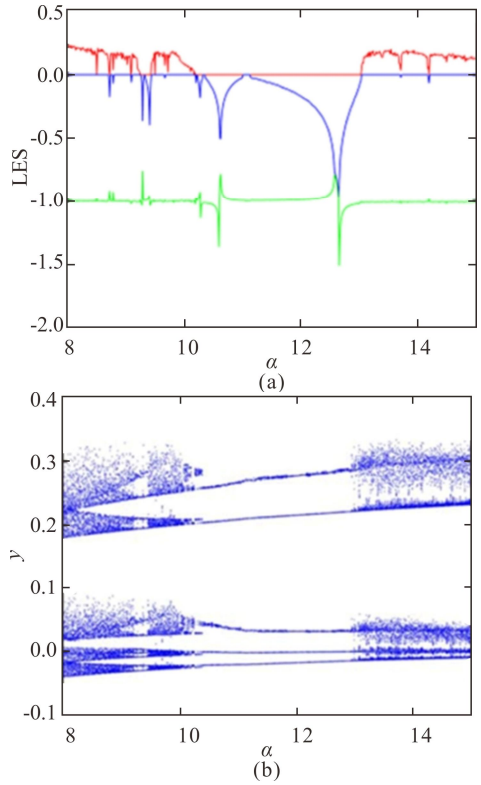


Fig.5 LES and BD of system (6) varying with *α*: (a) LES; (b) BD

(4) For the memristive system (6), take parameter $\varepsilon \in [0, 2]$, order α=10, β=5, γ=50, c=0.1, d=5, and the initial values are selected as (1, 3, −7, −1). Under this condition, the LES and BD are shown in Fig.6. It can be seen that compared with the memristor-involved system (5), the memristor-involved system (6) is also 0.2 units ahead of this parameter.

In order to better use chaotic systems for engineering applications, their complexity needs to be investigated. The higher the complexity of a chaotic system, the closer the resulting chaotic sequence is to a random sequence, and the safer it is. This paper will use spectral entropy (SE) algorithm to analyze the structural complexity. SE algorithm mainly adopts Fourier transform. Through the energy distribution in the Fourier transform domain, combined with Shannon entropy, the spectral entropy is obtained.

In this section, parameters α and parameters ε are chosen as variables, then the complexity of memristor-involved systems (5) and (6) is compared and analyzed. When the system parameter is selected as β=5, γ=50, c=0.1, $\alpha \in [8, 15]$, $\varepsilon \in [0, 2]$, the complexity simulation results of memristive systems (5) and (6) are shown in Fig.7. The state of memristor-involved chaotic system can be determined by the complexity graph. The yellow and white areas in the graph indicate that the complexity of the chaotic system sequence is very low, almost zero, which indicates that the system may be periodic in these areas. On the contrary, the red region represents a chaotic system with high sequence complexity. The darker the color, the better the pseudo randomness of the sequence.

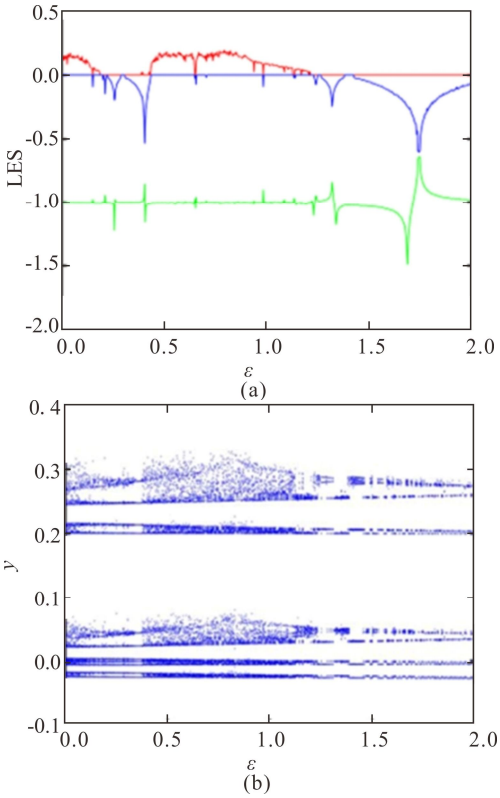
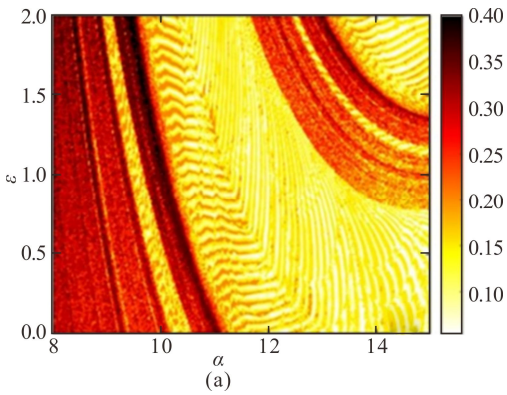


Fig.6 LES and BD of system (6) varying with *ε*: (a) LES; (b) BD

Through comprehensive comparison, the performance trend of the complexity diagram is consistent with the LES and BD of the memristor-involved system. When parameter α and parameter ε are located in the yellow and white area, the complexity of the system sequence is low, and the value of this area should be avoided in encryption and other work.

In this section, apply a four-dimensional memristor-involved system to design a color image encryption algorithm. In this algorithm, a color image is decomposed into R, G and B channels, and then the sequences generated by four-dimensional memristor-involved system are used in scrambling and diffusion algorithm for three channels, respectively. Furthermore, the steps for encryption algorithm are described as follows.



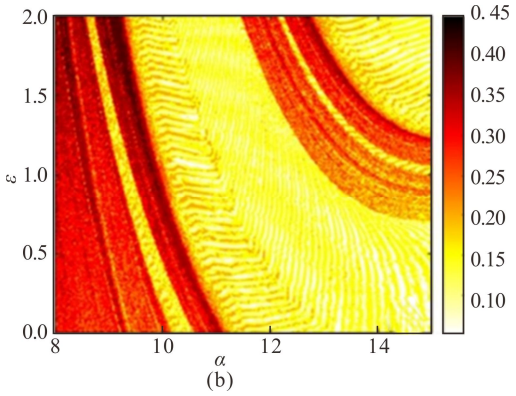


Fig.7 Complexity diagram of the memristor-involved systems (5) and (6) varying with *α* and *ε*: (a) *d*=0.5; (b) *d*=5

Step 1. A color image for size of $M\times N$ is loaded.

Step 2. A color image is decomposed into R, G and B channels, and the size is $M\times N$, respectively.

Step 3. The parameters values for the four-dimensional memristor-involved system (4) are selected at α=10, β=5, γ=50, c=0.1, d=0.5, ε=1, and initial values are selected as (1, 3, −7, −1). When the system is iterated $M\times N$ times, the four memristor-involved chaotic sequences x, y, z and w are obtained.

Step 4. By using the four memristor-involved chaotic sequences x, y, z and w, the two vectors X and Y, and two matrices Z and W can be generated as follows

$$\begin{cases} X=\mathrm{mod}(floor((x(1:M)+100)\times 10^{10}),M)+1 \\ Y=\mathrm{mod}(floor((y(1:M)+100)\times 10^{10}),M)+1 \\ Z(i,j)=\mathrm{mod}(floor(\mathrm{mod}(z((i-1)\times 256+j)+500,1)\times 10^{16}),256) \\ W(i,j)=\mathrm{mod}(floor(\mathrm{mod}(w((i-1)\times 256+j)+500,1)\times 10^{16}),256) \end{cases}, \quad (7)$$

where $i\in[1, M], j\in[1, N]$.

Step 5. R, G and B channels are scrambled by applying two vectors X and Y, respectively. The scrambling process can be described in the following way.

$$\begin{cases} t=R(i,:);R(i,:)=R(X(i),:);R(X(i),:)=t; \\ R_1=R; \\ t=R_1(:,j);Rl(:,j)=R_1(:,Y(j));R_1(:,Y(j))=t; \\ t=G(i,:);G(i,:)=G(X(i),:);G(X(i),:)=t; \\ G_1=G; \\ t=G_1(:,j);G_1(:,j)=G_1(:,Y(j));G_1(:,Y(j))=t; \\ t=B(i,:);B(i,:)=B(X(i),:);B(X(i),:)=t; \\ B_1=B; \\ t=B_1(:,j);B_1(:,j)=B_1(:,Y(j));B_1(:,Y(j))=t; \end{cases}, \quad (8)$$

where $i\in[1, M]$, $j\in[1, N]$. R_1, G_1 and B_1 denote the scrambling results, respectively. And t represents converted variable.

Step 6. R_1, G_1 and B_1 are diffused by using the matrix Z, respectively. The processes for the diffusion algorithm are described by

$$\begin{cases} R_2(M,N)=\mathrm{mod}(R_1(M,N)+Z(M,N),256); \\ R_2(M,j)=\mathrm{mod}(R_1(M,j)+R_2(M,j+1)+Z(M,j),256); \\ R_2(i,N)=\mathrm{mod}(R_1(i,N)+R_1(i+1,N)+Z(i,N),256); \\ R_2(i,j)=\mathrm{mod}(R_1(i,j)+R_2(i,j+1)+R_2(i+1,j)+Z(i,j),256); \\ G_2(M,N)=\mathrm{mod}(G_1(M,N)+Z(M,N),256); \\ G_2(M,j)=\mathrm{mod}(G_1(M,j)+G_2(M,j+1)+Z(M,j),256); \\ G_2(i,N)=\mathrm{mod}(G_1(i,N)+G_2(i+1,N)+Z(i,N),256); \\ G_2(i,j)=\mathrm{mod}(G_1(i,j)+G_2(i,j+1)+G_2(i+1,j)+Z(i,j),256); \\ B_2(M,N)=\mathrm{mod}(B_1(M,N)+Z(M,N),256); \\ B_2(M,j)=\mathrm{mod}(B_1(M,j)+B_2(M,j+1)+Z(M,j),256); \\ B_2(i,N)=\mathrm{mod}(B_1(i,N)+B_2(i+1,N)+Z(i,N),256); \\ B_2(i,j)=\mathrm{mod}(B_1(i,j)+B_2(i,j+1)+B_2(i+1,j)+Z(i,j),256); \end{cases}, \quad (9)$$

where $i\in[M-1, 1], j\in[N-1, 1]$. R_2, G_2 and B_2 represent the diffused results, respectively. And t represents converted variable.

Step 7. R_2, G_2 and B_2 are scrambled by Zigzag algorithm, respectively. A 4×4 matrix is scrambled by using the Zigzag algorithm, and the process is displayed in Fig.8.

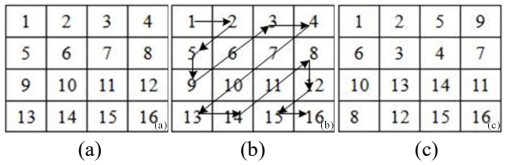


Fig.8 Zigzag scrambling algorithm: (a) Original matrix; (b) Process for scrambling; (c) Scrambled results

Step 8. The scrambled results R_3, G_3 and B_3 are obtained. And then R_3, G_3 and B_3 are diffused by using the matrix W, respectively. The processes for the diffusion algorithm can be described as follows

$$\begin{cases} C_1(i,j)=\mathrm{mod}(R_3(i,j)+W(i,j),256); i=M; j=N; \\ C_1(i,j)=\mathrm{mod}(R_3(i,j)+sum(C_1(i+1,:))+W(i,j),256); j=N; \\ C_1(i,j)=\mathrm{mod}(R_3(i,j)+C_1(i,j+1)+W(i,j),256); \mathrm{other} \\ C_2(i,j)=\mathrm{mod}(G_3(i,j)+W(i,j),256); i=M; j=N; \\ C_2(i,j)=\mathrm{mod}(G_3(i,j)+sum(C_2(i+1,:))+W(i,j),256); j=N; \\ C_2(i,j)=\mathrm{mod}(G_3(i,j)+C_2(i,j+1)+W(i,j),256); \mathrm{other} \\ C_3(i,j)=\mathrm{mod}(B_3(i,j)+W(i,j),256); i=M; j=N; \\ C_3(i,j)=\mathrm{mod}(B_3(i,j)+sum(C_3(i+1,:))+W(i,j),256); j=N; \\ C_3(i,j)=\mathrm{mod}(B_3(i,j)+C_3(i,j+1)+W(i,j),256); \mathrm{other} \end{cases}, \quad (10)$$

where $i\in[M-1, 1], j\in[N-1, 1]$. C_1, C_2 and C_3 mean the diffused results, respectively.

Step 9. A ciphertext image C can be obtained by combining the C_1, C_2 and C_3.

Furthermore, decryption algorithm is the process of recovering ciphertext image. It can be not given in this section.

For clear illustrations, the proposed algorithm can effectively encrypt images, the color images 4.1.01—4.1.08 are selected as test images. Based on the MATLAB-R2019a, by selecting parameters α=10, β=5, γ=50, c=0.1, d=0.5, ε=1, and initial values are selected as

(1, 3, −7, −1) for the key, and the test results for the color images 4.1.01, 4.1.02, 4.1.05 and 4.1.06 are displayed in Fig.9. Fig.9 confirmed that the proposed algorithm can effectively encrypt images.

In general, the key space of the image encryption algorithm is greater than 2 100, which indicates that the proposed algorithm can resist the brute-force attacks. The key for the proposed algorithm is the main constant parameters and initial values of the four-dimensional memristor-involved system. When the maximum error decryption range for parameter and initial is 10^{-14}, the key space is about 2^{465}. Therefore, the designed algorithm can resist the brute-force attacks.

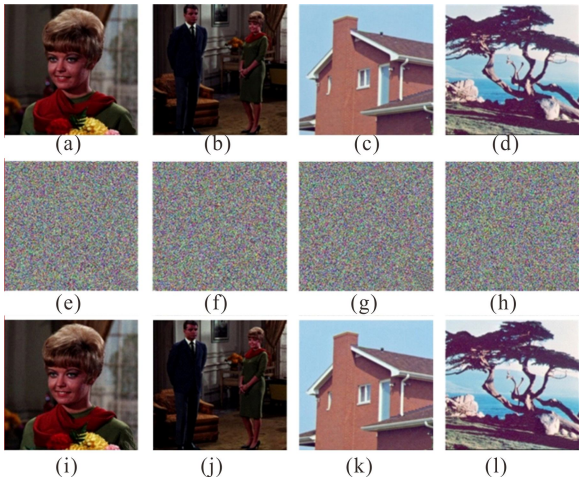


Fig.9 Simulation results: (a—d) Color images 4.1.01, 4.1.02, 4.1.05 and 4.1.06; (e—h) Cipher images; (i—l) Decryption color images

In a cryptosystem, the encryption algorithm should be highly sensitive to the key. In this test, the color image 4.1.01 is used in test. When the key for decryption algorithm is changed, the decrypted images are shown in Fig.10 by using the same key for the encryption algorithm. The results in Fig.10 illustrate that the proposed algorithm is highly sensitive to the key.

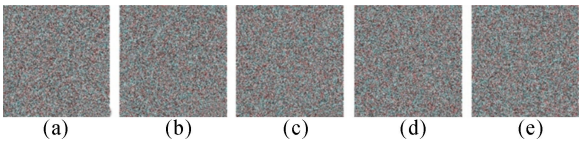


Fig.10 Key sensitive for (a) α=10+10^{-14}, (b) β=5+10^{-14}, (c) γ=50+10^{-14}, (d) c=0.1+10^{-14}, and (e) d=0.5+10^{-14}

Information entropy of the images can be calculated for estimated image information randomness. The information entropy of the images can be calculated by

$$H = -\sum_{i=0}^{L} p(i)\log_2 p(i), \tag{11}$$

where $p(i)$ denotes the probability of occurrence for the ith level. When L=256, H for grayscale image is about 8. Information entropy values for the test images are listed in Tab.1.

Tab.1 Information entropy values for the test image

Color image	4.1.01	4.1.02	4.1.03	4.1.04	4.1.05	4.1.06	4.1.07	4.1.08
Cipher image	7.999 0	7.999 0	7.999 1	7.999 1	7.999 1	7.999 1	7.999 0	7.999 1
R channel	7.997 2	7.997 1	7.997 4	7.997 0	7.997 3	7.997 2	7.997 1	7.997 2
G channel	7.997 2	7.997 2	7.997 6	7.997 3	7.997 2	7.996 8	7.997 0	7.997 5
B channel	7.997 1	7.996 9	7.997 0	7.997 4	7.997 6	7.997 8	7.997 2	7.997 1

The results in Tab.1 confirmed that the information entropy values for the test images almost are close to 8, which indicates that the cipher images encrypted have more randomness by applying the proposed image encryption algorithm. In order to clearly illustrate that the cipher image has greater randomness by using the proposed algorithm, the information entropy for color Lena image is calculated, and the compared results with the existing algorithms are shown in Tab.2.

Tab.2 Information entropy values for the Lena image with the existing algorithms

Lena image	Our algorithm	Ref.[21]	Ref.[22]	Ref.[23]	Ref.[24]	Ref.[25]
Cipher image	**7.999 0**	7.997 5	7.999 0	No	No	No
R channel	**7.997 5**	No	7.997 3	7.997 4	7.997 1	7.997 1
G channel	**7.997 2**	No	7.997 2	7.997 0	7.997 4	7.996 9
B channel	**7.997 8**	No	7.996 6	7.997 1	7.997 3	7.996 2

Tab.2 shows that cipher image has higher information entropy values by using the proposed algorithm, so the designed image encryption has more security.

The histogram distributions of R, G and B channels for the test images 4.1.01 and 4.1.02 are displayed in Fig.11. As we can seen from histogram distributions in Fig.11, the histogram distributions for the cipher image are close to smooth and uniform, so the algorithm can resist statistical attacks.

Furthermore, correlation for adjacent pixels is calculated for further estimation statistical attacks, and the correlation between pixels can be estimated by

$$r_{xy} = \frac{\mathrm{cov}(u,v)}{\sqrt{D(u)}\sqrt{D(v)}}, \tag{12}$$

$$\mathrm{cov}(u,v) = \frac{1}{N}\sum_{i=1}^{N}(u_i - E(u))(v_i - E(v)), \tag{13}$$

$$D(u) = \frac{1}{N}\sum_{i=1}^{N}(u_i - E(u))^2, \tag{14}$$

$$E(u) = \frac{1}{N}\sum_{i=1}^{N}u_i, \tag{15}$$

where u and v represent the two adjacent pixels.

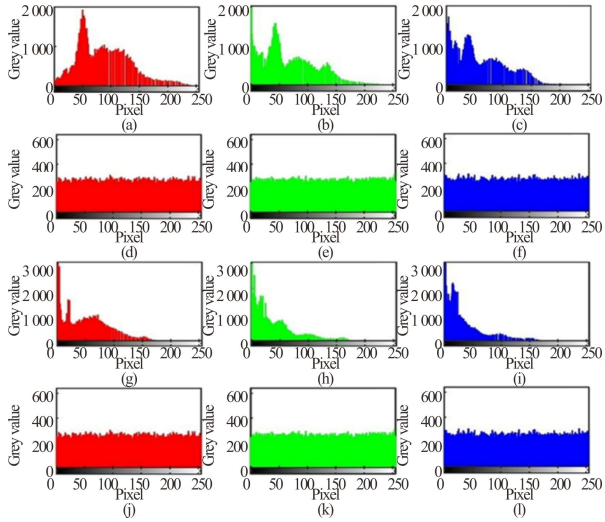


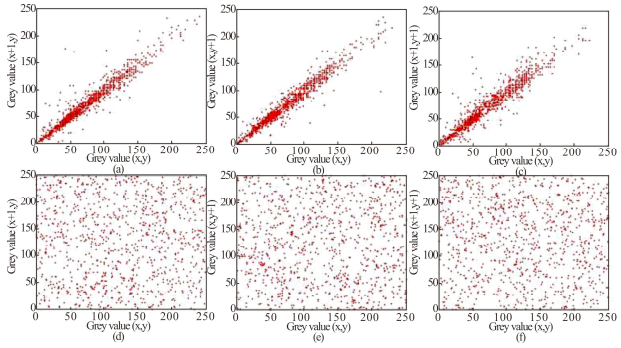
Fig.11 Histogram distributions of R, G and B channels for the test images 4.1.01 and 4.1.02: (a—c) For plaintext image 4.1.01; (d—f) For cipher image 4.1.01; (g—i) For plaintext image 4.1.02; (j—l) For cipher image 4.1.02

As we all know, plaintext image between pixels has higher correlate in the horizontal, vertical and diagonal directions. Because the encryption algorithm can reduce this correlation, there is no correlation between the cipher image pixels. The correlations of R, G and B for color image 4.1.01 in three directions are calculated by randomly selecting 2 000 pairs of pixels, and the correlation distributions are displayed in Fig.12.

The results in Fig.12 confirm that the plaintext for adjacent pixels exists higher correlation (x=y), while cipher image has no correlation in horizontal, vertical and diagonal directions, and the correlation is distributed in all plane.

Furthermore, the correlation coefficients for Lena image are calculated, and the compared results with the existing algorithms are listed in Tab.3.

In order to clearly illustrate that the algorithm can resist data loss assaults, the cipher image for test image 4.1.01 lost different data. By using the decryption algorithm, the results are shown in Fig.13. The results confirmed that the proposed algorithm can resist data loss attacks.



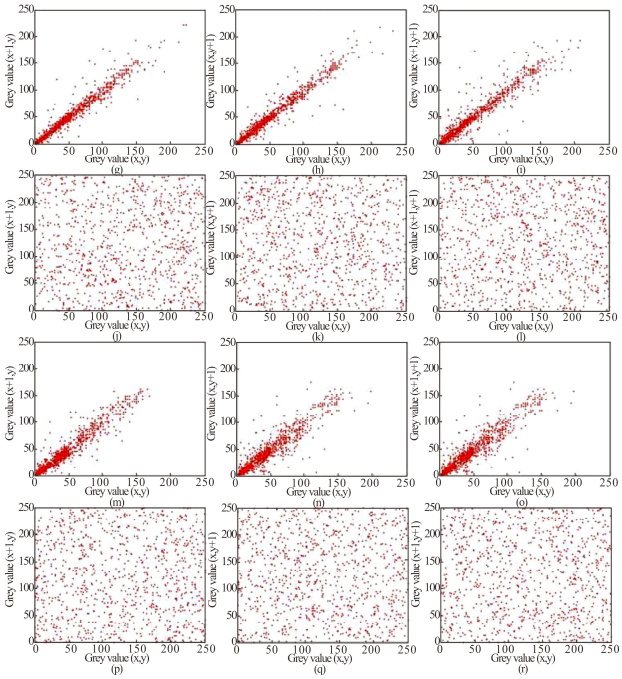


Fig.12 Correlation of R, G and B channels for the color image 4.1.01: (a—c) (d—f) (g—i) For plaintext image 4.1.01 in the horizontal, vertical and diagonal directions; (j—l) (m—o) (p—r) For cipher image 4.1.01 in the horizontal, vertical and diagonal directions

Tab.3 Correlation coefficient values for Lena image

Channel	Direction	Our algorithm	Ref.[22]	Ref.[23]	Ref.[24]	Ref.[25]
R	Horizontal	**−0.000 7**	0.000 7	−0.012 7	0.009 0	0.005 4
	Vertical	**0.007 5**	−0.000 4	0.006 7	−0.001 3	0.006 2
	Diagonal	**−0.001 1**	0.003 9	0.006 0	−0.002 5	0.001 7
G	Horizontal	**0.003 9**	−0.003 5	−0.007 5	−0.002 7	0.005 9
	Vertical	**0.004 9**	0.002 3	−0.006 8	−0.005 1	0.001 6
	Diagonal	**−0.002 7**	−0.007 9	−0.007 8	−0.010 3	0.002 9
B	Horizontal	**−0.004 6**	0.001 5	−0.000 7	−0.015 5	0.001 3
	Vertical	**−0.006 5**	0.002 8	−0.004 2	−0.007 8	0.002 2
	Diagonal	**−0.007 5**	−0.001 0	−0.002 6	0.009 9	0.000 4

In order to test the algorithm's resistance to a certain degree of noise, Gaussian noise is added to the ciphertext images in 4.1.05—4.1.08. By applying the decryption algorithm, then decrypted image are displayed in Fig.14. Fig.14 shows that the proposed algorithm can resist a certain degree of noise.

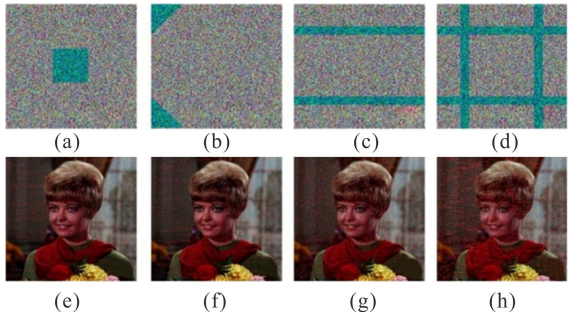


Fig.13 Data loss analysis: (a—d) Cipher images data loss; (e—h) Decrypted images

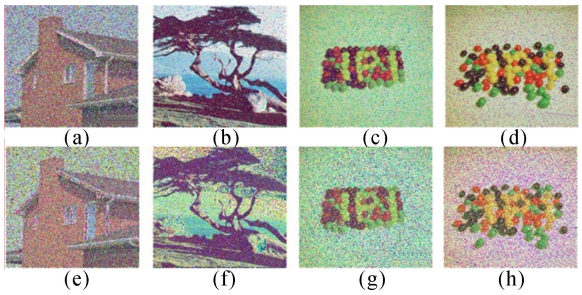


Fig.14 Noise attacks analysis: (a—d) Mean is 0.001 and variance is 0.005; (e—h) Mean is 0.01 and variance is 0.005

In order to further explore the value of the proposed new memristor-involved system in engineering applications, the memristor-involved system is only implemented by analog circuit with the basic electronic components, because commercial memristors are not available on the market. Before designing the circuit, we first consider transforming Eq.(5) into the corresponding state equation. Here, the normalized resistor is set as R=100 kΩ. Therefore, the corresponding equation of state for the designed circuit is given by

$$\begin{cases} \dot{x} = -\dfrac{100k}{10k}x - \dfrac{100k}{10k}y - \dfrac{100k}{1k}\times 0.1yz \\ \dot{y} = -\dfrac{100k}{20k}x + \dfrac{10k}{0.2k}\dfrac{100k}{100k}\times 0.1xz + \\ \quad \dfrac{100k}{100k}\dfrac{10k}{100k}y + \dfrac{10k}{0.2k}\dfrac{100k}{100k}\times 0.01yw^2 \\ \dot{z} = -\dfrac{100k}{100k}z - \dfrac{100k}{0.2k}\times 0.1xy \\ \dot{w} = -\dfrac{100k}{100k}y - \dfrac{100k}{100k}w \end{cases} . \qquad (16)$$

According to state Eq.(16), the specific circuit is designed as Fig.15. It is composed of 5 operational amplifiers, 5 analog multipliers, 13 resistors and 4 capacitors. Before building the actual circuit, the designed circuit should be subjected to circuit simulation firstly. Here, the Multisim circuit simulation software is selected. Based on Fig.15, the simulation result of the four-order memristor-involved circuit is shown in Fig.16(a). Fig.16(a) shows the x-w phase portrait of the four-order memristor-involved circuit.

In order to verify the effectiveness and practicality of the fourth order memristor circuit, the following hardware circuit was built using common electronic components as shown in Fig.15. Since chaotic circuits require very high accuracy, the discrete parameters of analog multiplier may cause difficulties in circuit debugging. Therefore, in the implementation of the hardware circuit in this paper, we need five analog multipliers, so we choose the low-power analog multiplier AD633. Because the analog multiplier AD633 has the precision of laser fine-tuning, it is stable in the working range of good linear voltage from −10 V to 10 V. The hardware circuit experimental result is shown in Fig.16(b) by observing on the oscilloscope. As can be observed from Fig.16(b), the chaotic attractor obtained from the hardware circuit experiments agrees with the simulation result. It is further proved that the four-order memristor-involved circuit is indeed effective and feasible.

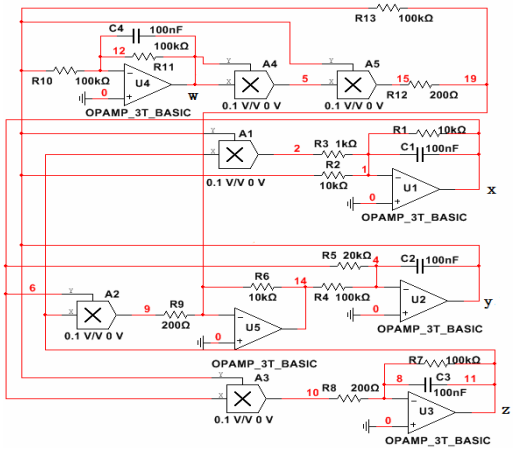
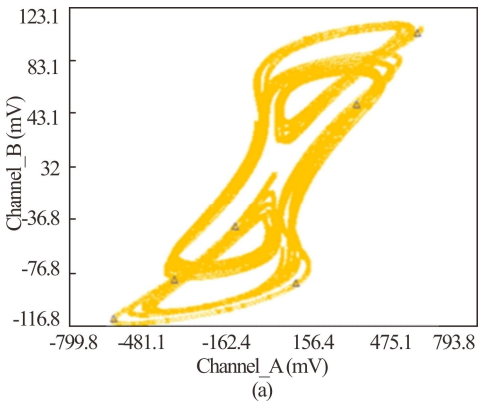


Fig.15 Schematic diagram of the four-order memristor-involved circuit

It is also noted that the Multisim simulation results are roughly the same as the figures of the computer numerical simulation results, but the difference between the attractor phase portraits obtained by the two methods is very small, which may be due to the discrete method used in numerical calculation is different from the continuous system solution obtained by direct simulation, and there are allowable errors in a certain range. In addition, the actual components are used for circuit simulation. The accuracy of the analog multiplier AD633 is 0.1 V, which has an error with the actual value. Therefore, this will also cause a slight difference between the numerical simulation results, circuit simulation results and hardware implementation results. Moreover, the operational amplifiers is not an ideal device, and there is offset voltage, which will also lead to weak differences between the chaotic phase portraits obtained by numerical simulation, circuit simulation and hardware implementation.



(b)

Fig.16 Results of the four-order memristor-involved circuit: (a) *x-w* phase portrait for Multisim simulation; (b) *x-w* phase portrait for hardware

In this paper, a novel four-dimensional memristor-involved chaotic system is proposed and its nonlinear dynamic characteristics are analyzed through chaotic attractors, BD, LES and complexity analysis. And a color image encryption algorithm is designed. A series of simulation results and security estimation show that the color encryption algorithm has higher reliability and security. Finally, based on the analog circuit simulation technology, the equivalent circuit of the constructed four-dimensional memristor-involved system is built by using the basic analog electronic devices, and the hardware circuit debugging is completed. And the experimental results are observed on the oscilloscope, which are mutually corroborated with the numerical simulation results and Multisim circuit simulation results.

Ethics declarations

Conflicts of interest

The authors declare no conflict of interest.

References

[1] CHUA L O. Memristor-the missing circuit element[J]. IEEE transactions on circuit theory, 1971, 18(5): 507-519.

[2] STRUKOV D B, SNIDER G S, STEWRT G R, et al. The missing memristor found[J]. Nature, 2008, 453(7191): 80-83.

[3] LU Y M, WANG C H, DENG Q L, et al. The dynamics of a memristor-based Rulkov neuron with fractional-order difference[J]. Chinese physics B, 2022, 31(6): 060502.

[4] LIN H R, WANG C H, CUI L, et al. Hyperchaotic memristive ring neural network and application in medical image encryption[J]. Nonlinear dynamics, 2022, 110: 841-855.

[5] WEN Z H, WANG C H, DENG Q L, et al. Regulating memristive neuronal dynamical properties via excitatory or inhibitory magnetic field coupling[J]. Nonlinear dynamics, 2022, 110(4): 3823-3835.

[6] LIN H R, WANG C H, XU C, et al. A memristive synapse control method to generate diversified multi-structure chaotic attractors[J]. IEEE transactions on computer-aided design of integrated circuits and systems, 2023.

[7] YANG L M, WANG C H. Emotion model of associative memory possessing variable learning rates with time delay[J]. Neurocomputing, 2021, 460(14): 117-125.

[8] JUN M A. Biophysical neurons, energy, and synapse controllability: a review[J]. Journal of Zhejiang University-science A, 2023, 24(2): 109-129.

[9] LIU T M, YAN H Z, SANTO B, et al. A fractional-order chaotic system with hidden attractor and self-excited attractor and its DSP implementation[J]. Chaos, solitons and fractals, 2021, 145: 110791.

[10] LAI Q, WAN Z, KAMDEM K P D, et al. Coexisting attractors, circuit implementation and synchronization control of a new chaotic system evolved from the simplest memristor chaotic circuit[J]. Communications in nonlinear science & numerical simulation, 2020, 89: 105341.

[11] MA C G, MOU J, XIONG L, et al. Dynamical analysis of a new chaotic system: asymmetric multistability, offset boosting control and circuit realization[J]. Nonlinear dynamics, 2021, 103(3): 2867-2880.

[12] LIN H R, WANG C H, SUN Y C, et al. Generating n-scroll chaotic attractors from a memristor-based magnetized hopfield neural network[J]. IEEE transactions on circuits and systems-II: express briefs, 2023, 70(1): 311-315.

[13] XIONG L, ZHANG X G, TENG S F, et al. Detecting weak signals by using memristor-involved chua's circuit and verification in experimental platform[J]. International journal of bifurcation and chaos, 2020, 30(13): 2050193.

[14] ZHU Y, WANG C H, SUN J, et al. A chaotic image encryption method based on the artificial fish swarms algorithm and the DNA coding[J]. Mathematics, 2023, 11: 767.

[15] LIU Z, WANG Y, ZHANG L Y, et al. A novel compressive image encryption with an improved 2D coupled map lattice model[J]. Security and communication networks, 2021, 6: 1-21.

[16] CHAI X L, WU H Y, GAN Z H, et al. An efficient visually meaningful image compression and encryption scheme based on compressive sensing and dynamic LSB embedding[J]. Optics and lasers in engineering, 2020, 124: 105837.

[17] YANG F F, MOU J, LIU J, et al. Characteristic analysis of the fraction-order hyperchaotic complexity system and its image encryption application[J]. Signal processing, 2020, 169: 107373.

[18] XIONG L, YANG F F, MOU J, et al. A memristive system and its applications in red-blue 3D glasses and image encryption algorithm with DNA variation[J]. Nonlinear dynamics, 2022, 107(5): 2911-2933.

[19] YANG F F, MOU J, MA C G, 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: 106031.

[20] LI X J, MOU J, XIONG L, et al. Fractional-order double-ring erbium-doped fiber laser chaotic system and its application on image encryption[J]. Optics and laser technology, 2021, 140: 107074.

[21] KUMAR M, IQBAL A, KUMAR P. A new RGB image encryption algorithm based on DNA encoding and elliptic curve Diffie-Hellman cryptography[J]. Signal processing, 2016, 125: 187-202.

[22] GAO X. A color image encryption algorithm based on an improved Hénon map[J]. Physica scripta, 2021, 96(6): 065203.

[23] WANG X, ZHANG H. A color image encryption with heterogeneous bit-permutation and correlated chaos[J]. Optics communications, 2015, 342: 51-60.

[24] WANG L, SONG H, LIU P. A novel hybrid color image encryption algorithm using two complex chaotic systems[J]. Optics and lasers in engineering, 2016, 77: 118-125.

[25] WEI X, GUO L, ZHANG Q, et al. A novel color image encryption algorithm based on DNA sequence operation and hyper-chaotic system[J]. Journal of systems and software, 2012, 85(2): 290-299.