Memristor-based hyper-chaotic circuit for image encryption*

Jiao-Jiao Chen(陈娇娇)[1,2], Deng-Wei Yan(闫登卫)[1,2],
Shu-Kai Duan(段书凯)[1,2,3,4,5,6], and Li-Dan Wang(王丽丹)[1,2,3,4,5,†]

[1] *College of Electronic and Information Engineering, Southwest University, Chongqing* 400715, *China*
[2] *Chongqing Key Laboratory of Nonlinear Circuits and Intelligent Information Processing, Southwest University, Chongqing* 400715, *China*
[3] *Intelligent Transmission and Control Technology Joint Engineering Laboratory, Chongqing* 400715, *China*
[4] *Brain-inspired Computing and Intelligent Control Chongqing Key Laboratory, Chongqing* 400715, *China*
[5] *Chongqing Collaborative Innovation Center for Brain Science, Chongqing* 400715, *China*
[6] *School of Artificial Intelligence, Southwest University, Chongqing* 400715, *China*

(Received 30 April 2020; revised manuscript received 4 September 2020; accepted manuscript online 28 September 2020)

The memristor is a kind of non-linear element with memory function, which can be applied to chaotic systems to increase signal randomness and complexity. In this paper, a new four-dimensional hyper-chaotic system is designed based on a flux controlled memristor model, which can generate complex chaotic attractors. The basic dynamic theory analysis and numerical simulations of the system, such as the stability of equilibrium points, the Lyapunov exponents and dimension, Poincare maps, the power spectrum, and the waveform graph prove that it has rich dynamic behaviors. Then, the circuit implementation of this system is established. The consistency of simulation program with integrated circuit emphasis (SPICE) simulation and numerical analysis proves the ability to generate chaos. Finally, a new image encryption scheme is designed by using the memristor-based hyper-chaotic system proposed in this paper. The scheme involves a total of two encryptions. By using different security analysis factors, the proposed algorithm is compared with other image encryption schemes, including correlation analysis, information entropy, *etc*. The results show that the proposed image encryption scheme has a large key space and presents a better encryption effect.

Keywords: memristor, SPICE simulation, hyper-chaotic system, image encryption

PACS: 05.45.–a, 05.45.Gg, 05.45.Jn, 05.45.Vx **DOI:** 10.1088/1674-1056/abbbfe

1. Introduction

Chaos exists in nonlinear deterministic systems, which is sensitive to initial conditions and possesses a complex and unpredictable long-term behavior. Lorenz discovered a chaotic system from a simple mathematical model of weather in 1963.[1] Subsequently, various complex chaotic systems were studied. In 1999, Chen proposed a novel chaotic system.[2] Bao *et al*.[3] discovered a three-dimensional (3D) chaotic system with simple equations and more complex attractors in 2009. In order to construct more complex chaotic systems, one has found various chaotic attractors in the past ten years, such as single-scroll, double-scroll and multi-scroll chaotic attractors.[4]

Memristor was proposed as the fourth basic circuit element in 1971.[5] It is a non-linear resistor with memorable function, which is easy to generate chaotic signals. It can remember the quantity of charge flowing through it and change its own resistance value by controlling the change in current. However, it was not until 2008 that the first physical model of memristor was successfully implemented in HP Labs, which has triggered a comprehensive study of memristor by scholars.[6] Due to its small size, low power consumption, and high potential application value, the memristor is widely used in computer science,[7] electrical engineering, and other fields.[8] Itoh and Chua[9] replaced Chua's diodes with memristor and obtained several nonlinear oscillators, which aroused the research interest in memristive chaotic circuits. Then Kyprianidis *et al*. discovered a simplest third-order memristive chaotic circuit.[10] Stork *et al*. proposed a feedback system based on the memristor, and verified the feasibility with performance of the system by the circuit simulation.[11] Yan *et al*. proposed a flux-controlled memristor model and applied it to chaotic systems, obtaining many complex chaotic attractors.[12] Lv and Min[13] introduced the flux-controlled memristor model into the improved Chua's circuit, and constructed a new memristive chaotic circuit. Wang *et al*. proposed a four-wing chaotic system based on the memristor in 2019, and implemented dynamic analysis and circuit simulation of the system.[14] The above researches have greatly promoted the development of memristor-based chaotic circuits, which give us a detailed introduction about the new chaotic dynamical characteristics. How to better apply the non-linear characteristics of memristor and design various new chaotic circuits based on memristor have become a research focus. In this paper, a new hyper-chaotic system based on the flux-controlled memristor is proposed and its simulation program

*Project supported by the National Key Research and Development Program of China (Grant No. 2018YFB1306600), the National Natural Science Foundation of China (Grant Nos. 62076207 and 62076208), and the Fundamental Science and Advanced Technology Research Foundation of Chongqing, China (Grant Nos. cstc2017jcyjBX0050).

†Corresponding author. E-mail: ldwang@swu.edu.cn

© 2020 Chinese Physical Society and IOP Publishing Ltd

with integrated circuit emphasis (SPICE) circuit is established. The proposed system has abundant dynamic behaviors and the main features of its circuit are as follows. Firstly, the circuit based on the flux-controlled model makes the system exhibit more superior dynamic characteristics; secondly, only three multipliers and some basic electronic components are used in this circuit; thirdly, the whole circuit contains three analog unit circuits: adder, inverter and integrator. Its structure is simple and easy to implement. These advantages enable the proposed system to be better applied.

To ensure the security of digital image, it is necessary to encrypt the image information in the transmission process. Unlike text data, digital images not only have a large number of data, but also have high redundancy and high correlation between datum points. Therefore, traditional encryption algorithms are time-consuming and difficult to meet the requirements for modern encryption. Because of its good randomness and sensitivity to initial values, chaotic systems have become a research hotspot in the field of image encryption. In 2017, Li *et al.*[15] proposed an image encryption scheme based on chaotic tent mapping, and proved the effectiveness and security of the scheme through analysis. Wang *et al.*[16] applied the proposed novel one-dimensional LP and PCLML chaotic systems to image encryption to improve the effectiveness and security of the encryption scheme. Ye *et al.*[17] designed a seventh-order memristive chaotic circuit in 2019 and used this system to generate chaotic keys for image encryption. Wang *et al.* studied the finite-time synchronization of memristive chaotic systems and proposed an image encryption scheme based on the memristive chaotic systems.[18] Zhang and Tang[19] discovered a symmetric image cryptosystem based on the piecewise linear map. Yang *et al.* proposed a color image compression and encryption algorithm based on fractional order memristor chaotic circuit.[20] A color image encryption scheme using fractional-order hyper-chaotic system and DNA sequence calculation was studied by Zhang *et al.*[21] Wang *et al.* proposed a chaotic system based on memristor and applied it to the image encryption.[22] Wang *et al.*[23] presented a new symmetric key encryption algorithm based on the ergodicity property of a logistic map. Wang *et al.* proposed a new hyper-chaotic system based on two memristors and applied it to the image encryption process.[24] Shi *et al.*[25] presented an image encryption scheme based on compressed sensing and multidimensional chaotic system. From all the above researches, we can find that the application of chaotic systems to the field of image encryption has become a very important trend. Therefore, in this article, we design an encryption scheme based on the proposed hyper-chaotic system, and proved its superiority by experimental results and encryption performance evaluations.

Compared with other simple systems, high-dimensional complex chaotic systems based on memristor have many advantages especially in the process of image encryption. On this basis, a four-dimensional hyper-chaotic system based on the flux-controlled memristor model is proposed in this paper. The rest of this paper is organized as follows. In Section 2, we introduce the mathematical model of this system and the dynamic characteristics, including phase diagram, equilibrium point, Poincare maps, the Lyapunov exponents, power spectrum, waveform, *etc*. The SPICE circuit simulation of the proposed system is realized in Section 3. The consistency of the circuit simulation and numerical simulation proves the ability of this hyper-chaotic system to produce chaos. An image encryption scheme based on the system is designed in Section 4. In order to increase the security of image encryption, three test images are encrypted twice by using the Lorenz chaotic system and the proposed hyper-chaotic system, the performances of which are evaluated by key space, histogram analysis, correlation analysis, differential attack, information entropy, etc. Finally, some conclusions are drawn in Section 5.

2. New hyper-chaotic system based on memristor

2.1. Hyper-chaotic system based on flux-controlled memristor model

The mathematical model of a new hyper-chaotic system based on memristor is as follows:

$$\begin{cases} \dot{x} = y - ax + yz, \\ \dot{y} = by - xz - w, \\ \dot{z} = xy - cz, \\ \dot{w} = my + ef(-|x|), \end{cases} \tag{1}$$

when the system parameters are $a = 3$, $b = 1$, $c = 9$, $e = 0.2$, $m = 1$, the system exhibits complex chaotic behaviors, x, y, z, and w are the states of the hyper-chaotic system and a, b, c, e, and m are parameters of it. The function $f(\cdot)$ represents the charge of the memristor, and we can describe it as

$$f(x) = \begin{cases} \dfrac{x - c_3}{R_{\text{off}}}, & x < c_5, \\ \dfrac{\sqrt{zkx + M(0)^2} - M(0)}{k}, & c_5 \le x \le c_6, \\ \dfrac{x - c_4}{R_{\text{on}}}, & x \ge c_6, \end{cases} \tag{2}$$

where x is the input of the memristor, and the memristor model parameters are set as follows:

$$\begin{cases} c_3 = \dfrac{(R_{\text{off}} - M(0))^2}{2k}, \\ c_4 = \dfrac{(R_{\text{on}} - M(0))^2}{2k}, \\ c_5 = \dfrac{R_{\text{off}}^2 - M(0)^2}{2k}, \\ c_6 = \dfrac{R_{\text{on}}^2 - M(0)^2}{2k}, \end{cases} \tag{3}$$

where $R_{\text{off}} = 20\ \text{k}\Omega$, $D = 10\ \text{nm}$, $R_{\text{on}} = 100\ \Omega$, $M(0) = 16000$, $u_v = 10^{-14}\ \text{m}^2 \cdot \text{s}^{-1} \cdot \text{V}^{-1}$, and k is a constant,

$$k = (R_{\text{on}} - R_{\text{off}})\, u_v R_{\text{on}} / D^2. \tag{4}$$

The initial conditions are assigned as follows: $x(0) = 1$, $y(0) = 1$, $z(0) = 1$, and $w(0) = 1$, and the system produces the hyper-chaotic attractors as shown in Fig. 1.

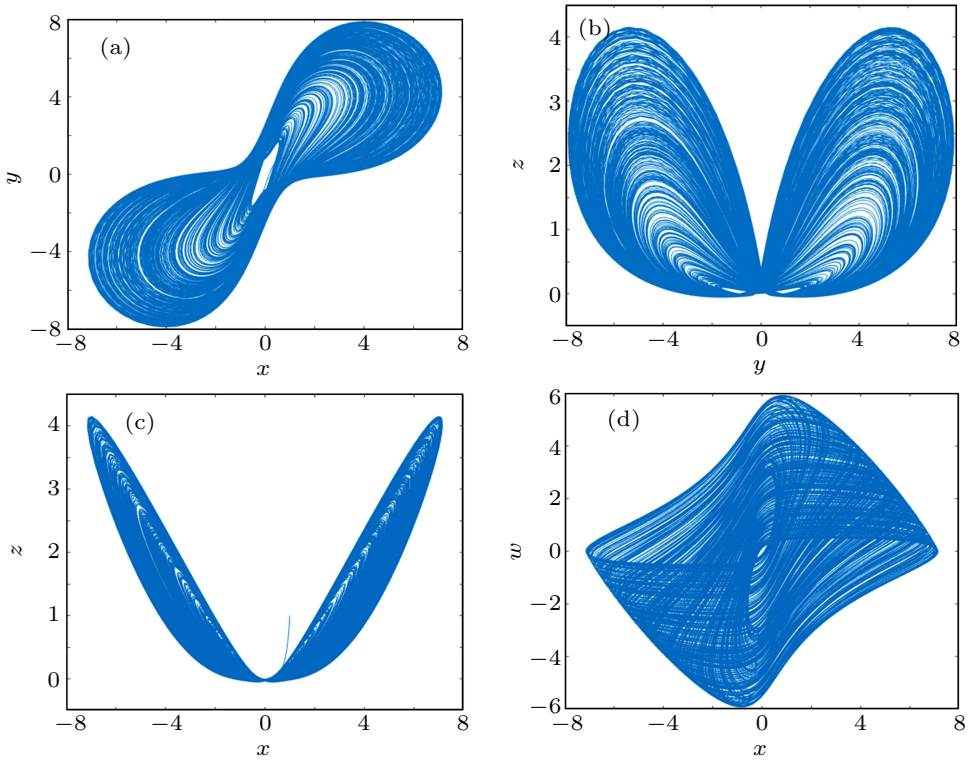


Fig. 1. Phase portraits of system (1) with $a = 3$, $b = 1$, $c = 9$, $e = 0.2$, $m = 1$ in (a) x–y plane, (b) y–z plane, (c) x–z plane, and (d) x–w plane.

The phase–orbit diagram is a record of the system's motion trajectory, reflecting changes in the state of the system. It is the most direct way to observe the dynamic behaviors of the system. Therefore, one usually observes the projection of the phase diagram on the plane and uses it to judge the dynamic behaviors of the system. As can be seen from Fig. 1, this system can generate complex chaotic attractors.

2.2. Equilibrium stability analysis

Setting the state variables of this system to be zero and the equilibrium of it can be obtained by the following equations:

$$\begin{cases} 0 = y - ax + yz, \\ 0 = by - xz - w, \\ 0 = xy - cz, \\ 0 = my + ef(-|x|). \end{cases} \tag{5}$$

Since $f(-|x|)$ is a piecewise function in the above formula, we need to find the equilibrium point of the system in pieces.

When $x < C_5$, that is, $x < -0.3618$, formula (5) has three equilibrium points. The calculated results are shown in the following Table 1.

Table 1. Equilibrium points of formula (5) when $x < C_5$.

	x	y	z	w
S_1	–155885327979.4965	–519616.0680	5.1961	–300000.9767
S_2	155885376219.5367	519616.1484	–5.1961	–300001.0232
S_3	0	0	0	0

As can be seen from Table 1, there is one equilibrium point, *i.e.* S_1, which satisfies the condition.

While $C_5 \le x \le C_6$, that is, $-0.3618 \le x \le 0.6431$, we can see the equilibrium points from Table 2.

Table 2. Equilibrium points of formula (4) when $C_5 \le x \le C_6$.

	x	y	z	w
S_4	-5.9999×10^{-38}	-2.0020×10^{-38}	-5.999×10^{-38}	0
S_5	–0.00003216	–0.00001072	–0.00003216	0
S_6	260428016091	–67162084306	–5.19615242	38776047452.94
S_7	–26043446442	–67162915693	5.196152427	–38776527455.9

There is only one point that meets the condition, which is S_5.

When $x > C_6$, that is, $x > 0.6431$, the equilibrium points of formula (5) are shown in Table 3.

Table 3. Equilibrium points of formula (5) when $x > C_6$.

	x	y	z	w
S_8	–3899109.2976	–2598.3098032	5.1978846064	–1500.63494764
S_9	3902904.93013	2599.57438182	–5.197883763	–1501.36505241
S_{10}	0.00126415720	0.00042138576	0.0012641572	0.000000059188

Point S_9 is the only equilibrium point that satisfies the condition.

In summary, there are three equilibrium points of the system, namely S_1, S_5, S_9 which meet the requirements. Through equilibrium points, the Jacobi matrix of the system can be ob-

tained as follows:

$$J=\begin{bmatrix} -3 & 1+z & y & 0 \\ -z & 1 & -x & -1 \\ y & x & -9 & 0 \\ 0.2f(-|x|) & 1 & 0 & 0 \end{bmatrix}. \tag{6}$$

According to the Jacobi matrix corresponding to each equilibrium point, the special values are calculated as follows:

$$S_1: \quad \lambda_1 = 1.5589\mathrm{i}, \quad \lambda_2 = -1.5589\mathrm{i}, \quad \lambda_3 = \lambda_4 = 0.$$
$$S_5: \quad \lambda_1 = -3, \quad \lambda_2 = -9, \quad \lambda_3 = 0.5 + 0.866\mathrm{i},$$
$$\lambda_4 = 0.5 - 0.866\mathrm{i}.$$
$$S_9: \quad \lambda_1 = 3.9029\mathrm{i}, \quad \lambda_2 = -3.9029\mathrm{i}, \quad \lambda_3 = \lambda_4 = 0.$$

2.3. Poincare maps

The Poincare maps are proposed by Poincare at the end of the 19th century and played a very important role in analyzing the complex dynamic behaviors. If the points on the Poincare maps are dense points with a fractal structure, the system is considered to be chaotic. On the contrary, the system is non-chaotic . The Poincare maps of the proposed system is illustrated in Fig. 2. We can draw conclusions from Fig. 2 that the system has extremely rich dynamic characteristics.

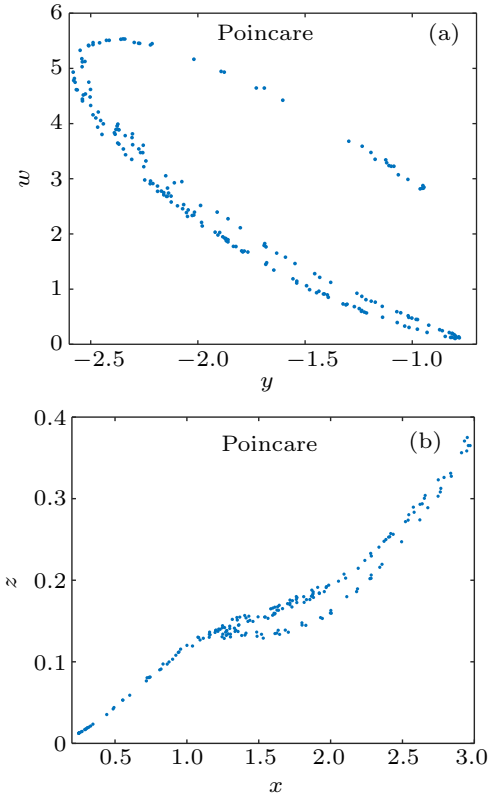


Fig. 2. Poincare map of (a) $x = 0$ and (b) $y = 0$.

2.4. Lyapunov exponents and Lyapunov dimension

The Lyapunov exponent (LE) can characterize the motion of the system. The positive and negative values indicate how long the system diverges or converges in the direction of the adjacent orbit in the attractor. Therefore, the largest Lyapunov exponent determines the orbital coverage of the entire attractor. The smallest Lyapunov exponent determines the orbital convergence and the sum of all Lyapunov exponents can express the orbital average divergence or convergence. The Lyapunov exponent is a useful tool to measure whether the system is chaotic or hyper-chaotic. In particular, the system with one positive Lyapunov exponent is termed chaotic system, and the system with two or more positive Lyapunov exponents are called hyper-chaotic system.

The Lyapunov exponents of the system (1) are obtained numerically, which are shown in the following Fig. 3. The Lyapunov exponents are $LE_1 = 0.1260$, $LE_2 = 0.1263$, $LE_3 = -2.1515$, and $LE_4 = -9.100$. Since $LE_1 > 0$, $LE_2 > 0$, $LE_4 < 0$, and $LE_{1+}LE_{2+}LE_4 < 0$, the system is a hyper-chaotic system.

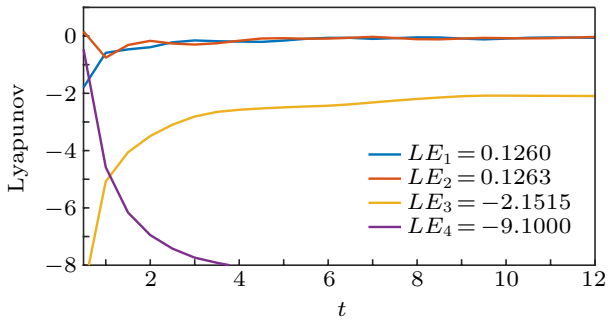


Fig. 3. Lyapunov exponents of the system with $a = 3$, $b = 1$, $c = 9$, $e = 0.2$, $m = 1$.

The Lyapunov dimension of this system can be calculated from the following expression:[12]

$$D_L = j + \frac{1}{|L_{j+1}|}\sum_{i=1}^{j} L_i$$
$$= 3 + \frac{1}{|L_4|}(L_1 + L_2 + L_3) \doteq 2.7913. \tag{7}$$

It can be seen from the above result that the system is of fractal dimension. In other words, under these parameters the system is a hyper-chaotic system.

2.5. Power spectrum analysis

As is well known, the power spectrum analysis is an important means to study chaos. According to the Fourier analysis, any periodic motion can be expanded into a Fourier series and the power spectrum of periodic motion is a discrete spectrum. While the power spectrum of aperiodic motion is a continuous spectrum. Under the initial conditions the power spectrum of this system is shown in Fig. 4.

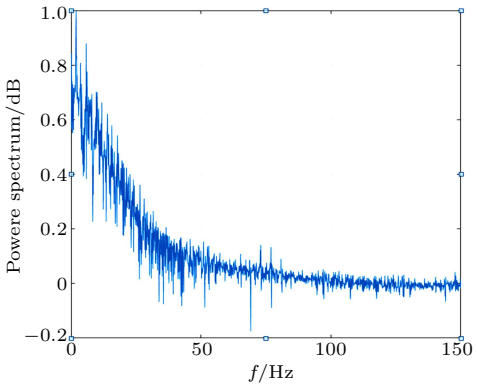


Fig. 4. Power spectrum of the system.

2.6. Time domain waveform

The time domain waveform of system (1) is obtained by using the Matlab 2016 as shown in Fig. 5. The first image is that it is a time-domain waveform of t–y, and the second image is that it is a time-domain waveform of t–w. The time-domain waveform diagram reflects that the system's motion orbit is a seemingly random and non-periodic orbit, which is exactly the phenomenon of chaos.

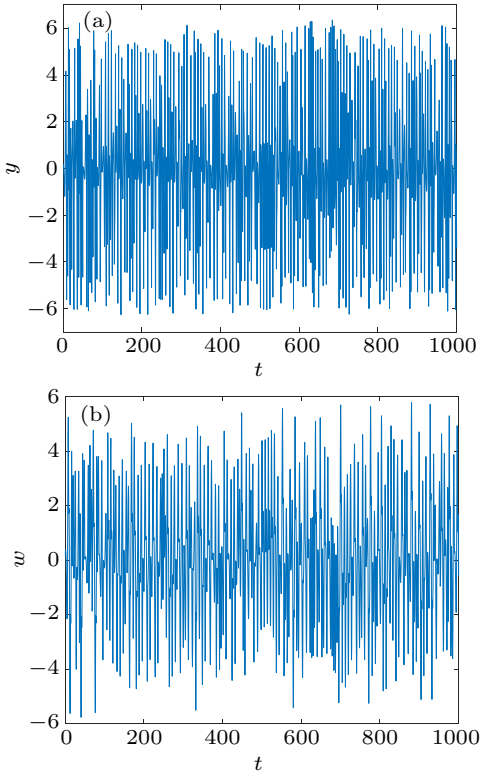


Fig. 5. Time domain waveform of (a) t–y and (b) t–w.

3. Circuit design and SPICE simulation

In practical engineering applications, hardware experiment is an important part of a chaotic system. The circuit is the most direct and effective method to implement the hyperchaotic system. In this paper, the SPICE circuit simulation experiment diagram is shown in Fig. 6. The circuit of new hyperchaotic system based on the flux-controlled memristor is comprised of the capacitor, resistor, operational amplifier and multiplier. The operational amplifier mainly performs functions such as addition, subtraction, and integral calculation in the system equation, whose model used in this paper is LM675 OPMAPs. The analog multiplier completes the multiplication function and performs nonlinear operation of the system equation. In this paper, the SPICE circuit consists of four channels corresponding to four ordinary differential equations. The circuit nodes V_x, V_y, V_z, and V_w represent the state variables of x, y, z, w respectively. In the actual circuit analysis, considering the allowable voltage range of the analog multiplier and the operational amplifier, the power supply voltage applied to the system is $V_{CC} = +30$ V and $V_{EE} = -30$ V.

According to the characteristics of the nonlinear circuit and the basic principle of the circuit, the mathematical equations of the state variable in the simulation circuit shown in Fig. 6 are obtained as follows:

$$\begin{cases} \dfrac{\mathrm{d}x}{\mathrm{d}t} = \dfrac{R_4R_2}{R_5C_1R_3R_1}v_x + \dfrac{R_4}{R_5C_1R_6}v_y + \dfrac{R_4}{R_5C_1R_7}v_yv_z, \\ \dfrac{\mathrm{d}y}{\mathrm{d}t} = \dfrac{R_9}{R_{10}C_2R_8}v_y + \dfrac{R_9R_{12}}{R_{10}C_2R_{13}R_{11}}v_xv_z + \dfrac{R_9R_{15}}{R_{10}C_2R_{16}R_{14}}v_w, \\ \dfrac{\mathrm{d}z}{\mathrm{d}t} = \dfrac{R_{18}}{R_{19}C_3R_{17}}v_xv_y + \dfrac{R_{18}R_{21}}{R_{19}C_3R_{22}R_{20}}v_z, \\ \dfrac{\mathrm{d}w}{\mathrm{d}t} = \dfrac{R_{33}}{R_{34}C_4R_{32}}v_y + \dfrac{R_{33}}{R_{34}C_4R_{35}}f(-|v_x|), \end{cases} \tag{8}$$

where $f(-|x|)$ is the mathematical model of the flux-controlled memristor. This model consists of diodes and amplifiers to realize the function of the absolute value. The parameters of components in the circuit are set as follows:

$$\begin{aligned} &R_1 = R_2 = R_{11} = R_{12} = R_{14} = R_{15} = R_{20} = R_{21} = 10\ \mathrm{k\Omega}, \\ &R_5 = R_{10} = R_{19} = R_{34} = 1000\ \mathrm{k\Omega}, \\ &C_1 = C_2 = C_3 = C_4 = 1\ \mu\mathrm{F}, \quad R_{31} = 250\ \Omega, \\ &R_4 = R_6 = R_7 = 3\ \mathrm{k}\ \Omega, \quad R_{17} = R_{18} = 9\ \mathrm{k\Omega}, \\ &R_{29} = R_{30} = 500\ \Omega, \\ &R_3 = R_8 = R_9 = R_{13} = R_{16} = R_{22} = R_{24} = R_{25} \\ = &\ R_{26} = R_{27} = R_{28} = R_{32} = R_{33} = R_{36} = 1\ \mathrm{k\Omega}. \end{aligned}$$

In the circuit simulation software SPICE, set the running time to be 4000 s in steps of 0.001 s. The circuit simulation results of this system are shown in Fig. 7.

We can see from the above that the circuit structure is so simple that it is easy to implement. The whole circuit contains only some basic electronic components such as multipliers and operational amplifiers, and three analog circuit units: adder, inverter and integrator. Moreover, the model of the flux-controlled memristor is applied to the circuit, which makes the circuit possible to produce more complicated chaotic attractors. The consistency between circuit simulation and numerical simulation can prove the ability of the system to generate chaos, and to further illustrate that the proposed system will be widely used in many fields.

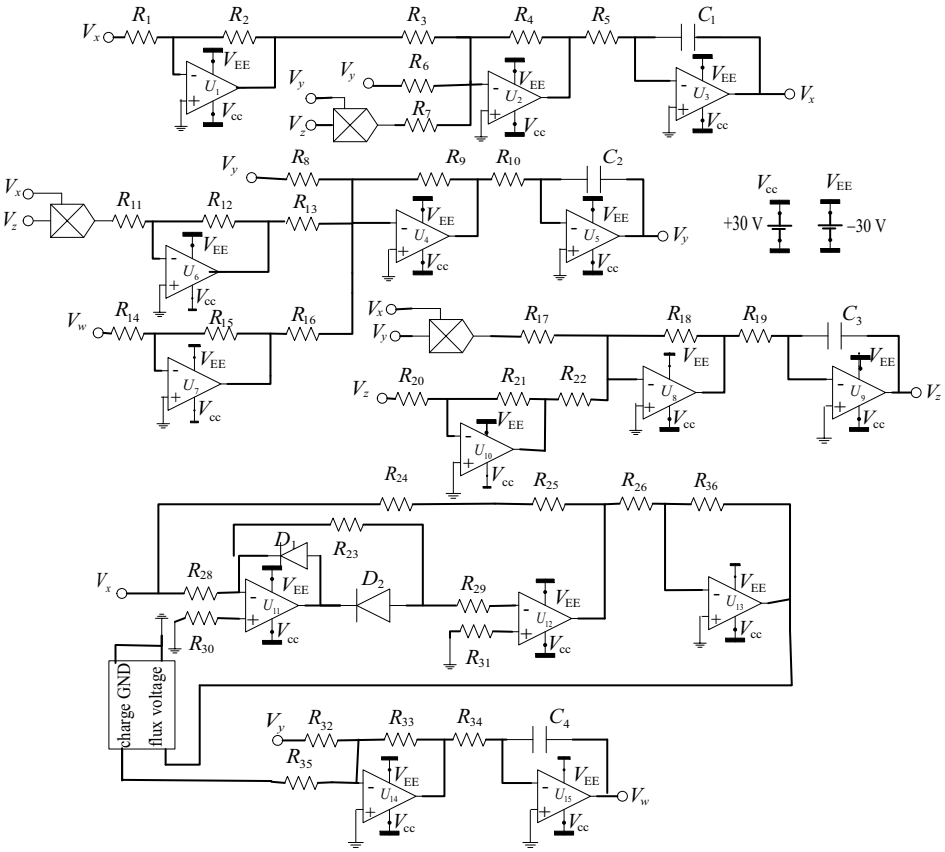


Fig. 6. Hardware circuit implementation of new hyper-chaotic system.

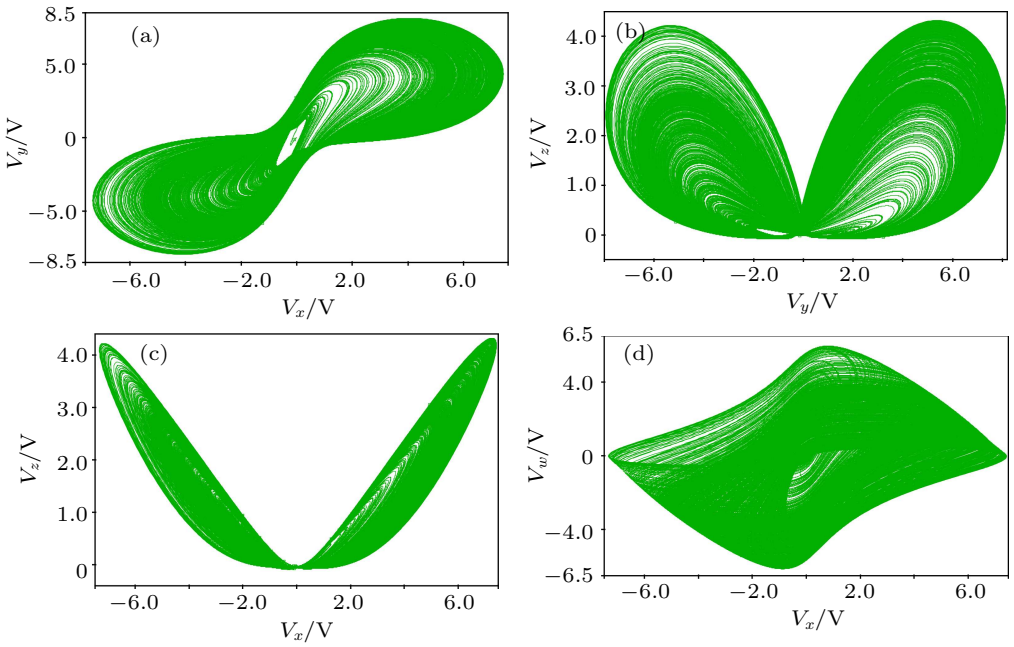


Fig. 7. SPICE simulation results in (a) *x*–*y*, (b) *y*–*z*, (c) *x*–*z*, and (d) *x*–*w* planes of the system.

4. Image encryption process based on new system

Because a chaotic system has the characteristics of initial value sensitivity and unpredictability, applying chaos theory to digital image encryption and improving the security of encrypted images has become a hot topic. Image scrambling is a simple and effective encryption method, but the single image encryption algorithm of the scrambling process has the drawback of poor security performance. On the basis of a simple scrambling, in this paper the proposed new hyper-chaotic system is used based on memristor to perform the secondary encryption on a scrambled image, thus further improving the security of image encryption.

4.1. Encryption scheme

If only one chaotic system is used to encrypt the image, the computational cost is low, easy to implement, but the parameters are less and the output is easy to predict. In this paper, in order to improve the safety of the encrypted image, we introduce multiple chaotic systems to encrypt images twice. The block diagram of the proposed scheme is given in Fig. 8.

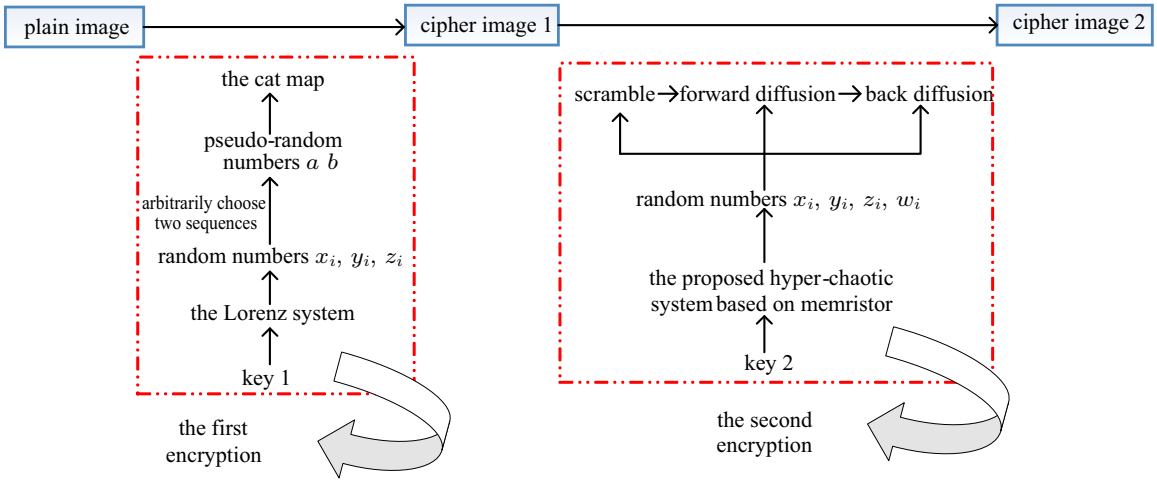


Fig. 8. Block diagram of proposed image encryption.

4.1.1. First image encryption

The three-dimensional Lorenz system is used to generate random numbers, which are used as parameters of the cat map to realize the first encryption of the image. The specific steps are as follows.

Step 1 Convert the input plaintext image into a matrix of $M \times N$ size, where M and N represent the row and column numbers of the image, respectively.

Step 2 The Lorenz system is used to generate three random sequences. Since the system is a very typical chaotic system, the generated sequence is unpredictable and can be used in the image encryption process. The mathematical model of the Lorenz system is as follows:[1]

$$\begin{cases} \dot{x} = a(y-x), \\ \dot{y} = cx - y - xz, \\ \dot{z} = xy - bz, \end{cases} \tag{9}$$

where $a = 10$, $b = 8/3$, $c = 28$, $x_0 = 0.2$, $y_0 = 0.2$, $z_0 = 0.2$, and this system generates three random sequences x_i, y_i, z_i.

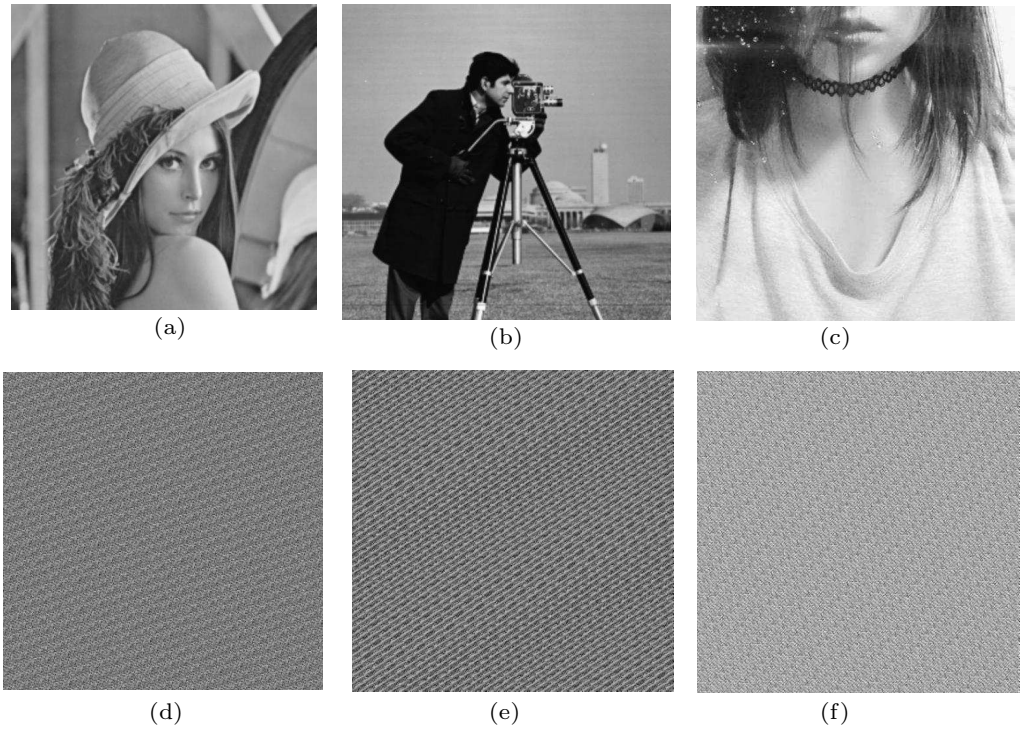


Fig. 9. Plain image of (a) Lena, (b) Cameraman, and (c) Girl; first encrypted image of (d) Lena, (e) Cameraman, and (f) Girl.

Step 3 Arbitrarily choose the two random sequences generated in the second step, and assign their values to a and b. Then the first encryption of the images is realized by formula (9),[26]

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{bmatrix} 1 & b \\ a & ab+1 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} \bmod \begin{bmatrix} M \\ N \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \end{bmatrix}. \quad (10)$$

The experimental results of the first image encryption are shown in Fig. 9.

4.1.2. Second image encryption

The first encrypted image and the proposed hyper-chaotic system are used to realize the second encryption in this paper. The specific process is as follows.

Step 1 Expand the first encrypted image into a one-dimensional vector of $M \times N$ (M and N are the row or column number), and record it as A_i.

Step 2 With the help of the proposed hyper-chaotic system based on memristor, a pseudo-random sequence of length $3M \times N$ is generated, which can further generate a pseudo random sequences X_i for scrambling the image and a pseudo random sequences S_i for disffusing the image.

Step 3 Scrambling A_i and S_i without duplication. The scrambled image and S_i are diffused based on the GF(257) multiplication domain. Finally, the second encrypted image is obtained.

As is well known, the decryption algorithm is the inverse process of the encryption algorithm. If one wants to decrypt images, one needs to decrypt images in reverse steps.

The experimental results of the second encryption and the decrypted image are presented in Fig. 10.

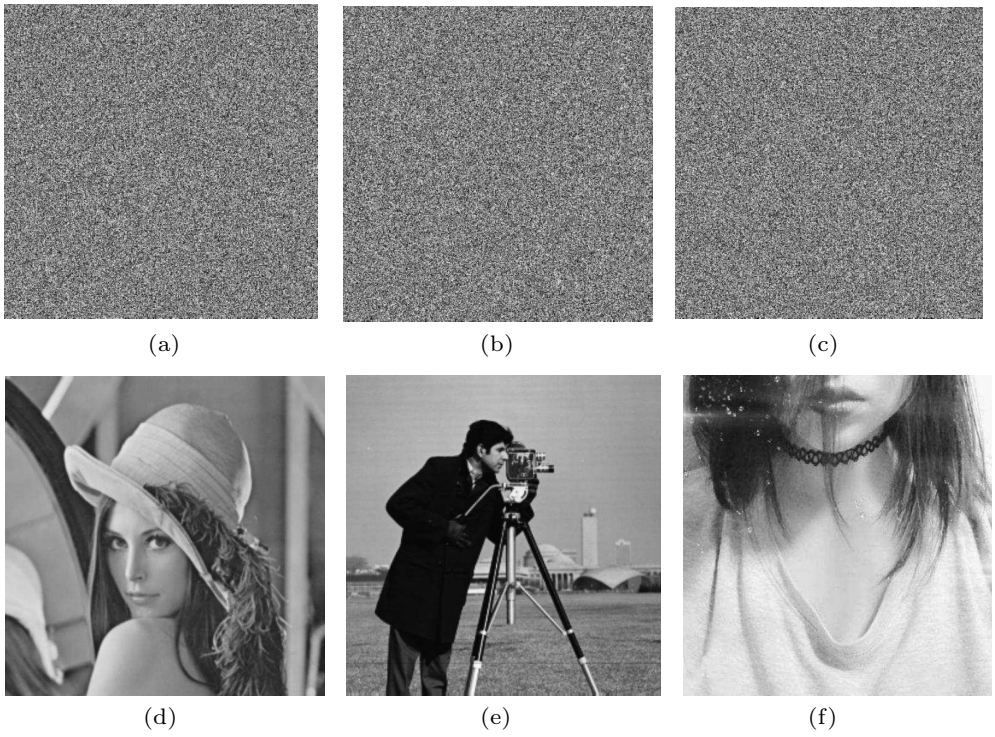


Fig. 10. Second encrypted image of (a) Lena, (b) Cameraman, and (c) Girl; decrypted image of (d) Lena, (e) Cameraman, and (f) Girl.

4.2. Experimental results and analysis

4.2.1. Histogram analysis

Histograms are used to reflect the distributions of pixel values in digital images. Generally, the abscissa of a grayscale histogram represents grayscale level, and the ordinate denotes frequency at which the grayscale level appears. The more uniform the pixel distribution, the better the encryption effect is,so that an attacker cannot obtain any useful information from the encrypted image. The histograms of the original and encrypted images used in this paper are shown in Fig. 11.

As can be seen from the figure above, the histogram of the encrypted images are evenly distributed, which can already hide useful information well. Therefore, the encryption algorithm proposed in this paper has a good performance in resisting statistical attacks.

4.2.2. Correlation between two adjacent pixels

For general digital images, there is a high correlation between adjacent pixels. For an ideal ciphered image, there should be no correlation between adjacent pixels. By testing the correlation of adjacent pixels in encrypted images, the superiority of the encryption scheme can be shown.

The correlation coefficient can reflect the degree of difference between adjacent pixels in the image. The smaller the correlation coefficient, the worse the pixel correlation of the image is. The closer to 1 the correlation coefficient, the stronger the correlation between the image pixels is.

The N pairs of adjacent pixels are selected from the image, whose gray values are recorded with (u_i, v_i), $i = 1, 2, \ldots, N$, the calculation formula of the correlation coefficient is as follows:[26]

$$\begin{cases} r_{xy} = \dfrac{\operatorname{cov}(u,v)}{\sqrt{D(u)}\sqrt{D(v)}}, \\ \operatorname{cov}(u,v) = \dfrac{1}{N}\sum\limits_{i=1}^{N}(x_i - E(u))(y_i - E(v)), \\ D(u) = \dfrac{1}{N}\sum\limits_{i=1}^{N}(u_i - E(u))^2, \\ E(u) = \dfrac{1}{N}\sum\limits_{i=1}^{N}u_i. \end{cases} \tag{11}$$

The calculated correlation coefficients of the adjacent pixels in horizontal, vertical, and diagonal directions are given in Table 4. Figures 12–14 show the distributions of the pixels in plain image and cipher images in the horizontal, vertical, and diagonal directions for test images of Lena, Cameraman, and Girl.

From Table 4 we can find that the correlation coefficients between adjacent pixels in encrypted images are close to zero in the proposed scheme, which can further explain that the encryption scheme has good performances.

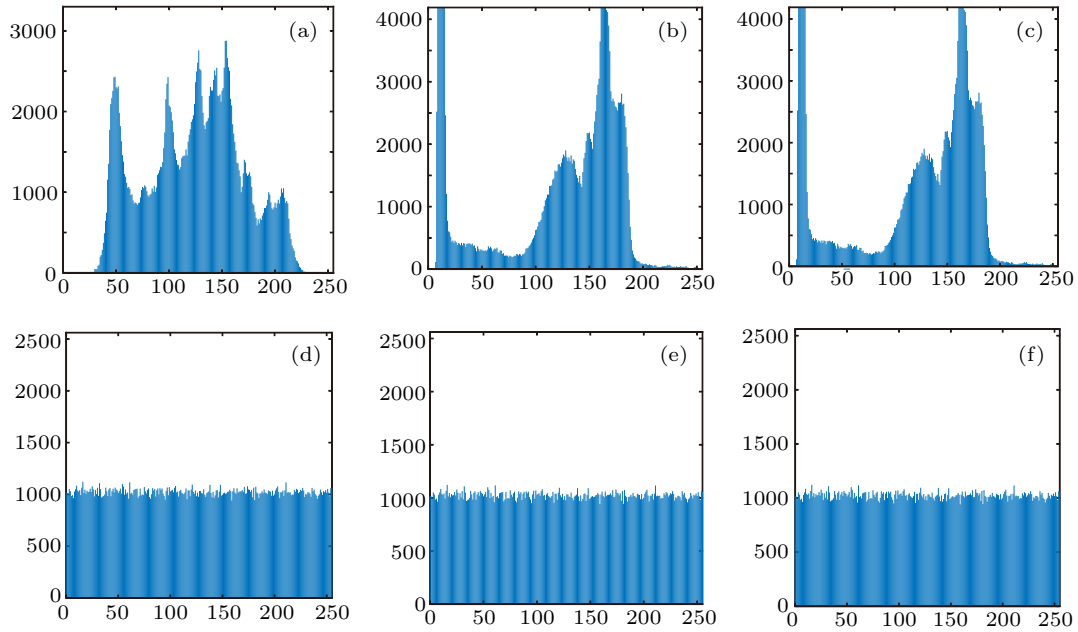


Fig. 11. Gray histogram of plaintext of (a) Lena, (b) Cameraman, (c) Girl; gray histogram of ciphered image of (d) Lena, (e) Cameraman, and (f) Girl.

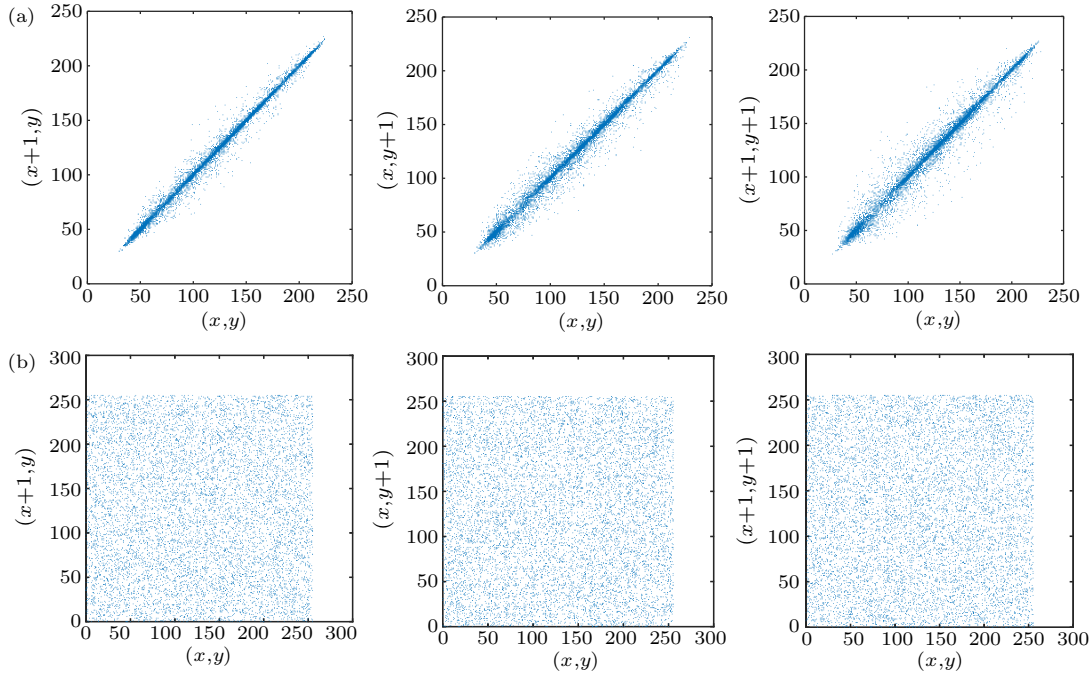


Fig. 12. Correlation distribution of (a) plaintext and (b) ciphertext image in horizontal, vertical, and diagonal direction of Lena.

Table 4. Correlation coefficients of plain image and cipher image.

Test image	Plain image			Cipher image		
	Horizontal	Vertical	Diagonal	Horizontal	Vertical	Diagonal
Lena (proposed)	0.99570	0.98470	0.99080	–0.00570	0.00160	0.00210
Lena (Ref. [17])	0.97190	0.94260	0.91990	0.01020	0.00670	0.00520
Lena (Ref. [20])	0.96457	0.97864	0.95098	–0.02457	–0.02264	–0.01930
Cameraman	0.99290	0.98040	0.98810	0.00590	0.00800	–0.00170
Girl	0.99620	0.98970	0.99270	0.00830	0.00520	–0.00460

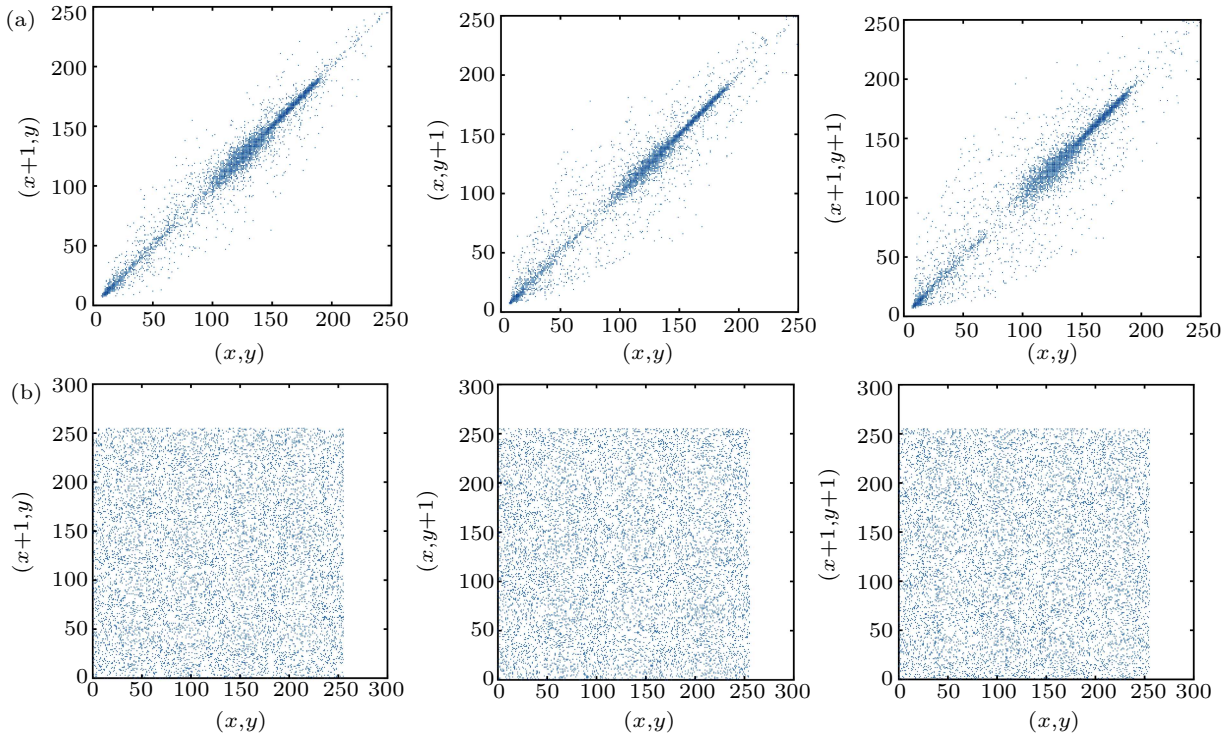


Fig. 13. Correlation distribution of (a) plaintext and (b) ciphertext image in horizontal, vertical, and diagonal direction of Cameraman.

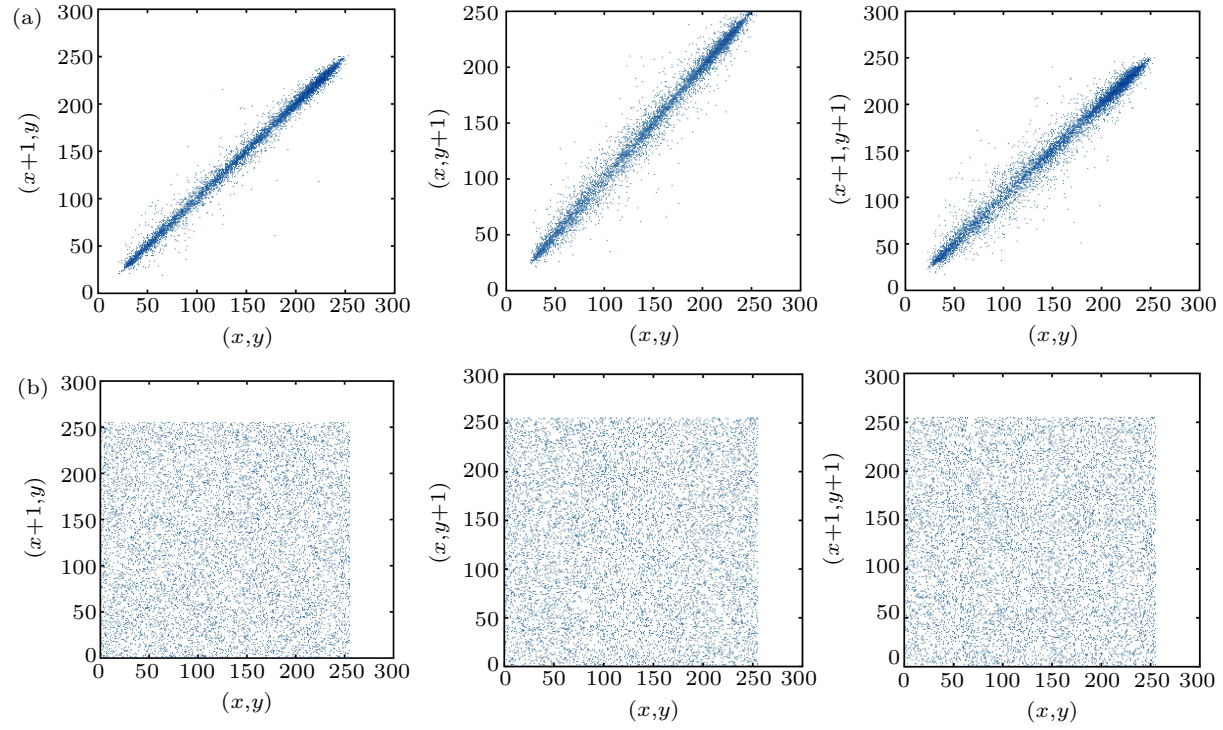


Fig. 14. Correlation distribution of (a) plaintext and (b) ciphertext image in horizontal, vertical, and diagonal direction of Girl.

4.2.3. Information entropy analysis

Information entropy reflects the uncertainty of image information. It is generally believed that the larger the entropy value, the greater the uncertainty of the image information is. The entropy of the image is given by[25]

$$H(X) = -\sum_{i=1}^{L} P_{\mathrm{r}}(I_i) \log_2 P_{\mathrm{r}}(I_i), \tag{12}$$

where X is the information entropy, and $P_{\mathrm{r}}(I_i)$ is the probability of I_i. In the formula, the L is the number of gray levels of the pixel. For an image with 256 Grey levels the theoretical value of $H(X)$ is 8 bits per pixel. Therefore, for an encrypted image, the closer to 8 the information entropy, the better the security performance of the encryption is. In Table 5 recorded are the information entropy of plaintext images and ciphertext images of test images used in this paper and other literature. We can find that the encrypted scheme has excellent performance as the information entropy of the cipher images is close to 8.

Table 5. Information entropy of test images.

Test image	Plaintext image	Ciphertext image
Lena (proposed)	7.39820	7.96920
Lena (Ref. [17])	–	7.99740
Lena (Ref. [20])	7.43087	7.98859
Cameraman	7.00060	7.96820
Girl	7.49570	7.98780

4.2.4. Plaintext sensitivity analysis

A new ciphertext image can be obtained by changing the pixels of the plaintext image slightly. By comparing the differences between the two ciphertext images, we can see whether the encryption system has strong plaintext sensitivity, a system with good plaintext sensitivity can effectively resist any selected plaintext attack or known plaintext attack. Therefore, if a small change in the plaintext image can cause a big change in the ciphertext image, the encryption system cannot be broken by selected plaintext attack or known plaintext attack. In general, there are qualitative method and quantitative method to measure the differences between two images of the same size. This paper mainly uses the following three indicators to quantitatively analyze the performance of encryption scheme against known plaintext attacks.

Compare the pixel values of the corresponding positions of two images and record the proportions of different pixel numbers to all pixel points. The calculation formula of number of pixel change rate (NPCR) is as follows:[26]

$$\mathrm{NPCR}(P_1, P_2) = \frac{1}{MN} \sum_{i=1}^{M} \sum_{i=1}^{N} |\mathrm{Sign}(P_1(i,j) - P_2(i,j))| \times 100\%, \tag{13}$$

where P_1 and P_2 represent two images of the same size, whose sizes are $M \times N$. Sign$(\cdot)$ denotes the sign function and its representation is shown below:[25]

$$\mathrm{Sign}(x) = \begin{cases} 1, & x > 0, \\ 0, & x = 0, \\ -1, & x < 0. \end{cases} \tag{14}$$

If two images are random images, then for any position, the probability with which the pixel values of two images are the same is 1/256 and the probability with which the pixel values of two images are different is 255/256. Due to the randomness of the location, the theoretical expected value of NPCR for two random images is about 99.6094%.

Compare the values of the pixels at the corresponding positions of the two images,record their differences and then calculate the average valuess of the ratio of the differences of the pixels at all corresponding positions to the maximum difference. The expression of unified average changing intensity (UACI) is shown below:[26]

$$\mathrm{UACI}(P_1, P_2) = \frac{1}{MN} \sum_{i=1}^{M} \sum_{i=1}^{N} \frac{|P_1(i,j) - P_2(i,j)|}{255 - 0} \times 100\%, \tag{15}$$

where P_1 and P_2 represent two images of the same size. UACI is used to compare different degrees of pixels at the corresponding positions of two images. When NPCR $= 1$, the theoretical expectation of UACI is 33.4635%.

Now, we come to compare the differences between two images P_1 and P_2. First we calculate their difference image $D = |P_1 - P_2|$. Second, we divide an image of size $M \times N$ into $(M-1) \times (N-1)$ image blocks, each with a size of 2×2. Third, we compute the average value of the absolute value of the difference between any two elements in each small image. For example, the i-th little image block is denoted as[26]

$$D_i = \begin{bmatrix} d_{i1} & d_{i2} \\ d_{i3} & d_{i4} \end{bmatrix}. \tag{16}$$

The average value of the absolute value of the difference between any two elements is as follows:[25]

$$m_i = \frac{1}{6}(|d_{i1} - d_{i2}| + |d_{i1} - d_{i3}| + |d_{i1} - d_{i4}| + |d_{i2} - d_{i3}| + |d_{i2} - d_{i4}| + |d_{i3} - d_{i4}|). \tag{17}$$

Finally, we calculate the ratio of the average value of the m_i of all small image blocks to the maximum difference among the pixel points, and name it block average changing intensity (BACI), whose definition is shown in Eq. (15),[25]

$$\mathrm{BACI}(P_1, P_2) = \frac{1}{(M-1)(N-1)} \sum_{i=1}^{(M-1)(N-1)} \frac{m_i}{255}, \tag{18}$$

where P_1 and P_2 represent two images of the same size. For two images, when NPCR and UACI are close to their own ideal values, it is also possible to present a similar visual effect. This indicates that the NPCR and UACI are defective

in describing the difference between two images, while BACI can make up for the deficiency. The expected value of BACI is 26.7712%.

In this paper, we modify one pixel value of test images. In two different encryption processes, the values of NPCR, UACI, and BACI are calculated and listed in Table 6.

Table 6. Values of NPCR, UACI, and BACI of different images after modifying one pixel value.

Test image	NPCR/%	UACI/%	BACI/%
Lena	99.62	33.42	26.73
Cameraman	99.59	33.54	26.79
Girl	99.60	33.43	26.76

As we can see from the table given above, within a certain error tolerance range, the three values are relatively close to the ideal value, which shows that the encryption scheme proposed in this paper can better resist differential attacks.

4.2.5. Key space

Key space is a collection of all legal keys. A good encryption scheme should have enough key space to resist brute force attacks. On 64-bit computers, the precision of a double floating-point number can attain 10^{-15}. In this paper, the key is composed of seven initial values of two chaotic systems. Therefore, the key space can reach $10^{15} \times 10^{15} \times 10^{15} \times 10^{15} \times 10^{15} \times 10^{15} \times 10^{15} \approx 2^{349}$. In other words, the length of the key is 349 bits. Obviously, the encryption system has a very large key space, which can effectively withstand exhaustive attacks and brute force cracking.

5. Conclusions

In this paper, we proposed a novel four-dimensional hyper-chaotic system based on the flux-controlled memristor model, which has abundant dynamic behaviors. The basic dynamic theory analysis and numerical simulation, such as the stability of equilibrium point, the Lyapunov exponents, and dimension, Poincare maps, power spectrum, and waveform graph, prove that the system can produce complex chaotic attractors. Furthermore, the SPICE circuit of the system is established. The results of circuit simulation and numerical simulation are consistent, which proves the feasibility, effectiveness, and the ability to generate chaos of this system. Finally, an image encryption scheme is designed based on the proposed novel hyper-chaotic system. In order to improve the security of image information, the scheme includes double encryptions. The performances of the encryption scheme are further verified through key space, information entropy, differential attack, and correlation analysis. The above experiments provide a certain foundation for the applications of novel hyper-chaotic systems in image encryption, hoping that this field will have a major breakthrough in the future.

References

[1] Lorenz E N 1963 *J. Atmos. Sci.* **20** 130
[2] Chen G R 1999 *Int. J. Bifurcat. Chaos.* **9** 1465
[3] Bao B C, Liu Z and Xu J P 2009 *J. Syst. Eng. Electron.* **20** 1179
[4] Xiao Y Q, Wang Z Y, Cao J, Long C X, Chen Y T, Deng R, Shi J and Liu Y 2019 *Opt. Commun.* **440** 126
[5] Chua L O 1971 *IEEE Trans. Circ. Theor.* **18** 507
[6] Strukov D B, Snider G S, Stewart D R and Williams R S 2008 *Nature* **453** 80
[7] Yang Y C, Pan F, Liu Q, Liu M and Zeng F 2009 *Nano. Lett.* **9** 1636
[8] Shin S H, Kim Kyungmin and Kang S M 2010 *IEEE Trans.* **10** 1536
[9] Itoh M and Chua L O 2008 *Int. J. Bifurcat. Chaos* **18** 3183
[10] Kyprianidis I M, Volos Ch K and Stouboulos I N 2010 *AIP Conf. Proc.* **1203** 626
[11] Stork M, Hrusak J and Mayer D 2009 *Electrical and Electronics Engineering*, December 2009
[12] Yang D W, Wang L D, Duan S K 2018 *Acta Phys. Sin.* **67** 110502 (in Chinese)
[13] Lv Y W and Min F H 2019 *Acta Phys. Sin.* **68** 130502 (in Chinese)
[14] Wang M J, Deng Y, Liao X H, Li Z J, Ma M L and Zeng Y C 2019 *Int. J. Nonlinear Mech.* **111** 149
[15] Li C H, Luo G C and Qin K 2017 *Nonlinear Dyn.* **87** 127
[16] Wang X Y, Wang Y, Wang S W, Zhang Y Q and Wu X J 2018 *Chin. Phys. B* **27** 110502
[17] Ye X L, Wang X Y, Gao S, Mou J, Wang Z S and Yang F F 2019 *Nonlinear Dyn.* **99** 1489
[18] Wang L M, Dong T D and Ge M F 2019 *Appl. Math. Comput.* **347** 293
[19] Zhang Y and Tang Y J 2017 *Multimed. Tools Appl.* **77** 6647
[20] Yang F F, Mou J, Sun K H, Cao Y H and Jin J Y 2019 *IEEE Access*
[21] Zhang L M, Sun K H, Liu W H and He S B 2017 *Chin. Phys. B* **26** 100504
[22] Wang B, Zou F C and Cheng J 2018 *Optik* **154** 538
[23] Wang X Y, Xie Y X and Qin X 2012 *Chin. Phys. B* **21** 040504
[24] Wang Z L, Min F H and Wang E R 2016 *AIP Adv.* **6** 095316
[25] Shi H, Wang L D 2019 *Acta Phys. Sin.* **68** 200501 (in Chinese)
[26] Zhang Y 2016 *Chaos digital image encryption* Vol. 1 (Beijing: Tsinghua University Press) p. 218 (in Chinese)