IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 22 October 2023, accepted 17 December 2023, date of publication 25 December 2023,
date of current version 8 January 2024.

*Digital Object Identifier 10.1109/ACCESS.2023.3347448*

RESEARCH ARTICLE

# Dynamic Analysis of a Four-Wing Chaotic System and Application in Image Encryption Based on Compressive Sensing

**LI ZHANG[1] AND XIN-LEI AN[2]**
[1]Basic Courses Department, Lanzhou Institute of Technology, Lanzhou 730050, China
[2]School of Mathematics and Physics, Lanzhou Jiaotong University, Lanzhou 730070, China

Corresponding author: Li Zhang (zhangli.01@126.com)

This work was supported in part by the National Natural Science Foundation under Grant 11962012, in part by the Key Project of the Gansu Province Natural Science Foundation of China under Grant 23JRRA861, and in part by the Youth Science and Technology Innovation Project of the Lanzhou Institute of Technology under Grant 2021KJ-08.

**ABSTRACT** Compared with the conventional multi-scroll attractor, the multi-wing butterfly chaotic attractors are easier to design and implement through analog circuitry, thus they has more potential applications. To explore the dynamic property of the multi-wing butterfly system and its application to image encryption. A chaotic system with four-wing attractors is designed and the dynamic behaviors are analyzed in terms of phase diagram, bifurcation diagram, Lyapunov exponential spectrum and $C_0$ structural complexity. It is found that each parameter has a large range of intervals that can keep the system in the chaotic state and the generated sequences have sufficient pseudorandom to be well suited for application in secure communications. Then, the circuit model of the constructed four-wing chaotic system is built with a basic operational amplifier circuit, and the accuracy of the circuit implementation is verified. Finally, a color image compression encryption scheme is designed based on the theory of compressive sensing and DNA dynamic coding. The algorithm is mainly composed of five parts: sparse, compression calculation, 3D projection scrambling, DNA diffusion and plaintext association confusion. The security test results show that the designed scheme not only has superior compression performance and high security, but also has no limitation on the size of the test image.

**INDEX TERMS** Four-wing attractor, compressive sensing, DNA encoding, color image encryption, multisim circuit simulation.

## I. INTRODUCTION

With the rapid development of electronic information technology, a lot of image information is continuously transmitted and stored all the time [1], [2], [3], [4], [5]. And there is no shortage of image communication containing some extremely secret and important information. Once the information is leaked, it will cause irreversible effects. For example, if the images involving military information or medical information are leaked or tampered with, it will threaten the security of individuals and even the country. Then how to ensure the security of image information in the transmission process becomes an important issue that people pay attention to. It is worth mentioning that with its inherent ergodicity, randomness and sensitivity to initial conditions, chaotic systems are widely used in the field of image encryption [6], [7], [8], [9], [10], [11], [12], [13], [14], [15].

DNA technology has the advantages of high parallelism and high information density. To improve the security, some researchers have combined DNA technology with chaotic encryption [16], [17], [18], [19], [20], [21], [22], [23], [24], [25], [26], [27], [28]. Xiong et al. [16] proposed a memristor circuit system and designed an image encryption algorithm to verify the image encryption application of the memristive system based on DNA variation. Shi et al. [17] constructed a fractional hyper-chaotic system and designed a

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

color image encryption scheme combine with DNA dynamic coding. In the literature [18], a three-dimensional discrete hyperchaotic map is introduced on the basis of the Marotto theorem and then an improved color image encryption scheme is designed. A color image cryptosystem based on dynamic DNA encryption and chaos is presented in the literature [19]. Different from the traditional DNA sequence operation according to binary calculation, a diffusion pattern based on random numbers related to plaintext is proposed. Chen et al. [20] cracked an image encryption scheme based on two-dimensional Hénon-sin map and DNA encoding. The proposed concept of extending DNA encryption to s-box replacement is expected to contribute to the security evaluation and theoretical design of future DNA-based image encryption schemes. Belazi et al. [21] proposed a new chaos-based medical images encryption scheme which is based on the combination of chaos and DNA computation and follows a permutation-substitution-diffusion structure.

Performing the corresponding compression operation before image encryption can effectively reduce the storage and transmission costs. Since compressive sensing (CS) theory was proposed in 2006 [29], many image encryption schemes based on CS theory have been proposed [30], [31], [32], [33], [34], [35], [36], [37], [38], [39]. In the literature [30], an image encryption algorithm based on CS theory and hyperchaotic map is presented, including permutation, compression and diffusion processes. Yang et al. [31] defined a fractional-order memristor chaotic circuit system and introduced a new color image compression and encryption algorithm based on the constructed circuit system. Based on a four-wing hyperchaotic system combining CS theory and DNA coding, an image encryption scheme is proposed in the literature [32]. The measurement matrix is constructed by combining the Kronecker product (KP) with the chaotic system, and the KP is used to extend the low-dimensional seed matrix to the high-dimensional measurement matrix. In order to reduce the storage space of the measurement matrix and improve memory usage, Wen et al. [33] proposed a CS strategy based on the semitensor product and submitted an image compression encryption scheme with visual security. In the literature [34], an efficient image compression and encryption algorithm based on chaotic system and CS theory is introduced to overcome the drawback that linear image encryption systems are vulnerable to selective plaintext attacks and to reduce the correlation between encrypted image pixels. To improve the security of the image encryption system, Gong et al. [35] proposed an optical image compression encryption scheme based on CS theory and RSA public-key cryptographic algorithm, which uses the optical compression imaging system to sample the original image.

In order to improve the security of the encryption algorithm while saving transmission bandwidth and storage space, a color image compression and encryption scheme is designed in this paper. The algorithm is mainly composed of five parts: sparse, compression calculation, 3D projection scrambling, DNA diffusion and plaintext association confusion. The main contributions are as follows.

(1) A four-wing chaotic system is constructed and its comprehensive dynamics analysis are realized. The simulation results show that the system has complex dynamic behavior and enough randomness to be applied to the field of chaotic cryptography. The circuit design and Multisim simulation results are in good agreement with the theoretical analysis results.

(2) Based on CS theory and DNA coding technology, a color image compression and encryption scheme is designed. The proposed 3D projection confusion scheme can effectively minimize the correlation between the components of color images.

(3) The experimental results show that the encryption scheme has excellent compression and encryption effects and good practical application prospects.

The rest parts are arranged as follows. Section II constructed a four-wing chaotic system and explored the basic properties. In Section III, some detailed analysis of the model dynamic behavior is investigated and the analog circuit of the system is designed and implemented through the Multisim platform. Section IV gives some basics and the designed image compression encryption scheme. In Section V, a detailed analysis of the security performance of the algorithm is provided. Finally, Section VI gives some conclusions.

## II. THE FOUR-WING CHAOTIC SYSTEM AND ITS BASIC PROPERTIES

### A. MATHEMATICAL MODEL

The 4D autonomous system is described by:

$$\begin{cases} \dot{x} = -ax + ez - yzw \\ \dot{y} = -by + fw - xzw \\ \dot{z} = c(w - z) - xyw \\ \dot{w} = d(w + z) + xyz \end{cases} \tag{1}$$

where $x, y, z, w$ are the state variables and $a, b, c, d, e, f$ are real parameters. Especially, every equation contains a cube, which ensure the system can exhibit abundant dynamical behaviors.

### B. SYMMETRY AND DISSIPATION

When the transformation is $(x, y, z, w) \to (-x, -y, -z, -w)$, system (1) is symmetric. That is to say, the system is symmetric about the origin.

For the system, we have

$$\nabla V(t) = \frac{\partial \dot{x}}{\partial x} + \frac{\partial \dot{y}}{\partial y} + \frac{\partial \dot{z}}{\partial z} + \frac{\partial \dot{w}}{\partial w} = -a - b - c + d \tag{2}$$

where $V(t)$ denotes the volume of the region in $R^3$ with smooth boundaries. It is well known that $V(t) = \exp(et)V(0)$ by Liouville's theorem, which means that any volume in $R^3$ will shrink to zero exponentially and rapidly. When $-a - b - c + d < 0$, $\nabla V(t) < 0$. Therefore, in order

to ensure the dissipation, the selection of parameters in this paper needs to meet the condition $-a-b-c+d<0$.

### C. EQUILIBRIUM AND STABILITY

Setting

$$\begin{cases} -ax+ez-yzw=0 \\ -by+fw-xzw=0 \\ c(w-z)-xyw=0 \\ d(w+z)+xyz=0 \end{cases} \tag{3}$$

Obviously, $S_0=[0,\ 0,\ 0,\ 0]$ is one equilibrium. Furthermore, one can obtain

$$\begin{cases} \dfrac{A}{2d}z^4-fBz^2-bC=0 \\ x=Az \\ y=\dfrac{C}{z} \\ w=-Bz \end{cases} \tag{4}$$

where $A=(e\pm\sqrt{\frac{de^2+2ac(c+3d\pm\sqrt{c^2+d^2+6cd})}{d}})/2a, B=c+d\pm\sqrt{c^2+d^2+6cd}/2d$ and $C=a(c-d\pm\sqrt{c^2+d^2+6cd})/(e\pm\sqrt{\frac{de^2+2ac(c+3d\pm\sqrt{c^2+d^2+6cd})}{d}})$.

Setting $\sqrt{c^2+d^2+6cd}=g$, $c+3d+g=p, c+3d-g=q, c+d+g=m, c+d-g=n, c-d+g=s, c-d-g=t, \sqrt{f^2(c+d\pm g)^2+4bd(c+d\pm g)(c-d\pm g)}=k, e\pm\sqrt{de^2+2ac(c+3d\pm g)/d}=h,\ fm+k=l, fm-k=r$.

Then one can get

$$x_{11}=\sqrt{ahl/m}\Big/2a, x_{12}=\sqrt{ahr/m}\Big/2a, x_{13}=\sqrt{ahl/n}\Big/2a,$$
$$x_{14}=\sqrt{ahr/n}\Big/2a, x_{21}=\sqrt{am/hl}, x_{22}=\sqrt{am/hr},$$
$$x_{23}=s\sqrt{an/hl},\ x_{24}=s\sqrt{an/hr}, x_{31}=\sqrt{al/hm},$$
$$x_{32}=\sqrt{ar/hm},\ x_{33}=\sqrt{al/hn},\ x_{34}=\sqrt{ar/hn},$$
$$x_{41}=-\sqrt{aml/h}\Big/2d,\ x_{42}=-\sqrt{amr/h}\Big/2d,$$
$$x_{43}=-\sqrt{anl/h}\Big/2d,\ x_{44}=-\sqrt{anr/h}\Big/2d.$$

From the above analysis, it can be seen that the system has nine equilibria which can be divided into the following five groups:

(1) The first group of equilibria is $S_1=[x_{11},\ x_{21},\ x_{31},\ x_{41}]$ and $S_2=-S_1$;

(2) The second group of equilibria is $S_3=[x_{12},\ x_{22},\ x_{32},\ x_{42}]$ and $S_4=-S_3$;

(3) The third group of equilibria is $S_5=[x_{13},\ x_{23},\ x_{33},\ x_{43}]$ and $S_6=-S_5$;

(4) The fourth group of equilibria is $S_7=[x_{14},\ x_{24},\ x_{34},\ x_{44}]$ and $S_8=-S_7$;

(5) The fifth group of equilibrium is the origin.

When $a=9, b=38, c=50, d=5, e=5, f=2$, the nine equilibria are

$S_0=(0,0,0,0)$, $S_1=(4.5,-3.7,2.6,5.3)$,
$S_2=(3.5,5.2,-1.8,4.2)$, $S_3=(-14.5,-10,-5.4,1.2)$,
$S_4=(-15.1,11.2,4.9,1.3)$, $S_5=(-4.5,3.7,-2.6,-5.3)$,
$S_6=(-3.5,-5.2,1.8,-4.2)$, $S_7=(14.5,10,5.4,-1.2)$,
$S_8=(15.1,-11.2,-4.9,-1.3)$.

Since the system is symmetrical about the origin, we only need to analyze the stability of equilibrium points $S_0, S_1, S_3, S_5$ and $S_7$.

Linearizing the Eq. (3) at the equilibrium point $S_0$, the Jacobian matrix is obtained as

$$J_{S_0}=\begin{bmatrix} -9 & 0 & 5 & 0 \\ 0 & -38 & 0 & 2 \\ 0 & 0 & -50 & 50 \\ 0 & 0 & 5 & 5 \end{bmatrix} \tag{5}$$

And its characteristic equation is

$$(\lambda+9)(\lambda+38)(\lambda^2+45\lambda-500)=0 \tag{6}$$

Obviously, there are four nonzero eigenvalues $\lambda_0^1=-9$, $\lambda_0^2=-38, \lambda_0^3=-54.22, \lambda_0^4=9.22$. According to the Routh-Hurwitz criterion, the equilibrium point $S_0$ is an unstable saddle point.

Similarly, the eigenvalues at the equilibrium point $S_1$ are $\lambda_1^1=-35.85, \lambda_1^2=-69.53, \lambda_1^{3,4}=6.69\pm28.83i$. Obviously, there are two conjugate complex roots with positive real part, and two real roots which is less than zero, according to Routh-hurwitz criterion, the equilibrium point $S_1$ is an unstable node focus.

And at the equilibrium points $S_3, S_5$ and $S_7$, the characteristic roots of them are calculated to be

$$\lambda_3^1=-35.07,\ \lambda_3^2=-63.22, \lambda_3^{3,4}=3.15\pm8.02i;$$
$$\lambda_5^{1,2}=-20.21\pm144.37i,\ \lambda_5^{3,4}=-30.79\pm8.33i;$$
$$\lambda_7^1=-17.85,\ \lambda_7^2=-65.62, \lambda_7^{3,4}=-4.26\pm187.58i.$$

According to Routh-Hurwitz criterion, $S_3$ is unstable node focus, $S_5$ is stable focus and $S_7$ is stable node focus.

## III. DYNAMICS ANALYSIS

In this section, the dynamical properties of the system (1) are analyzed in detail by means of phase diagrams, bifurcation diagrams, Lyapunov exponent spectrum, and $C_0$ structural complexity. It is worth noting that in the following numerical calculations, the fourth Runge-Kutta algorithm is used for the solution. In addition, for the convenience of discussion, the initial values of the system are fixed as (0.1, 0.2, 0.3, 0.4).

### A. PHASE DIAGRAM

The phase diagram can be used to visualize the motion of the system and then the reciprocating aperiodic motion characteristics of chaotic motion can be observed. And in finite phase

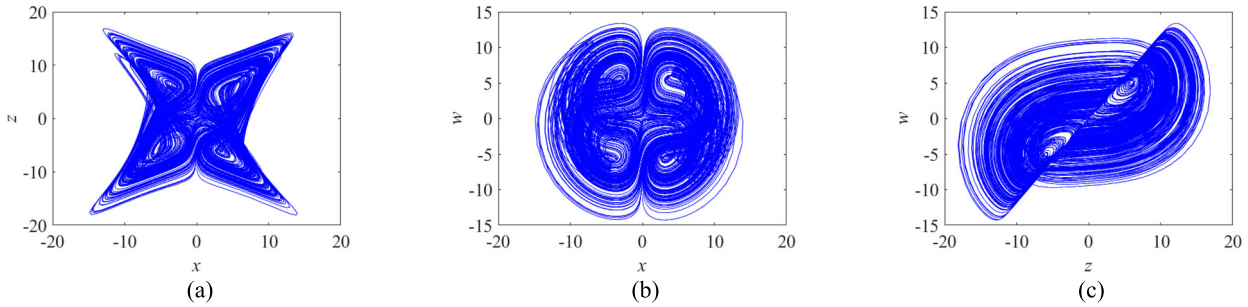


**FIGURE 1.** Typical chaotic attractors (a) x-z plane, (b) x-w plane, (c) z-w plane.

space, the larger the space occupied by the system trajectory, the better the randomness and ergodicity of the system.

In this section, the system parameters are selected as $a = 9, b = 38, c = 50, d = 5, e = 5, f = 2$. Several typical chaotic attractors of the system are obtained by numerical simulation as shown in Fig.1. As can be seen from the figure, the chaotic attractors of the system occupy a considerable space, indicating that the system has excellent ergodicity in terms of obtaining chaotic sequences with better pseudorandom properties.

### B. BIFURCATION DIAGRAM

The variation of the system with parameters can be visualized from the bifurcation diagram. When the control parameters are changed, the motion state of the system will be changed essentially.

Fig. 2 gives the bifurcation diagram with different parameter intervals. It can be seen from the figure that the output trajectory points of the system are randomly distributed with alternating periodic and chaotic windows over different parameter ranges, and there is always a large chaotic cross-section. In addition, one can also observe various bifurcation behaviors such as folding bifurcation, tangent bifurcation and internal crisis bifurcation. In other words, the system has relatively complex dynamic behavior and has enough potential to be applied in the field of secure communication.

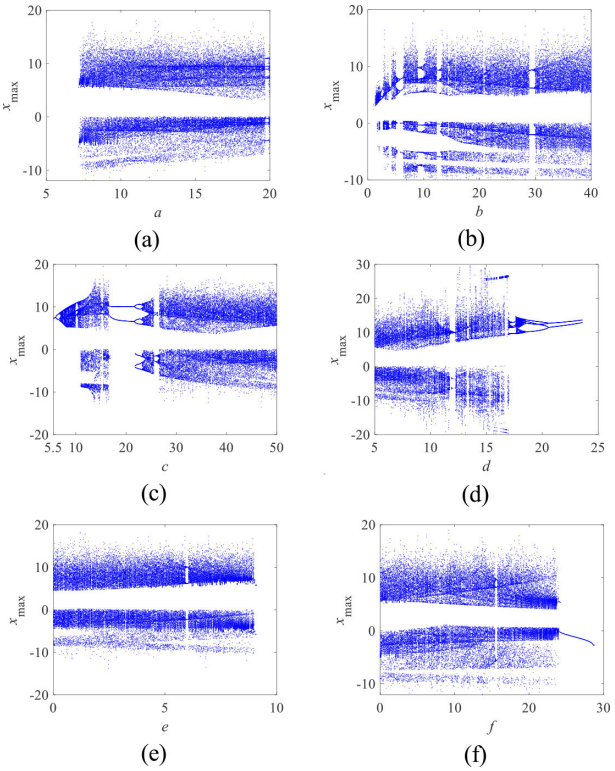


**FIGURE 2.** Bifurcation diagram with (a) $a \in [5, 20]$, (b) $b \in [0, 40]$, (c) $c \in [5.5, 50]$, (d) $d \in [5, 25]$, (e) $e \in [0, 10]$, (f) $f \in [0, 30]$.

### C. LYAPUNOV EXPONENT SPECTRUM (LEs)

Lyapunov exponent describes the time asymptotic separation rate of adjacent trajectories in the dynamic system, which can be used as an important index to distinguish whether the system is chaotic. And the positive Lyapunov exponent usually indicates that the system is chaotic.

Take the system parameter as $a = 9, b = 38, c = 50, d = 5, e = 5, f = 2$. After calculation, the Lyapunov exponent of the system is $\lambda_1 = 3.0697, \lambda_2 = 0, \lambda_3 = -37.7339, \lambda_4 =$ -57.3261. And according to Kaplan-Yorke conjecture, the corresponding Lyapunov dimension is $D_L = 2.0814$. Obviously, the system is chaotic under this set of parameters.

The LEs with different parameters are given in Fig. 3. It should be noted that the third and fourth exponents are always much smaller than zero, so they are omitted from the figure. As can be seen from the figure that system always has a positive Lyapunov exponent within a large range of parameters. That is to say the system has a large chaotic interval and thus has the potential to generate chaotic sequences with a higher degree of randomness. More importantly, it can be observed that the LEs and the bifurcation diagrams change in a consistent manner.

### D. COMPLEXITY CHAOTIC DIAGRAM OF DIFFERENT PARAMETER

In fact, the complexity of a chaotic system is one of the methods to portray its dynamics and has the same observation as phase diagram, bifurcation diagram and LEs. Complexity is the degree to which a chaotic sequence

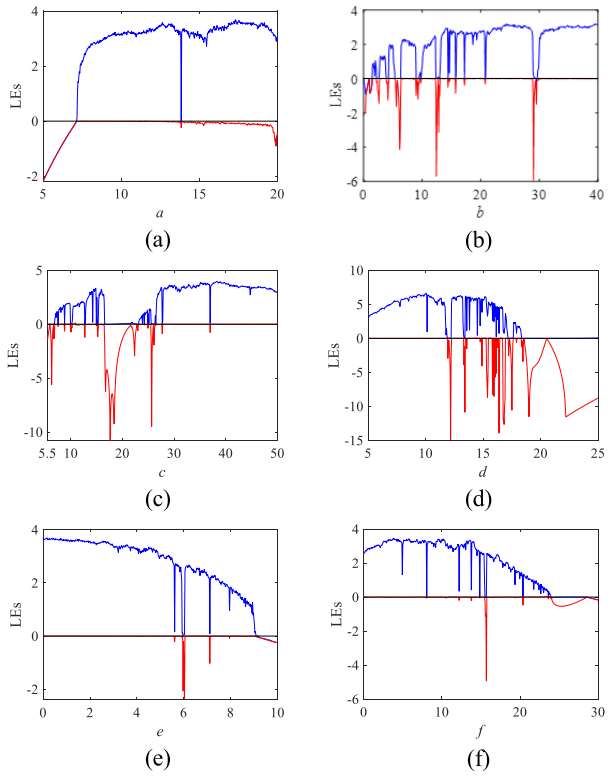


**FIGURE 3.** LEs with (a) $a \in [5, 20]$, (b) $b \in [0, 40]$, (c) $c \in [5.5, 50]$, (d) $d \in [5, 25]$, (e) $e \in [0, 10]$, (f) $f \in [0, 30]$.

is close to a random sequence. In general, the larger the value of complexity is, the closer the sequence is to a random sequence and the higher the corresponding security. Therefore, complexity is an important indicator for testing the randomness of a sequence. Moreover, the complexity of chaotic sequences is divided into behavioral complexity and structural complexity. Where, the structural complexity refers to the complexity of a sequence by analyzing the frequency characteristics and energy spectrum characteristics in the transform domain. The more balanced the energy spectrum distribution in the transform domain of the sequence, the closer the original sequence is to the random signal, and the higher the complexity of the sequence. More importantly, compared with the behavioral complexity, the structural complexity has more global statistical significance.

In this section, the complexity of the system is analyzed by the $C_0$ structural complexity algorithm. The main calculation idea of $C_0$ complexity is to decompose the sequence into regular and irregular components, and its measurement value is the proportion of irregular components in the sequence. The specific calculation steps are as follows.

**Step 1** The discrete Fourier transform is applied to the chaotic pseudo-random sequence $\{x(n)\}_0^{N-1}$ with length of $N$ by

$$X(k) = \sum_{n=0}^{N-1} x(n) e^{-j\frac{2\pi}{N}nk} = \sum_{n=0}^{N-1} x(n) W_N^{nk} \tag{7}$$

where $k = 0, 1, \ldots, N-1$.

**Step 2** Let the mean square value of $\{X(k)\}_0^{N-1}$ be

$$G_N = \frac{1}{N} \sum_{k=0}^{N-1} |X(k)|^2 \tag{8}$$

The parameter $r$ is introduced to retain the spectrum that exceeds $r$ times than the mean square value, and the rest is regarded as zero, that is

$$\tilde{X}(k) = \begin{cases} X(k), & |X(k)|^2 > rG_N \\ 0, & |X(k)|^2 \le rG_N \end{cases} \tag{9}$$

**Step 3** The inverse Fourier transform is applied to $\tilde{X}(k)$ as

$$\tilde{x}(n) = \frac{1}{N} \sum_{k=0}^{N-1} \tilde{X}(k) e^{j\frac{2\pi}{N}nk} = \frac{1}{N} \sum_{k=0}^{N-1} \tilde{X}(k) W_N^{-nk} \tag{10}$$

where $n = 0, 1, \ldots, N-1$.

**Step 4** Define $C_0$ complexity as

$$C_0(r, N) = \sum_{n=0}^{N-1} |x(n) - \tilde{x}(n)|^2 \Big/ \sum_{n=0}^{N-1} |x(n)|^2 \tag{11}$$

Keep the initial value of the system unchanged and some classic complexity chaotic images are shown in Fig. 4. The depth of the image color represents the complexity of the chaotic system under this parameter range. The darker color indicates the higher complexity value of the system and the corresponding sequence randomness. On the contrary, the lighter the color, the lower the complexity value is gotten and the worse the sequence randomness is. It can be seen from the figure that the system is in the chaotic state within a large range of parameters. In addition, one can also observe that the $C_0$ complexity diagrams are consistent with the bifurcation diagrams and LEs diagrams.

### E. CIRCUIT DESIGN FOR THE CHAOTIC ATTRACTOR

The dynamics of many chaotic systems are validated by Circuit realization [43]. To made the experiments effectively, so the variation of state variables is kept within the tolerable voltage range for integrated circuit. Reduce the chaotic output level to 1/200 of the original one, and set $m = 200x, n = 200y, u = 200z, v = 200w$. Because the transformations of system variable do not affect the state and function, so let $x_1 = m, x_2 = n, x_3 = u, x_4 = v$. The original system is described

$$\begin{cases} \dot{x}_1 = -ax_1 + ex_3 - 40000x_2x_3x_4 \\ \dot{x}_2 = -bx_2 + fx_4 - 40000x_1x_3x_4 \\ \dot{x}_3 = c(x_4 - x_3) - 40000x_1x_2x_4 \\ \dot{x}_4 = d(x_4 + x_3) + 40000x_1x_2x_3 \end{cases} \tag{12}$$

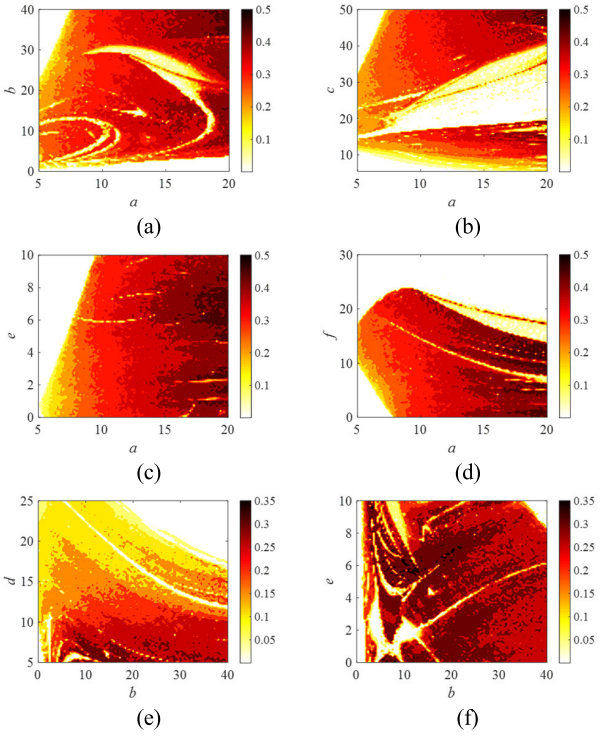


**FIGURE 4.** $C_0$ complexity with (a) $a \in [5, 20]$, $b \in [0, 40]$, (b) $a \in [5, 20]$, $c \in [5.5, 50]$, (c) $a \in [5, 20]$, $e \in [0, 10]$, (d) $a \in [5, 20]$, $f \in [0, 30]$, (e) $b \in [0, 40]$, $d \in [5, 25]$, (f) $b \in [0, 40]$, $e \in [0, 10]$.

Based on the circuit theory and characteristics of components, the circuit equations is

$$\begin{cases} \dot{U}_1 = -\dfrac{R_4R_7}{R_1R_5R_6C_1}U_1 + \dfrac{R_4}{R_2R_5C_1}U_3 - \dfrac{R_4R_{17}}{R_3R_5R_{13}C_1}U_2U_3U_4 \\ \dot{U}_2 = -\dfrac{R_{11}R_{44}}{R_8R_{12}R_{13}C_2}U_2 + \dfrac{R_{11}}{R_9R_{12}C_2}U_4 - \dfrac{R_{11}R_{28}}{R_{10}R_{12}R_{27}C_2}U_1U_3U_4 \\ \dot{U}_3 = \dfrac{R_{18}}{R_{15}R_{19}C_3}(U_4 - U_3) - \dfrac{R_7R_{18}}{R_6R_{17}R_{19}C_3}U_1U_2U_4 \\ \dot{U}_4 = \dfrac{R_{25}}{R_{22}R_{26}C_4}(U_4 + U_3) - \dfrac{R_{25}}{R_{24}R_{26}C_4}U_1U_2U_3 \end{cases} \tag{13}$$

Based on electronic circuitry design Principle and circuit equations, the designed circuit is shown in Fig. 5. The whole circuit consists of four parts: add and subtract operational circuit, integral circuit, inverting circuits and multiplication circuit. On the circuit, the model operational amplifier is TL084CN, the model multipliers is AD633, value of voltage is 12V.

Based on the above figure, build a circuit platform and test the circuit. Then get the Multisim11.0 simulation figure on the oscilloscope as shown in Fig.6. Obviously, the simulation figure in Fig.1 and Fig.6 are consistent.

## IV. APPLICATION IN IMAGE ENCRYPTION

### A. PRELIMINARY KNOWLEDGE

#### 1) COMPRESSIVE SENSING

From CS theory, the original signal can be reconstructed with high probability using a small fraction of non-adaptive

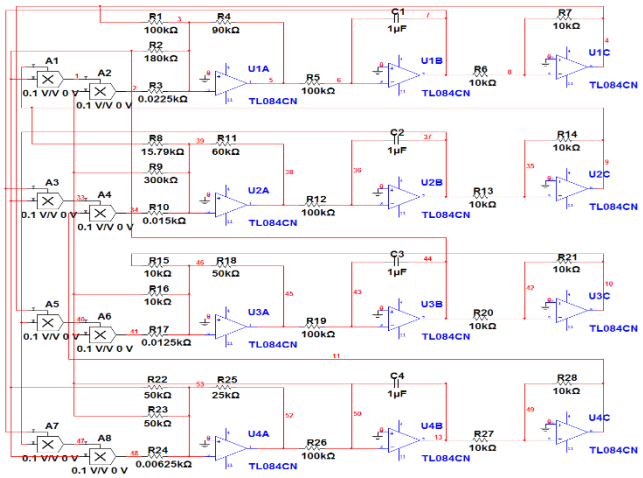

**FIGURE 5.** Circuit implementation of the 4D chaotic system.

projection values when the sparse signal is sampled at a sampling rate well below Nyquist. The main principle can be expressed as follows: the high-dimensional sparse signal is transformed into a low-dimensional signal using an observation matrix independent of the transformation basis, and then a small amount of high probability signal in that is used to reconstruct the original signal.

For an. $N \times 1$.dimensional signal $x = [x(1), x(2), \ldots, x(N)]^T$, it can be expressed as

$$x = \Psi\alpha = \sum_{i=1}^{N} \Psi_i\alpha_i \tag{14}$$

where $\Psi_i$ is the i-th column of $\Psi$ and $\alpha$ represents $N \times 1$ coefficient vector. If there are only $k$ non-zero elements in $\alpha$, the vector $x$ is called $k$-sparse. The common sparse transform methods primarily include discrete cosine transform (DCT), Fourier transform and discrete wavelet transform (DWT). And the operation of obtaining $M$ measurements from $x$ is

$$y = \Phi x = \Phi\Psi\alpha = \Theta\alpha \tag{15}$$

where $\Phi$ denotes the measurement matrix of size $M \times N$ and $\Theta = \Phi\Psi$ means the sensing matrix with size $M \times N$. If $M \ll N$, then $x$ can be considered as a linearly descending function from $R^N$ to $R^M$.

The process of signal reconstruction is actually that of finding the optimal solution to the underdetermined equation. Since the number of measurements $M$ in Eq. (13) is much smaller than the length $N$ of the signal, Eq. (13) is considered as an underdetermined equation, which usually has infinite number of solutions. Only when the measurement matrix $\Phi$ satisfies the Restricted Isometry Property (RIP) can it be ensured that Eq. (13) has only one $k$-sparse solution.

If for all $k$-sparse signals $x$, there exists $\delta_k \in (0, 1)$, such that the following inequality holds

$$(1 - \delta_k)||x||_2^2 \leq ||\Theta x||_2^2 \leq (1 + \delta_k)||x||_2^2 \tag{16}$$

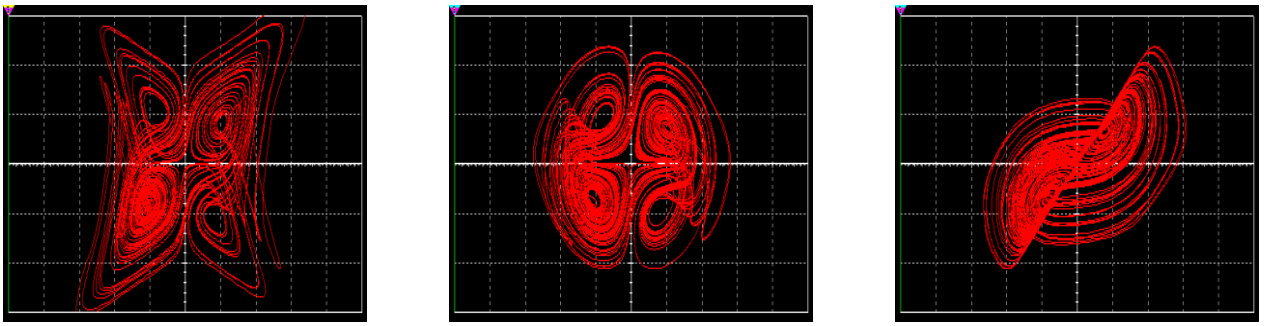


**FIGURE 6.** Experimental observations of the chaotic attractor in different planes, (a) $U_1 - U_3$(500$mV$/$Div$, 500$mV$/$Div$), (b) $U_1 - U_4$(500$mV$/$Div$, 500$mV$/$Div$), (c) $U_3 - U_4$(500$mV$/$Div$, 500$mV$/$Div$).

where $\delta_k$ denotes RIP constant of the sensing matrix $\Theta$. Then $\Theta$ is described as satisfying the $k$ order RIP [40].

And $\alpha$ can be accurately reconstructed by

$$\hat{\alpha} = \arg\min ||\alpha||_0, \quad s.t.\ y = \Phi\Psi\alpha = \Theta\alpha \tag{17}$$

where $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_N)$, and $||\alpha||_0$ denotes the number of non-zero elements in the vector $\alpha$.

### 2) CHAOS-BASED MEASUREMENT MATRIX

In this paper, the measurement matrix $\Phi$ is obtained from the four-wing chaotic system and Hadamard matrix, and the specific steps are as follows.

**Step 1** Firstly, the initial values are set and the system is allowed to iterate $m+M$ times and the previous $m$ values are discarded to obtain chaotic pseudo-random sequences $X$, $Y$, $Z$ of length $M$. Where $M = floor(cr * H)$, $floor(x)$ represents the maximum integer smaller than or equal to $x$, $cr$ denotes compression ratio and $H$ stands for the length of the test image.

**Step 2** Then the sequences $s_1, s_2, s_3$ are obtained by arranging the elements of $X, Y, Z$ in the order from highest to lowest.

**Step 3** Finally, Hadamard matrices $ph_i(M \times W), i = 1, 2, 3$ are generated using the seed $\begin{pmatrix} -1 & 1 \\ 1 & -1 \end{pmatrix}$, and the measurement matrix $\Phi_i(M \times W),\ i = 1, 2, 3$ is obtained by

$$\begin{cases} \Phi_1(i, 1:W) = ph_1(s_1(i), 1:W) \\ \Phi_2(i, 1:W) = ph_2(s_2(i), 1:W) \\ \Phi_3(i, 1:W) = ph_3(s_3(i), 1:W), \end{cases} \quad i = 1, 2, \ldots, M \tag{18}$$

where $W$ is the width of the test image.

### 3) DNA ENCODING AND DECODING RULES

The DNA sequence is made of four nucleic acid bases, adenine (A), thymine (T), cytosine (C) and guanine (G). In effect, A and T are complementary, while C and G are complementary. In the theory of computers, information is typically represented in binary, while in the theory of DNA coding it is represented by A, T, C and G. Since 0 and 1 are complementary in binary, it can be assumed that 00 and 11 are complementary, and 01 and 10 are complementary. Thus, when 00, 01, 10 and 11 are used to encode A, T, C and G, there are 24 encoding rules, but only eight of them match the Watson-Crick complementary rule [41], as presented in Table 1. In addition, the DNA decoding rules are opposite to the encoding rules.

**TABLE 1.** DNA encoding rules.

| Rule | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|---|
| 00 | A | A | T | T | G | G | C | C |
| *01* | C | G | C | G | T | A | A | A |
| *10* | G | C | G | A | C | A | T | A |
| *T11* | T | T | C | A | C | C | G | G |

### 4) DNA ADDITION AND SUBTRACTION RULES

The rules of addition and subtraction of DNA sequences can be inferred from that operations of binary numbers 0 and 1. Therefore, according to the above DNA coding rules, eight DNA addition and subtraction rules can be accessed, as shown in Table 2.

**TABLE 2.** DNA addition and subtraction rules.

| + | A | C | G | T | - | A | C | G | T |
|---|---|---|---|---|---|---|---|---|---|
| A | A | C | G | T | A | A | T | G | C |
| C | C | G | T | A | C | C | A | T | G |
| G | G | T | A | C | G | G | C | A | T |
| T | T | A | C | G | T | T | G | C | A |

### 5) DNA COMPLEMENTARY RULE

For every nucleotide $x_i$, the DNA complementary rule [42] is governed by

$$\begin{cases} x_i \neq L(x_i) \neq L(L(x_i)) \neq L(L(L(x_i))) \\ x_i = L(L(L(L(x_i)))) \end{cases} \tag{19}$$

where $x_i$ and $L(x_i)$ are a couple of complementary nucleic acid bases that satisfy single mapping. Six pairs of complementary

bases can be obtained from Eq. (19) as:

(1) $L_1(A) = T, L_1(T) = C, L_1(C) = G, L_1(G) = A$
(2) $L_2(A) = T, L_2(T) = G, L_2(G) = C, L_2(C) = A$
(3) $L_3(A) = C, L_3(C) = T, L_3(T) = G, L_3(G) = A$
(4) $L_4(A) = C, L_4(C) = G, L_4(G) = T, L_4(T) = A$
(5) $L_5(A) = G, L_5(G) = T, L_5(T) = C, L_5(C) = A$
(6) $L_6(A) = G, L_6(G) = C, L_6(C) = T, L_6(T) = A$

where $L_i, i = 1, 2, \ldots, 6$ is the $i$th complement rule. It is worth noting that after the basic DNA encoding operation, this paper will then randomly select a complementary principle for further diffusion of the pixel values.

#### 6) THE 3D PROJECTION CONFUSION

Aiming at the problem of high pixel correlation between color image components, a 3D projection scrambling scheme is designed. The component matrices $R$, $G$ and $B$ of the color image can be regarded as the three mutually vertical planes in a cube, as shown in Fig. 7.

Assume that a point $(X(i), Y(i), Z(i))$ exists in space, then it is projected onto $R$, $G$ and $B$ plane as $R(X(i))$, $G(Y(i))$, $B(Z(i))$. Then the scrambling method can be chosen randomly based on the chaotic sequence, as described in Section IV-B.

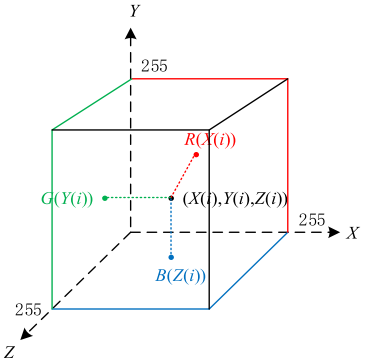


**FIGURE 7.** Schematic diagram of 3D projection.

### B. ENCRYPTION ALGORITHM DESCRIPTION

The dynamic analysis in Section III indicates that the system (1) has complex dynamics performance to be applied in image encryption. In this section, a color image encryption scheme based on CS theory and DNA dynamic encoding is designed. The algorithm consists of sparse, CS calculation, 3D projection confusion, DNA diffusion and plaintext association scrambling. Fig. 8 displays the major process of the designed encryption algorithm, which is detailed as described below.

**Step 1** Input the original color image $I(3 \times H \times W)$ and decompose it into red, green and blue parts to obtain matrices $R, G$ and $B$ with size of $H \times W$. It should be noted that since the three channels $R, G, B$ have the same permutation and diffusion process, the following part is an example of the process of $R$ channel, while that of $G$ and $B$ channels can be obtained in the same way.

**Step 2** DWT is used to obtain the sparse coefficient matrix $R_1(H \times W)$ and the measurement matrix $\Phi_1(M \times W)$ is generated by Section IV-A2.

**Step 3** The sparse image $R_1(H \times W)$ is compressed longitudinally using the measurement matrix $\Phi_1(M \times W)$ to obtain the final compressed image $C_{11}(M \times H)$, where $P_2 = \Phi P_1'$.

**Step 4** In order to keep all pixel values of the compressed image $C_{11}$ in [0, 256], it needs to be quantized by

$$Q_1 = \text{round}(255 \times (C_{11} - \text{Min}_1)/(\text{Max}_1 - \text{Min}_1)) \quad (20)$$

where $\text{Max}_1$=max(max($C_{11}$)),$\text{Min}_1$=min(min($C_{11}$)).

**Step 5** Let model (1) iterate $m + M \times H$ times, and then discard the first $m$ iterations to avoid transient effects, then the chaotic sequences $\{x_i\}_{i=1}^{MH}, \{y_i\}_{i=1}^{MH}, \{z_i\}_{i=1}^{MH}$ and $\{w_i\}_{i=1}^{MH}$ are obtained. And random matrices $q, X_1, X_2, X_3$ with size of $M \times H$ can be obtained by

$$\begin{cases} q = floor((x + 100) \times 10^{14}) \bmod 3 + 1 \\ X_1 = floor((y + 100) \times 10^{14}) \bmod MH + 1 \\ X_2 = floor((z + 100) \times 10^{14}) \bmod MH + 1 \\ X_3 = floor((w + 100) \times 10^{14}) \bmod MH + 1 \end{cases} \quad (21)$$

**Step 6** Keep only one of the recurring random numbers in the pseudo-random sequence $X_1, X_2, X_3$ (i.e. the one that appears for the first time), and then add the values of $\{1, 2, \cdots, MN\}$ that do not appear in the sequence $X_1, X_2, X_3$ to the end in descending order. The non-repeating sequences $Y_1, Y_2, Y_3$ are obtained.

**Step 7** The 3D projection scrambling scheme described in Section IV-A6 is used to reduce the pixel correlation between color image components, which is described in detail as follows.

The quantized compressed matrices $Q_1(M \times H)$, $Q_2(M \times H)$ and $Q_3(M \times H)$ are developed into one-dimensional column vectors $AR(1 \times MH)$, $AG(1 \times MH)$ and $AB(1 \times MH)$. Suppose there exists a point $(Y_1(i), Y_2(i), Y_3(i))$ in space, then project it onto $AR, AG$ and $AB$ plane as $AR(Y_1(i))$, $AG(Y_2(i))$, $AB(Y_3(i))$, as shown in Fig. 5. The scrambling method can be selected based on the values of sequence $q(i)$ received in Step 5.

**Case 1** If $q(i) = 1$, exchange the positions of $AR(Y_1(i))$ and $AG(Y_2(i))$;

**Case 2** If $q(i) = 2$, exchange the positions of $AR(Y_1(i))$ and $AB(Y_3(i))$;

**Case 3** If $q(i) = 3$, exchange the positions of $AG(Y_2(i))$ and $AB(Y_3(i))$.

Restore $AR$, $AG$ and $AB$ to the matrix with size of $M \times H$.

**Step 8** The scrambling matrices $AR$, $AG$ and $AB$ are transformed into binary matrices $bAR$, $bAG$ and $bAB$ with size of $8 \times M \times H$. Then, the binary matrices are transformed into DNA matrices $DAR$, $DAG$ and $DAB$ through DNA coding rule $r_1$ and the size is $4 \times M \times H$.

**Step 9** According to the DNA complementary rule, the sequence $S_1 = \{s_i, i = 1, 2, \ldots, 4MH\}$ can be received by

$$\begin{aligned}
&\text{If } s_{2i-2} = A, \text{ then } s_{2i-1} = L_{l1}(d_{2i-1}).\\
&\text{If } s_{2i-2} = C, \text{ then } s_{2i-1} = L_{l2}(d_{2i-1}).\\
&\text{If } s_{2i-2} = G, \text{ then } s_{2i-1} = L_{l3}(d_{2i-1}).\\
&\text{If } s_{2i-2} = T, \text{ then } s_{2i-1} = L_{l4}(d_{2i-1}).\\
&\text{If } s_{2i-1} = A, \text{ then } s_{2i} = L_{l5}(d_{2i}).\\
&\text{If } s_{2i-1} = C, \text{ then } s_{2i} = L_{l6}(d_{2i}).\\
&\text{If } s_{2i-1} = G, \text{ then } s_{2i} = L_{l7}(d_{2i}).\\
&\text{If } s_{2i-1} = T, \text{ then } s_{2i} = L_{l8}(d_{2i}).
\end{aligned}$$

where $s_i$ is the ith element of the sequence $S_1, i \in \{1, \ldots, 4MH\}$. $d_i$ is the ith element after the DNA matrix $DAR$ is expanded into a one-dimensional row vector and $l_i, i \in \{1, 2, \ldots, 8\}$ is any DNA complementarity principle.

**Step 10** As in step 9, the other two sequences $S_2$ and $S_3$ are obtained.

**Step 11** The parameters and initial values are entered again, and the system is iterated $n + MH$ times. Then the former $n$ values are removed and the chaotic sequences $\{x_i\}_{i=1}^{MH}$, $\{y_i\}_{i=1}^{MH}$, $\{z_i\}_{i=1}^{MH}$ and $\{w_i\}_{i=1}^{MH}$ are received.

**Step 12** Transform all elements of the sequences obtained in step 11 to get the pseudo-random sequences $k1, k2$ and $k3$ by

where $k_1(i)$, $k_2(i)$ and $k_3(i)$, $i \in \{1, 2, \ldots, MH\}$ are the i-th element of chaotic sequences $k_1$, $k_2$ and $k_3$.

**Step 13** Transform the pseudo-random sequences $k_1, k_2$ and $k_3$ into binary sequences $K_1, K_2$ and $K_3$ with size of $8 \times M \times H$ and then transform them into DNA sequences $DK_1$, $DK_2$ and $DK_3$ with size of $4 \times M \times H$ by DNA coding rule $r_2$.

**Step 14** The DNA sequences $DTR, DTG$ and $DTB$ are obtained by

$$DTR(i) = S_1(i) + DK_1(i) + DTR(i-1) \tag{22}$$

$$DTG(i) = S_2(i) + DK_2(i) + DTG(i-1) \tag{23}$$

$$DTB(i) = S(i) + DK_3(i) + DTB(i-1) \tag{24}$$

where $DTR(0) = S_1(4MN)$, $DTG(0) = S_2(4MN)$, $DTB(0) = S_2(4MN)$ and '+' represents DNA addition.

**Step 15** The DNA sequences $DTR, DTG$ and $DTB$ are reverted to matrices, which are transformed into binary matrices by DNA decoding rule $r_3$. And then reverted to decimal matrices $BR$, $BG$ and $BB$ with size of $M \times H$.

**Step 16** According to the chaotic sequence $\{x_i\}_{i=1}^{MH}$, $\{y_i\}_{i=1}^{MH}$, $\{z_i\}_{i=1}^{MH}$ and $\{w_i\}_{i=1}^{MH}$ in step 5, random matrices $Y_5$, $Y_6$, $Y_7$ with size of $M \times H$ can be obtained by

$$\begin{cases}
Y_5 = floor((x+y) \times 10^{16}) \bmod M + 1\\
Y_6 = floor((y+z) \times 10^{16}) \bmod M + 1\\
Y_7 = floor((z+w) \times 10^{16}) \bmod H + 1\\
Y_8 = floor((w+x) \times 10^{16}) \bmod H + 1
\end{cases} \tag{25}$$

**Step 17** Swap the positions of pixel points $BR$(i,j), i $= 1, 2, \ldots$ M; j $= 1, 2, \ldots$ H and $BR(s, t)$. Scramble $BR$ in order from left to right, top to bottom. Furthermore, the scrambled matrix is denoted as $CR$.

**Step 18** The coordinate of $(s, t)$ is calculated by

$$\begin{cases}
s = \bmod(Y_5(i,j) + \text{sum}(BR(Y_6(i,j), 1:H)), M) + 1\\
t = \bmod(Y_7(i,j) + \text{sum}(BR(1:M, Y_8(i,j))), H) + 1
\end{cases} \tag{26}$$

If $s = i$ or $s = Y_6(i, j)$ or $t = j$ or $t = Y_8(i, j)$, the positions of $BR$(i,j) and $BR(s, t)$ remain unchanged. Otherwise $BR$(i,j) and $BR(s, t)$ swap positions.

**Step 19** Similarly, the component encryption matrices $CG$ and $CB$ are obtained. And the final encrypted image $C$ can be obtained by combining $CR$, $CG$ and $CB$.

It is worth to be noted that the designed encryption scheme is symmetric, so the decryption algorithm is the inverse process of that encryption algorithm, which is not described in detail here. In addition, Orthogonal Matching Pursuit (OMP) is selected to restore the ciphertext image in the decryption process.

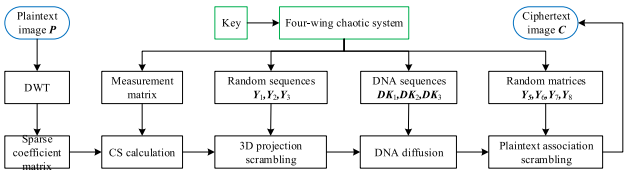


**FIGURE 8.** Encryption algorithm flow chart.

### C. NIST SP800-22 TEST

This section uses the NIST SP800-22 test suite to check the randomness of the chaotic sequence obtained in Section IV-B, and the results are shown in Table 3. It is worth noting that the tests marked with $*$ in the table contain more than one test, and the one with the worst result is given. As can be seen from the table, all P-values are larger than 0.01, which means that the sequence is random, i.e., the constructed four-wing chaotic system can be well applied in the field of image encryption.

**TABLE 3.** NIST SP800-22 test result.

| Order number | Statistical test terms | P-value | Result |
|---|---|---|---|
| 1 | Frequency | 0.3909 | Pass |
| 2 | Block Frequency | 0.3191 | Pass |
| 3 | Runs | 0.7820 | Pass |
| 4 | Longest Run | 0.2673 | Pass |
| 5 | Rank | 0.1143 | Pass |
| 6 | FFT | 0.1550 | Pass |
| 7 | Non-overlapping Template | 0.7194 | Pass |
| 8 | Overlapping Template | 0.2866 | Pass |
| 9 | Universal | 0.9414 | Pass |
| 10 | Linear Complexity | 0.9719 | Pass |
| 11 | Serial (*) | 0.0115 | Pass |
| 12 | Approximate Entropy | 0.5206 | Pass |
| 13 | Cumulative Sums (*) | 1 | Pass |
| 14 | Random Excursions (*) | 0.4143 | Pass |
| 15 | Random Excursions Variant (*) | 0.7461 | Pass |

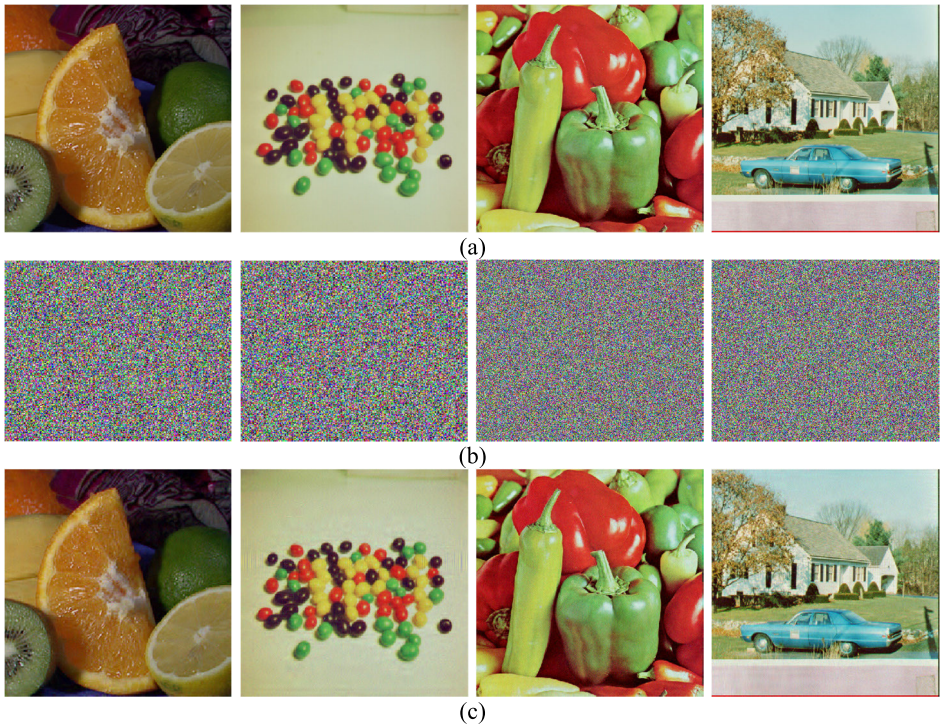


**FIGURE 9.** Experimental results of Fruits256, Beans256, Pappers512 and Car512: (a) Original images, (b) Encrypted images, (c) Decrypted images.

### D. SIMULATION RESULTS

In this section, color Fruits, Beans images of size 256 and Peppers, Car images of size 512 are taken as test images (for the sake of description, they are noted as Fruits256, Beans256 and Pappers512, Car512, respectively). The testing equipment is a personal computer with 8.00GB of memory, AMDA9-9410 processor, 2.90GHz CPU, and Windows 7 system. The testing software is MATLAB R2018b.

Setting the key of the designed algorithm, where the parameters are $a = 9, b = 38, c = 50, d = 5, e = 5, f = 2$, the initial values are $(0.1, 0.2, 0.3, 0.4)$, the random numbers are $m = 500, n = 800$ and the compression rate $cr = 0.8$. Fig. 9(a) presents the original images of Fruits256, Beans256, Peppers512 and Car512. The respective encrypted and decrypted images gained by numerical simulation are displayed in Fig. 9(b) and (c), respectively. It is obvious that the encrypted images are always noise-like, and no any useful information about the plaintext image can be observed, which proves that the designed encryption scheme can compress and encrypt the test image effectively. Additionally, there is little difference between the decrypted image and the plaintext image, which demonstrates the effectiveness and feasibility of the decryption algorithm. Moreover, the designed algorithm has no limitation on the size of test images.

## V. PERFORMANCE ANALYSIS

### A. THE EFFECT OF THE COMPRESSION RATIO ON SIMULATION

In this section, the effect of different $cr$ values on the encryption algorithm performance is investigated by mean structural similarity (MSSIM) and peak signal-to-noise ratio (PSNR). And $cr$ can be calculated by

$$cr = \frac{H_C W_C}{H_I W_I} \tag{27}$$

where $H_I$ and $W_I$ are the height and width of plaintext image, while $H_C$ and $W_C$ are that of cipher image.

The PSNR and MSSIM are defined by

$$\mathrm{MSE} = \frac{1}{\mathrm{HW}} \sum_{i=1}^{H} \sum_{j=1}^{W} (I_1(i,j) - I(i,j))^2 \tag{28}$$

$$\mathrm{PSNR} = 10 \log_{10}(\frac{\mathrm{L}^2}{\mathrm{MSE}}) \tag{29}$$

$$\mathrm{SSIM}(X,Y) = \frac{2\mu_X\mu_Y + C_1}{\mu_X^2\mu_Y^2 + C_1} \times \frac{2\sigma_X\sigma_Y + C_2}{\sigma_X^2\sigma_Y^2 + C_2} \times \frac{\sigma_{XY} + C_3}{\sigma_X\sigma_Y + C_3} \tag{30}$$

$$\mathrm{MSSIM}(X,Y) = \sum_{k=1}^{64} \mathrm{SSIM}(x_k, y_k)/64 \tag{31}$$

where H, W are the length and width of the original image. $I_1$ and $I$ represent the decrypted image and the plaintext image, respectively. $\mu_X$ and $\mu_Y$ denote the average values of image $X$ and $Y$, $\sigma_X$ and $\sigma_Y$ are the variance, $\sigma_{XY}$ indicates the covariance, $C_1 = (k_1 \times L)^2, C_2 = (k_2 \times L)^2, C_3 = \frac{C_2}{2}, k_1 = 0.01, k_2 = 0.03$. And L is the maximum pixel value of the image and $L = 255$ when the test image is represented by 8 bits of pixels. In image compression, the typical PSNR value is between 30dB and 40dB, and the larger the PSNR value is, the more similar the original image and the processed

image are to each other. In addition, the value of MSSIM always lies in the interval [−1,1], and the closer the value is to 1, the higher similarity between the two test images.

In this section, color Lena256, Fruits256 and Beans256 images are selected as test images, and the PSNR and MSSIM values at different $cr$ are presented in Table 4. As can be seen from the table, the values of PSNR and MSSIM are all proportional to the $cr$ values. In other words, the larger the $cr$ value is, the more similar the reconstructed image and the original image is, and the better the reconstruction effect is. Therefore, to make sure the quality of the reconstructed images, $cr$ =0.8 is taken in this paper.

**TABLE 4. PSNR and MSSIM values under different cr values.**

| Images | Channels | PSNR | | | MSSIM | | |
|---|---|---|---|---|---|---|---|
| | | $cr$=0.8 | $cr$ =0.6 | $cr$ =0.4 | $cr$ =0.8 | $cr$ =0.6 | $cr$ =0.4 |
| Lena256 | R | 32.8632 | 29.5276 | 28.2935 | 0.8599 | 0.7727 | 0.7588 |
| | G | 33.1646 | 28.8648 | 27.2741 | 0.8933 | 0.7926 | 0.7696 |
| | B | 34.7376 | 31.2804 | 29.9131 | 0.8994 | 0.8244 | 0.8085 |
| Fruits256 | R | 33.5594 | 30.1448 | 29.3422 | 0.8616 | 0.7601 | 0.7357 |
| | G | 32.4612 | 29.0432 | 27.7812 | 0.8636 | 0.7519 | 0.7113 |
| | B | 28.8226 | 25.3519 | 24.2804 | 0.8342 | 0.6861 | 0.6309 |
| Beans256 | R | 34.3406 | 31.2247 | 30.2996 | 0.8715 | 0.8018 | 0.8476 |
| | G | 33.6631 | 29.9557 | 28.6238 | 0.8694 | 0.7699 | 0.8306 |
| | B | 34.8727 | 30.9557 | 29.4155 | 0.8778 | 0.8050 | 0.7712 |

### B. KEY SPACE AND KEY SENSTIVITY ANALYSIS

A good encryption algorithm should not only have a large enough key space, but also should be highly sensitive to the key. The keys of the proposed algorithm mainly consist of system parameters $a, b, c, d, e, f$ and initial values $(x_0, y_0, z_0, w_0)$. The maximum error of each key in the decryption process is obtained by numerical simulation, where $w_0$ is $10^{-16}$, $x_0, z_0, a, d, e, f$ are $10^{-15}$, $b, c$ are $10^{-14}$ and $y_0$ are $10^{-13}$. Therefore, the key space is $10^{16+15\times6+14\times2+13} > 2^{488}$,which can be completely resistant to violent attacks. In addition, the key space comparison results with other literatures [18], [22], [30] are presented in Table 5. Clearly, the designed scheme has a much larger key space and can effectively withstand exhaustive attacks.

**TABLE 5. Key space comparison results.**

| Algorithms | Ours | Ref [18] | Ref [22] | Ref [30] |
|---|---|---|---|---|
| Key space | $>2^{488}$ | $2^{448}$ | $>2^{212}$ | $>2^{398}$ |

To test key sensitivity, the Fruits256 image is chosen as the test image and a small perturbation is applied to the key. For convenience, the correct key is noted as $K_0$ and the slightly modified keys are $K_i(i = 1, 2, \ldots, 4)$. The resulting decrypted images are provided in Fig. 10, where Fig. 10(a) presents that obtained using the correct key. It can be noticed from the figure that when the key is slightly varied, the decrypted image will be completely unlike the one obtained using the correct key. Without loss of completeness, Table 6 gives the PSNR and MISSIM values among

**TABLE 6. PSNR and MSSIM values between different decrypted images.**

| Images | PSNR | MSSIM |
|---|---|---|
| (a) – (b1) | 5.3039 | 0.00009 |
| (a) – (b2) | 5.2109 | -0.00005 |
| (a) – (b3) | 5.2659 | -0.00003 |
| (a) – (b4) | 5.3031 | 0.00002 |

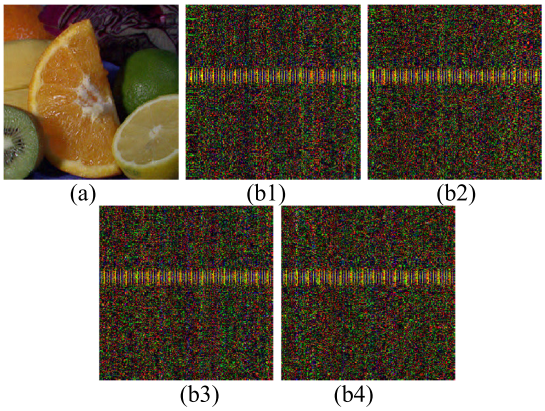


**FIGURE 10. Decrypted image of Cameraman256 with: (a) $K_0$, (b1). $K_1 = x_0 + 10^{-15}$, (b2) $K_2 = y_0 + 10^{-13}$, (b3) $K_3 = a + 10^{-15}$, (b4) $K_4 = b + 10^{-14}$.**

Fig. 10(a), (b1) and (b2). It can be noticed that the PSNR values are all approaching 5 and the MISSIM values are all nearly 0, which indicates that there is little similarity between the decrypted images obtained by slightly changing the key and those obtained by the correct key. In other terms, the designed algorithm is highly sensitive to the key and can successfully defend against brute force attacks.

### C. HISTOGRAM ANALYSIS

Histograms can clearly reveal the distribution of image pixel and are mainly employed to estimate the ability of algorithms to defend against statistical attacks. In this section, color Fruits256, Beans256, Peppers512 and Car512 are chosen as testing images. Figure 11 displays the histograms of the original images and the corresponding histograms of encrypted and decrypted images. Obviously, the histograms of the original images are undulating, while that of the encrypted images are flat. Consequently, it is hardly for an attacker to get any valuable information from the histogram of encrypted images. It can also be found that the pixel value distribution of the decrypted image is almost the same as the original image, which indicates the feasibility of the decryption algorithm.

Additionally, the chi-square statistic is commonly used to numerically measure the homogeneity of image histograms. For an image with gray level of 256 and size of $M \times N$, the chi-square statistic can be calculated by

$$\chi^2 = \sum_{i=0}^{255} \frac{(f_i - g)^2}{g} \tag{32}$$

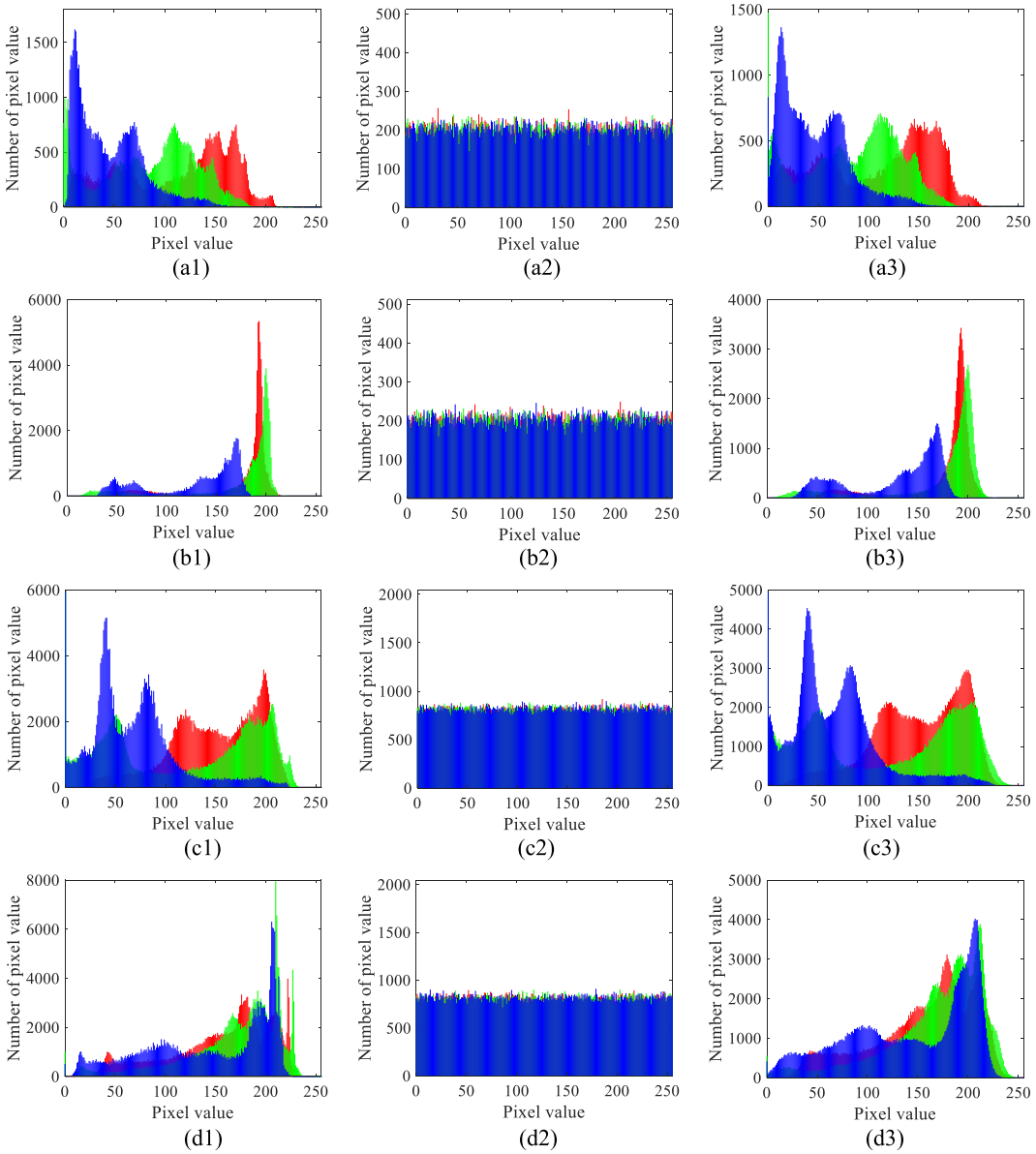


**FIGURE 11.** Histogram analysis results for plaintext images, ciphertext images and decrypted images: (a1) Original Fruits256, (a2) Encrypted Fruits256, (a3) Decrypted Fruits256, (b1) Original Beans256, (b2) Encrypted Beans256, (b3) Decrypted Beans256, (c1) Original Pappers512, (c2) Encrypted Pappers512, (c3) Decrypted Pappers512, (d1) Original Car512, (d2) Encrypted Car512, (d3) Decrypted Car512.

where $f_i$ denotes the frequency of each grayscale value and $g = MN/256$ are the corresponding theoretical frequency distributions. When the significance level is taken as 0.05, the chi-square statistic is $\chi^2_{0.05}(255) = 293.24783$. Table 7 lists the chi-square statistics of color Fruits256, Beans256, Peppers512 and Car512 plaintext images and the corresponding ciphertext images. It can be seen that the values of the chi-square statistics of plaintext images are substantially larger than $\chi^2_{0.05}(255)$, and that of the corresponding ciphertext images are all smaller than $\chi^2_{0.05}(255)$. The above analysis shows that ciphertext image histograms are almost uniformly distributed, which suggests that the proposed algorithm can successfully resist statistical attacks.

**TABLE 7.** The analysis results of chi-square statistics.

| Image | | Fruits256 | Beans256 | Papper512 | Car512 |
|---|---|---|---|---|---|
| R | plaintext | $3.7694\times10^4$ | $5.3750\times10^5$ | $2.1319\times10^5$ | $1.9203\times10^5$ |
| | ciphertext | 291.8725 | 243.8333 | 212.2103 | 250.8020 |
| G | plaintext | $5.1614\times10^4$ | $3.4925\times10^5$ | $3.1838\times10^5$ | $3.3254\times10^5$ |
| | ciphertext | 252.1765 | 223.1863 | 246.0709 | 254.7213 |
| B | plaintext | $1.2947\times10^5$ | $1.2976\times10^5$ | $4.9143\times10^5$ | $2.4801\times10^5$ |
| | ciphertex | 254.7745 | 264.1765 | 251.7873 | 292.7702 |

### D. CORRELATION ANALYSIS

In general, the closer the correlation coefficient is to 0, the stronger the algorithm is against statistical attacks. However,

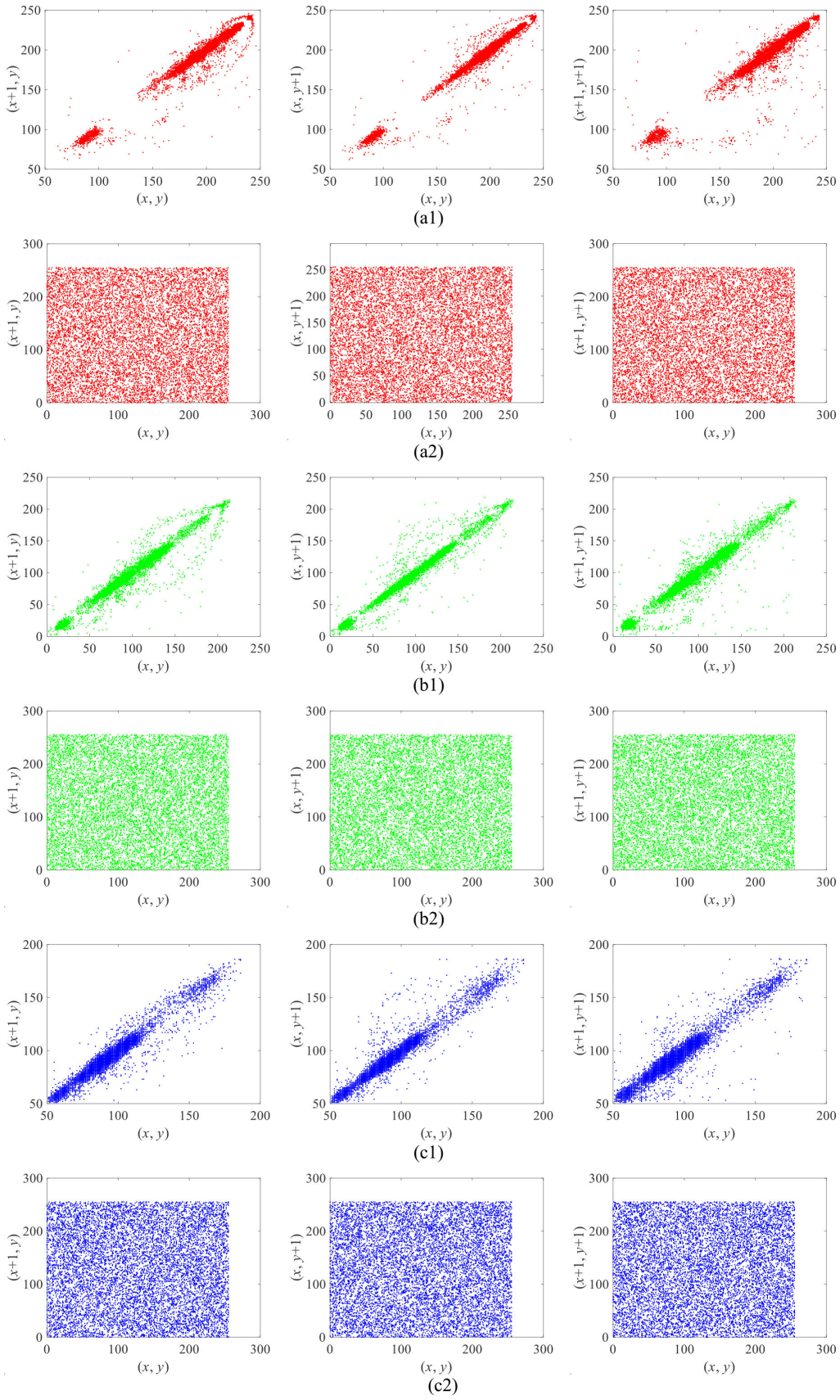


**FIGURE 12.** Correlation distribution of adjacent pixels in horizontal, vertical and diagonal directions of Lena256, (a1) R channel of plaintext, (a2) R channel of ciphertext, (b1) G channel of plaintext, (b2) G channel of ciphertext, (c1) B channel of plaintext, (c2) B channel of ciphertext.

**TABLE 8.** Correlation coefficients in different channel.

| Channel | Direction | plaintext | | | ciphertext | | |
|---|---|---|---|---|---|---|---|
| | | R | G | B | R | G | B |
| Lena256 | H | 0.9556 | 0.9443 | 0.9280 | -0.0029 | -0.0038 | -0.0036 |
| | V | 0.9780 | 0.9711 | 0.9575 | 0.0021 | -0.0042 | 0.0005 |
| | D | 0.9435 | 0.9301 | 0.9093 | 0.0028 | -0.0003 | -0.0035 |
| Fruits256 | H | 0.9879 | 0.9732 | 0.8682 | 0.0010 | 0.0008 | 0.0014 |
| | V | 0.9866 | 0.9714 | 0.8619 | 0.0006 | -0.0057 | 0.0005 |
| | D | 0.9791 | 0.9558 | 0.7889 | 0.0058 | -0.0047 | 0.0000 |
| Beans256 | H | 0.9734 | 0.9707 | 0.9778 | 0.0002 | 0.0027 | -0.0024 |
| | V | 0.9740 | 0.9740 | 0.9793 | 0.0045 | 0.0021 | -0.0029 |
| | D | 0.9509 | 0.9496 | 0.9628 | 0.0005 | -0.0001 | -0.0023 |
| Lena512 | H | 0.9752 | 0.9666 | 0.9333 | -0.0032 | 0.0003 | -0.0011 |
| | V | 0.9853 | 0.9801 | 0.9557 | -0.0011 | -0.0022 | -0.0010 |
| | D | 0.9691 | 0.9582 | 0.9225 | 0.0001 | 0.0005 | -0.0005 |
| Pappers512 | H | 0.9635 | 0.9811 | 0.9665 | 0.0006 | 0.0005 | 0.0006 |
| | V | 0.9663 | 0.9817 | 0.9664 | 0.0019 | -0.0019 | -0.0009 |
| | D | 0.9574 | 0.9697 | 0.9477 | -0.0012 | -0.0036 | 0.0003 |
| Car512 | H | 0.9535 | 0.9390 | 0.9724 | -0.0013 | 0.0044 | 0.0012 |
| | V | 0.9578 | 0.9423 | 0.9686 | 0.0005 | 0.0022 | 0.0016 |
| | D | 0.9231 | 0.8919 | 0.9451 | 0.0001 | 0.0003 | -0.0017 |

**TABLE 9.** The correlation comparison results of Lena256 and Lena512 images in different algorithms.

| Algorithm | Direction | Lena256 | | | Algorithm | Direction | Lena512 | | |
|---|---|---|---|---|---|---|---|---|---|
| | | R | G | B | | | R | G | B |
| Ours | H | -0.0029 | -0.0038 | -0.0036 | Ours | H | -0.0032 | 0.0003 | -0.0011 |
| | V | 0.0021 | -0.0042 | 0.0005 | | V | -0.0011 | -0.0022 | -0.0010 |
| | D | 0.0028 | -0.0003 | -0.0035 | | D | 0.0001 | 0.0005 | -0.0005 |
| Ref. [10] | H | 0.0083 | -0.0054 | -0.0010 | Ref. [4] | H | 0.0007 | 0.0086 | 0.0012 |
| | V | -0.0049 | 0.0100 | 0.0124 | | V | 0.0118 | -0.0154 | 0.0014 |
| | D | -0.0095 | -0.0017 | -0.0042 | | D | 0.0154 | -0.0166 | 0.0124 |
| Ref. [11] | H | -0.0053 | 0.0030 | 0.0062 | Ref. [9] | H | 0.0066 | 0.0291 | -0.0052 |
| | V | -0.0069 | 0.0047 | 0.0031 | | V | 0.0065 | 0.0191 | -0.0003 |
| | D | -0.0087 | 0.0024 | 0.0022 | | D | -0.0308 | -0.0140 | 0.0056 |
| Ref. [31] | H | -0.0020 | -0.0022 | 0.0069 | Ref. [22] | H | 0.0092 | 0.0002 | 0.0076 |
| | V | -0.0013 | -0.0041 | 0.0059 | | V | 0.0203 | -0.0025 | 0.0006 |
| | D | -0.0059 | 0.0014 | 0.0035 | | D | -0.0073 | -0.0131 | 0.0111 |

the correlation of the original image is always quite high, and thus a good encryption scheme should minimize it.

In order to measure the resistance of the proposed algorithm to statistical attacks, n pairs of adjacent pixels are randomly chosen from the experimental images, which grayscale values are remembered as $u_i$ and $v_i, i = 1, 2, \cdots, MN$. The correlation coefficient between $u = \{u_i\}$ and $v = \{v_i\}$ is calculated as

$$r_{uv} = \frac{E((u - E(u))(v - E(v)))}{\sqrt{D(u)}\sqrt{D(v)}} \tag{33}$$

$$D(u) = \frac{1}{N}\sum_{i=1}^{N}(u_i - E(u))^2 \tag{34}$$

$$E(u) = \frac{1}{N}\sum_{i=1}^{N}u_i \tag{35}$$

where $u_i = (x_i, y_i)$. If $v_i = (x_i + 1, y_i)$, then the correlation coefficient in the horizontal direction is calculated. Similarly, if $v_i = (x_i, y_i + 1)$ or $v_i = (x_i + 1, y_i + 1)$, the correlation coefficient in the vertical or diagonal direction is calculated.

In this section, color Lena256, Fruits256, Beans256, Lena512, Pappers512 and Car512 are chosen as the experimental images. And 10,000 pairs of pixels are randomly picked from these experimental images to calculate the correlation coefficients. The pixel distribution of the R, G, B channels of color Lena256 are presented in Fig. 12. It is observed that the pixels of the original image are concentrated around y=x in each channel, while that of the encrypted image are uniformly distributed over the whole range of pixel values, which indicates that the proposed algorithm can completely reduce the correlation of the original image. Additionally, Table 8 presents the correlation coefficients of the original and corresponding encrypted experimental images in different orientations. Table 9 shows the correlation coefficient results for the color Lena256 and Lena512 encrypted images in this paper with the existing literature [4], [9], [10], [11], [22], [31]. It is clear that the correlation coefficients of the encrypted images obtained in this paper are closer to 0 and can efficiently withstand statistical attacks.

It is important to note that the correlation between the color image components is commonly high. In this paper, 3D projection scheme is introduced to vary the pixel positions

**TABLE 10.** Adjacent-position correlation coefficients.

| Image | Plaintext | | | Ciphertext | | |
|---|---|---|---|---|---|---|
| | R-G | R-B | G-B | R-G | R-B | G-B |
| Lena256 | 0.8570 | 0.6700 | 0.8934 | 0.0018 | 0.0038 | -0.0018 |
| Fruits256 | 0.8617 | 0.4586 | 0.6282 | -0.0038 | -0.0019 | 0.0022 |
| Beans256 | 0.6470 | 0.6111 | 0.8352 | -0.0048 | 0.0040 | -0.0008 |
| Lena512 | 0.8652 | 0.6735 | 0.8967 | 0.0013 | 0.0016 | 0.0012 |
| Pappers512 | 0.2617 | 0.3847 | 0.8308 | -0.0002 | 0.0006 | 0.0012 |
| Car512 | 0.7643 | 0.6652 | 0.8581 | 0.0013 | 0.0000 | 0.0001 |

**TABLE 11.** The correlation comparison results of Lena256 and Lena512 at adjacent position in different algorithms.

| Algorithm | Lena256 | | | Algorithm | Lena512 | | |
|---|---|---|---|---|---|---|---|
| | R-G | R-B | G-B | | R-G | R-B | G-B |
| Ours | 0.0018 | 0.0038 | -0.0018 | Ours | 0.0013 | 0.0016 | 0.0012 |
| Ref. [12] | -0.0003 | -0.0045 | -0.0085 | Ref. [9] | -0.0111 | -0.0003 | 0.0082 |
| Ref. [18] | -0.0015 | 0.0088 | -0.0072 | Ref. [19] | -0.0009 | 0.0042 | 0.0031 |

between the components specially to decrease the correlation. The correlation coefficients between the components of the test images at adjacent locations are presented in Table 10. It can be found that the correlation coefficients between the components of the encrypted images at adjacent positions are very near to zero, which indicates that the proposed scheme can efficiently destroy the correlation between the components. Additionally, Table 11 presents the results of the Lena256 and Lena512 encrypted images correlation coefficients in this paper at adjacent locations compared to the existing literature [9], [12], [18], [19]. It is clear that the correlation coefficients in this paper are closer to zero, which proves the effectiveness of the proposed encryption scheme.

### E. INFORMATION ENTROPY ANALYSIS

Information entropy is an essential metric to estimate the security of an encryption scheme, which can reveal the uncertainty of image information. The larger the entropy value is, the fewer visual information is obtained, and the better the encryption effect is. And the information entropy value can be calculated by

$$H = -\sum_{i=0}^{L} p(i)\log_2 p(i) \tag{36}$$

where L denotes the number of gray levels, and $p(i)$ shows the probability of occurrence of $i$. For an image with the gray level of 256, the theoretical information entropy value H is 8.

The information entropy of the original and corresponding encrypted Lena256, Fruits256, Beans256, Lena512, Pappers512 and Car512 images is presented in Table 12. It can be seen that the encrypted images information entropy is very near to 8, while that of each original image is quite different from the theoretical value. The above findings show that the proposed encryption scheme greatly changes the pixel values of the original image and significantly increases the randomness of the encrypted image. Additionally, the information entropy comparison results of Lena256 and Lena512 in this paper and literature [13], [14], [15], [22], [26], [37], are

**TABLE 12.** Information entropy of test images in different channel.

| Image | Plaintext | | | Ciphertext | | |
|---|---|---|---|---|---|---|
| | R | G | B | R | G | B |
| Lena256 | 7.1655 | 7.5578 | 6.8571 | 7.9972 | 7.9967 | 7.9967 |
| Fruits256 | 7.5071 | 7.3231 | 6.7437 | 7.9959 | 7.9965 | 7.9964 |
| Beans256 | 5.7920 | 6.2195 | 6.7986 | 7.9966 | 7.9969 | 7.9963 |
| Lena512 | 5.0465 | 5.4576 | 4.8001 | 7.9991 | 7.9991 | 7.9992 |
| Pappers512 | 7.3388 | 7.4963 | 7.0583 | 7.9993 | 7.9992 | 7.9991 |
| Car512 | 7.4156 | 7.2295 | 7.4354 | 7.9991 | 7.9991 | 7.9990 |

**TABLE 13.** Information entropy comparison results of Lena256 and Lena512 in different algorithms.

| Algorithm | Lena256 | | | Algorithm | Lena512 | | |
|---|---|---|---|---|---|---|---|
| | R | G | B | | R | G | B |
| Ours | 7.9972 | 7.9967 | 7.9967 | Ours | 7.9991 | 7.9991 | 7.9992 |
| Ref. [14] | 7.9958 | 7.9950 | 7.9949 | Ref. [13] | 7.9917 | 7.9912 | 7.9917 |
| Ref. [15] | 7.7771 | 7.7190 | 7.7150 | Ref. [22] | 7.9980 | 7.9979 | 7.9978 |
| Ref. [25] | 7.9892 | 7.9902 | 7.9896 | Ref. [37] | 7.9988 | 7.9985 | 7.9988 |

presented in Table 13. It can be observed from the table that the information entropy of the encrypted image in this paper is much closer to 8, which indicates that the proposed algorithm has a more prominent encryption effect and can successfully withstand information entropy attacks.

## VI. CONCLUSION

Firstly, a four-wing chaotic system is constructed and its dynamic characteristics are analyzed in detail. Simulation results show that the system exhibits rich dynamics with chaotic states distributed over a large interval and is well suited for applications in the field of secure communication. Then, the circuit design and Multisim simulation results are in good agreement with the theoretical analysis results. Finally, a color image compression encryption scheme is designed based on the constructed system. The security performance of the proposed algorithm is evaluated detailly in terms of key space, key sensitivity, histogram, correlation and information entropy. The experimental results indicate that the proposed encryption scheme not only has a considerable key space, but also has better key sensitivity. Additionally, the scheme can also be effective against common attacks, such as exhaustive attacks, statistical attacks, and information entropy attacks. It should be noted that the designed 3D projection scrambling scheme can significantly minimize the correlation between the components of color images. In the future research work, we will continue to explore chaotic systems with special attractors and their practical engineering applications.

## REFERENCES

[1] F. H. Min, Z. L. Wang, E. R. Wang, and Y. Cao, "New memristor chaotic circuit and its application to image encryption," *J. Electron. Inf. Technol.*, vol. 38, no. 10, pp. 2681–2688, Oct. 2016.

[2] H. Liu, F. Wen, and A. Kadir, "Construction of a new 2D Chebyshev-sine map and its application to color image encryption," *Multimedia Tools Appl.*, vol. 78, no. 12, pp. 15997–16010, Jun. 2019.

[3] C. Chen, K. Sun, and Q. Xu, "A color image encryption algorithm based on 2D-CIMM chaotic map," *China Commun.*, vol. 17, no. 5, pp. 12–20, May 2020.

[4] J. Y. Sun, C. B. Li, T. N. Lu, A. Akgul, and F. H. Min, "A memristive chaotic system with hypermultistability and its application in image encryption," *IEEE Access*, vol. 8, no. 5, pp. 139289–139298, Jul. 2020.

[5] X. L. An, L. Xiong, and S. Qiao, "Dynamic response of a class of hybrid neuron model by electromagnetic induction and application of image encryption," *J. Electron. Inf. Technol.*, vol. 45, no. 3, pp. 929–940, Mar. 2023.
[6] Q. Lai, Z. Wan, H. Zhang, and G. Chen, "Design and analysis of multiscroll memristive Hopfield neural network with adjustable memductance and application to image encryption," *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 34, pp. 7824–7837, Oct. 2023.
[7] Q. Lai, C. Lai, H. Zhang, and C. Li, "Hidden coexisting hyperchaos of new memristive neuron model and its application in image encryption," *Chaos, Solitons Fractals*, vol. 158, May 2022, Art. no. 112017.
[8] C. Chen, K. Sun, and S. He, "An improved image encryption algorithm with finite computing precision," *Signal Process.*, vol. 168, Mar. 2020, Art. no. 107340.
[9] Z.-H. Gan, X.-L. Chai, D.-J. Han, and Y.-R. Chen, "A chaotic image encryption algorithm based on 3-D bit-plane permutation," *Neural Comput. Appl.*, vol. 31, no. 11, pp. 7111–7130, May 2018.
[10] J. Zhou, N.-R. Zhou, and L.-H. Gong, "Fast color image encryption scheme based on 3D orthogonal Latin squares and matching matrix," *Opt. Laser Technol.*, vol. 131, Nov. 2020, Art. no. 106437.
[11] D. Q. Ouyang, J. Shao, H. J. Jiang, S. K. Nguang, and H. T. Shen, "Impulsive synchronization of coupled delayed neural networks with actuator saturation and its application to image encryption," *Neural Netw.*, vol. 128, pp. 158–171, Aug. 2020.
[12] M. Yildirim, "A color image encryption scheme reducing the correlations between R, G, B components," *Optik*, vol. 237, Jul. 2021, Art. no. 166728.
[13] Y.-Q. Zhang, Y. He, P. Li, and X.-Y. Wang, "A new color image encryption scheme based on 2DNLCML system and genetic operations," *Opt. Lasers Eng.*, vol. 128, May 2020, Art. no. 106040.
[14] H. Lin, C. Wang, F. Yu, C. Xu, Q. Hong, W. Yao, and Y. Sun, "An extremely simple multiwing chaotic system: Dynamics analysis, encryption application, and hardware implementation," *IEEE Trans. Ind. Electron.*, vol. 68, no. 12, pp. 12708–12719, Dec. 2021.
[15] O. S. Faragallah, M. A. Alzain, H. S. El-Sayed, J. F. Al-Amri, W. El-Shafai, A. Afifi, E. A. Naeem, and B. Soh, "Block-based optical color image encryption based on double random phase encoding," *IEEE Access*, vol. 7, pp. 4184–4194, 2019.
[16] L. Xiong, F. Yang, J. Mou, X. An, and X. Zhang, "A memristive system and its applications in red–blue 3D glasses and image encryption algorithm with DNA variation," *Nonlinear Dyn.*, vol. 107, no. 3, pp. 2911–2933, Jan. 2022.
[17] Q. Shi, X. An, L. Xiong, F. Yang, and L. Zhang, "Dynamic analysis of a fractional-order hyperchaotic system and its application in image encryption," *Phys. Scripta*, vol. 97, no. 4, Feb. 2022, Art. no. 045201.
[18] F. Yang, J. Mou, C. Luo, and Y. Cao, "An improved color image encryption scheme and cryptanalysis based on a hyperchaotic sequence," *Phys. Scripta*, vol. 94, no. 8, Apr. 2019, Art. no. 085206.
[19] X. Chai, X. Fu, Z. Gan, Y. Lu, and Y. Chen, "A color image cryptosystem based on dynamic DNA encryption and chaos," *Signal Process.*, vol. 155, pp. 44–62, Feb. 2019.
[20] J. Chen, L. Chen, and Y. Zhou, "Cryptanalysis of a DNA-based image encryption scheme," *Inf. Sci.*, vol. 520, pp. 130–141, May 2020.
[21] A. Belazi, M. Talha, S. Kharbech, and W. Xiang, "Novel medical image encryption scheme based on chaos and DNA encoding," *IEEE Access*, vol. 7, pp. 36667–36681, 2019.
[22] 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.
[23] T. Li, J. Shi, X. Li, J. Wu, and F. Pan, "Image encryption based on pixel-level diffusion with dynamic filtering and DNA-level permutation with 3D Latin cubes," *Entropy*, vol. 21, no. 3, p. 319, Mar. 2019.
[24] H. Dong, E. Bai, X.-Q. Jiang, and Y. Wu, "Color image compression-encryption using fractional-order hyperchaotic system and DNA coding," *IEEE Access*, vol. 8, pp. 163524–163540, 2020.
[25] X. Ouyang, Y. Luo, J. Liu, L. Cao, and Y. Liu, "A color image encryption method based on memristive hyperchaotic system and DNA encryption," *Int. J. Modern Phys. B*, vol. 34, no. 4, Feb. 2020, Art. no. 2050014.
[26] Q. Liu and L. Liu, "Color image encryption algorithm based on DNA coding and double chaos system," *IEEE Access*, vol. 8, pp. 83596–83610, 2020.
[27] C. Zhu, Z. Gan, Y. Lu, and X. Chai, "An image encryption algorithm based on 3-D DNA level permutation and substitution scheme," *Multimedia Tools Appl.*, vol. 79, nos. 11–12, pp. 7227–7258, Mar. 2020.
[28] L.-P. Chen, H. Yin, L.-G. Yuan, A. M. Lopes, J. A. T. Machado, and R.-C. Wu, "A novel color image encryption algorithm based on a fractional-order discrete chaotic neural network and DNA sequence operations," *Frontiers Inf. Technol. Electron. Eng.*, vol. 21, no. 6, pp. 866–879, Jul. 2020.
[29] D. L. Donoho, "Compressed sensing," *IEEE Trans. Inf. Theory*, vol. 52, no. 4, pp. 1289–1306, Apr. 2006.
[30] Q. Xu, K. Sun, S. He, and C. Zhu, "An effective image encryption algorithm based on compressive sensing and 2D-SLIM," *Opt. Lasers Eng.*, vol. 134, Nov. 2020, Art. no. 106178.
[31] F. Yang, J. Mou, K. Sun, Y. Cao, and J. Jin, "Color image compression-encryption algorithm based on fractional-order memristor chaotic circuit," *IEEE Access*, vol. 7, pp. 58751–58763, 2019.
[32] X. Wang and Y. Su, "Image encryption based on compressed sensing and DNA encoding," *Signal Process., Image Commun.*, vol. 95, Jul. 2021, Art. no. 116246.
[33] W. Wen, Y. Hong, Y. Fang, M. Li, and M. Li, "A visually secure image encryption scheme based on semi-tensor product compressed sensing," *Signal Process.*, vol. 173, Aug. 2020, Art. no. 107580.
[34] L. Gong, K. Qiu, C. Deng, and N. Zhou, "An image compression and encryption algorithm based on chaotic system and compressive sensing," *Opt. Laser Technol.*, vol. 115, pp. 257–267, Jul. 2019.
[35] L. Gong, K. Qiu, C. Deng, and N. Zhou, "An optical image compression and encryption scheme based on compressive sensing and RSA algorithm," *Opt. Lasers Eng.*, vol. 121, pp. 169–180, Oct. 2019.
[36] N. Zhou, S. Pan, S. Cheng, and Z. Zhou, "Image compression-encryption scheme based on hyper-chaotic system and 2D compressive sensing," *Opt. Laser Technol.*, vol. 82, pp. 121–133, Aug. 2016.
[37] X. Chai, J. Bi, Z. Gan, X. Liu, Y. Zhang, and Y. Chen, "Color image compression and encryption scheme based on compressive sensing and double random encryption strategy," *Signal Process.*, vol. 176, Nov. 2020, Art. no. 107684.
[38] X. Chai, H. Wu, Z. Gan, D. Han, Y. Zhang, and Y. Chen, "An efficient approach for encrypting double color images into a visually meaningful cipher image using 2D compressive sensing," *Inf. Sci.*, vol. 556, pp. 305–340, May 2021.
[39] J. Mou, F. Yang, R. Chu, and Y. Cao, "Image compression and encryption algorithm based on hyper-chaotic map," *Mobile Netw. Appl.*, vol. 26, no. 5, pp. 1849–1861, Jun. 2019.
[40] E. J. Candes and T. Tao, "Decoding by linear programming," *IEEE Trans. Inf. Theory*, vol. 51, no. 12, pp. 4203–4215, Nov. 2005.
[41] A. N. DeMaria, "A structure for deoxyribose nucleic acid," *J. Amer. College Cardiol.*, vol. 42, no. 2, pp. 373–374, Jul. 2003.
[42] 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, May 2012.
[43] W. Fa-Qiang and L. Chong-Xin, "Synchronization of liu chaotic system based on linear feedback control and its experimental verification," *Acta Phys. Sinica*, vol. 55, no. 10, pp. 5055–5060, 2006.

**LI ZHANG** was born in Lanzhou, Gansu, China, in 1982. She received the master's degree from the School of Mathematics and Physics, Lanzhou Jiaotong University. She is currently an Associate Professor with the Basic Courses Department, Lanzhou Institute of Technology. Her current research interests include nonlinear circuits and image encryption.

**XIN-LEI AN** was born in Kaifeng, Henan, China, in 1983. He received the Ph.D. degree from Lanzhou Jiaotong University. He is currently a Professor with the School of Mathematics and Physics, Lanzhou Jiaotong University. His current research interests include nonlinear dynamics, neuronal networks, and image encryption.