An image encryption algorithm based on a new memristor chaotic system and DNA variation

Li Xiong², Peng Li¹*, Yingqian Zhang³, Feifei Yang¹,², Chenguang Ma¹

1 School of Information Science and Engineering, Dalian polytechnic University, Dalian, 116034, China
2 School of Physics and Electromechanical Engineering, Hexi University, Zhangye, 734000, China
3 School of Information Science and Technology, Xiamen University Tan Kah Kee College, Zhangzhou 363105, China

Abstract In this paper, a new memristor chaotic system is designed based on Chua’s memristor chaotic system. To get the complete picture of the brain of a three-dimensional chaotic attractor, red and blue 3D glasses is used to observe the chaotic attractor, and using Lyapunov exponent spectrum, SE complexity and C0 complexity to analyze dynamical characteristics of new memristor chaotic system. The results illustrate that the chaotic state of the new memristor chaotic system is distributed over a large parameter range, which shows that the new memristor chaotic system is more suitable for image encryption applications. To verify the image encryption application of the new memristor chaotic system, a novel image encryption algorithm is designed based on the new memristor chaotic system and DNA variation. The security performances of the designed algorithm indicate that the proposed algorithm can effectively encrypt image and has better security performance.

Keywords: Memristor chaotic system; Image encryption algorithm; DNA variation

P. Li (Author for correspondence), F. Yang, C. Ma
School of Information Science and Engineering, Dalian polytechnic University, Dalian, 116034, China
e-mail: lipeng@dlpu.edu.cn

L. Xiong, F. Yang
School of Physics and Electromechanical Engineering, Hexi University, Zhangye, 734000, China

Y. Zhang
School of Information Science and Technology, Xiamen University Tan Kah Kee College, Zhangzhou 363105, China

1. Introduction

In 1971, memristor is proposed by Chua, it is considered to be the fourth circuit element in
addition to the other three well-known basic components of the circuit. In 2008, Stan Williams found the first prototype memristor used nanoscale coupling ions and electrons [1]. In addition, memristor has many potentially unique applications, such as spintronic devices, ultra-dense information storage, neural circuits, and programming electronic devices [2-4]. Memristor is a nonlinear element, and it can produce complex nonlinear phenomena. Therefore, there is more and more interest in studying the nonlinear system of memristor.

Memristor has typical nonlinear behaviors, chaos phenomena have been found in many memristor circuits. For example, Muthuswamy and Chua proposed a three-dimensional simplest chaotic circuit [5]. Based on Wien-bridge, Ye et al. designed a new hyperchatoic memristor circuit and the circuit was implemented by the actual circuit element hardware [6]. On the base of Chua’s circuit, a four-dimensional hyperchatoic circuit was proposed by Yang et al. [7]. Leng et al. designed a simplest four-dimensional hyperchatoic circuit and analyzed its dynamic characteristics [8]. A simple third-order memristive was obtained by band pass filter circuit in Ref [9]. Dynamic performance of a mixed memristor chaotic circuit was analyzed by Ye et al. [10]. Mou et al. [11] analyzed dynamic characteristic of four-dimensional fractional-order hyperchatoic memristor circuit. And a series of memristor chaotic circuit systems are researched in Ref [12-20]. In the background of the memristor above, in this paper, we designed a new memristor chaotic system based on Chua’s circuit, and used red and blue 3D glasses method to observed chaotic trajectory of the new memristor chaotic system.

Image encryption is an important research direction in chaotic secure communication. At present, there are some image encryption algorithms based on chaotic system [21-34]. Such as Yang et al. [35, 36] designed image encryption algorithm by using fractional-order chaotic system. Chai et al. [37] proposed an image compression and encryption algorithm based on chaotic system and compression sensing. An image encryption scheme by high dimensional chaotic system is introduced by Tong et al. [38]. Yang et al. [39] designed an image encryption algorithm through complex chaotic system. On the base of hyperchatoic map and compression sensing, Xu et al. [40] proposed an fast image compression and encryption scheme. Chai et al. [41] designed a visually secure image encryption algorithm through skew tent map and compression sensing.

To improve security performance of image encryption algorithm, DNA operation is used to image encryption scheme. There are many image encryption algorithms through DNA operation and chaotic system [42-48]. For instance, Liu et al. [48] using DNA complementary rules and chaotic system proposed an image encryption algorithm. An image encryption scheme through DNA computing and chaotic system is designed in Ref [49]. Based on chaotic map and DNA addition rules, an color image encryption scheme is designed by Yang et al. [50]. Liu et al. [51] proposed an image encryption algorithm by chaotic system and DNA operation. Based on DNA deletion and DNA insertion, an image encryption scheme is designed in [52]. So far, image encryption algorithm not using DNA variation. Therefore, we designed an image encryption algorithm based on DNA variation in this paper.

The rest of the paper is organized in the following. In section 2, a new memristor system is obtained and analyzed its dynamic characteristics. The principle of DNA is introduced in section 3. In section 4, we designed an image encryption algorithm based on memristor system and DNA variation. Performance of the designed algorithm is explored in section 5. In section 6, we have given some conclusions.
2 The novel memristor chaotic system

2.1 Mathematical model of the system

As a comparison, the expression of the classical Chua’s circuit is given. In order to show their correspondence more clearly, the shape of the classical Chua’s circuit is written as follows

\[
\begin{align*}
\dot{x} &= \alpha_1 y - \alpha_2 x - \alpha_3 f(x) \\
\dot{y} &= x - y + z \\
\dot{z} &= -\beta y - \gamma z
\end{align*}
\]

(1)

where \(-\gamma z\) represents the additional resistance of the inductor, the nonlinear term \(f(x)\) is

\[
f(x) = \frac{1}{2} (|x + 1| - |x - 1|),
\]

(2)

The mathematical model of Chua's circuit composed of memristor elements as

\[
\begin{align*}
\dot{x} &= \alpha_1 y + \alpha_2 x - \alpha_3 w(x)x \\
\dot{y} &= x - y + z \\
\dot{z} &= -\beta y - \gamma z
\end{align*}
\]

(3)

where

\[
\begin{align*}
\dot{u} &= x \\
w(x) &= a + 3bu^2
\end{align*}
\]

(4)

where \(w(x)\) is memristor, the volt-ampere characteristics as follows

\[
i = (a + 3b\varphi^2)u,
\]

(5)

or

\[
i = au + 3bu(\int udt)^2.
\]

(6)

On the base of Eq.(3)-Eq.(6), the mathematic model of the new memristor chaotic system is obtained as

\[
\begin{align*}
\dot{w}(x) &= a + 3xbu^2 \\
\dot{x} &= \alpha_1 y + \alpha_2 x - \alpha_3 w(x)x \\
\dot{y} &= x - y + z \\
\dot{z} &= -\beta y - \gamma z \\
\dot{u} &= x
\end{align*}
\]

(7)

For the mathematic model of the new memristor chaotic system, when parameters \(\alpha_1=16.4, \alpha_2=6.56, \alpha_3=16.4, \beta=15, \gamma=0.5, a=0.2, b=0.4\), initial value \((x, y, z, u) = (0.2, 0.1, 0.1, 0.1)\), the Lyapunov exponents are 0.3329, 0, -0.0066 and -7.8613, so the new memristor system is chaotic system.

2.2 Red and blue 3D attractor phase diagram of the system

For the traditional method of observe three-dimensional chaotic attractor, although it works, but it is a 2D plane method, it is not able to give full play to the nature of information processing between human eyes and brain information. To get a complete picture of the brain of a three-dimensional...
chaotic attractor, the effect can be achieved using red and blue 3D glasses. The method of red and blue 3D glasses is described as follows.

**Fig. 1** A diagram of the relationship between phase trajectories and the eye.

A conical projection method is shown in Fig. 1. Fig. 1(a) is a description of the chaotic attractor. Assumption three-dimensional origin of chaotic system is O₁, the equation variables of the phase trajectory are x, y and z, the coordinates of the moving point P is (x, y, z). Let x run from left to right, y run from bottom to top, and z run from O₁ run from eye to eye. In Fig. 1(b), Display midpoint position is O₂, and there are two display images, a red image for the left eye and a blue image for the right eye. The two points of P point in chaotic phase diagram are Q_L(x_L, y_L) and Q_R(x_R, y_R) respectively. L is the position of the left eye, R is the position of the right eye, the midpoint between L and R is O₃. Setting the distance between O₁ and O₂ is m, the distance between O₂ and O₃ is m, the distance between L and R is 2d. The graphs of Q_L(x_L, y_L) and Q_R(x_R, y_R) can be obtained from the above relation, and the correlation function can be determined.

The projection point QL and QR ordinate principle of point P on the display is shown in Fig.2.

**Fig. 2** The ordinate coordinates of point P on the display.

According to Fig. 2, we get their relationship as follows

\[
\frac{y}{m + n - z} = \frac{y_R}{n},
\]

(8)

\[
y = \frac{y_R(m + n - z)}{n}.
\]

(9)

The principle of the two abscissa coordinates of point P on the display is Fig. 3.
According to Fig. 3, their relationship is described as follows.

\[ \frac{x_R - x}{m - z} = \frac{d - x}{m + n - z}, \]  
(10)

\[ x_R = \frac{dm + nx - dz}{m + n - z}, \]  
(11)

If \( d \) switch to \(-d\)

\[ x_L = \frac{-dm + nx + dz}{m + n - z}, \]  
(12)

\[ y_R = y_L = \frac{ny}{m + n - z}. \]  
(13)

![Fig.3](image)

**Fig.3** The two horizontal coordinates of point \( P \) on the display.

Based on above to observe the principle, by using write a program, we get the chaotic phase diagram of system (7) as Fig.4. The Fig.4 illustrate that using red and blue 3D glasses not only sees immersive 3D chaotic attractors, but also has significant effects.

**2.3 Dynamic performances of the system**

In this section, to investigate the dynamical performances of the new memristor chaotic system, the Lyapunov exponent spectrum, SE complexity and C0 complexity are used to analyze dynamical characteristics of the new memristor chaotic system.

Keeping initial values and other parameter values, the parameter \( a_1 \in [15.2, 16.6] \) and \( a_2 \in [6.3, 7.3] \), then the corresponding Lyapunov exponent spectra are obtained as Fig. 5. As we see from Fig. 5, when other parameter values are fixed, there is only one parameter changed, the new memristor chaotic system has rich dynamic performance, for example, chaos states, periodic states and so on. In
addition, the chaos state of the system is within a larger parameter range, which illustrates the new memristor chaotic system more suitable for the application of chaotic secure communication.

**Fig.5** Lyapunov exponents spectrum, (a) $\alpha_1 \in [15.2, 16.6]$, (b) $\alpha_2 \in [6.3, 7.3]$.

**Fig.6** Complexity of z sequence, (a) $\alpha_1 \in [15.2, 16.6]$, (b) $\alpha_1 \in [15.2, 16.6]$, (c) $\alpha_2 \in [6.3, 7.3]$, (d) $\alpha_2 \in [6.3, 7.3]$.

In order to test random of chaotic sequence, the SE complexity and C0 complexity tested structural complexity and sequence complexity of chaotic sequence. Based on SE complexity and C0 complexity algorithm, fixing other parameter values and initial values, the parameter $\alpha_1 \in [15.2, 16.6]$ and $\alpha_2 \in [6.3, 7.3]$, then the corresponding complexity results are shown in Fig.6. The Fig.6 shows that chaotic sequence produced by the new memristor chaotic system has good randomness in structure and sequence. Therefore, the chaotic sequences which are produced by the new memristor chaotic system are suitable in secure communication.
3 Principle of DNA

3.1 DNA coding rule

For a DNA sequence, it is constituted by nucleic acid bases A, T, C and G, where A and T are complementary, C and G are complementary. In the modern theory of electronic computers, all information is represented in binary, but in DNA coding theory, all information is represented by DNA sequences with four nucleic acid bases A, T, C and G. In binary sequence, 0 and 1 are complementary, it can be deduced that sequence 00 and 11 are complementary, and sequence 01 and 10 are complementary. Therefore, 00, 01, 10 and 11 are used to code DNA sequence. All coding schemes are 4! = 24, but only 8 coding schemes conform to the Watson Crick complementary rule, the corresponding result is shown in Table 1.

Table 1 DNA coding rule

| Rule | 0  | 1  | 2  | 3  | 4  | 5  | 6  | 7  |
|------|----|----|----|----|----|----|----|----|
| A    | 00 | 00 | 01 | 01 | 10 | 10 | 11 | 11 |
| T    | 11 | 11 | 10 | 10 | 01 | 01 | 00 | 00 |
| C    | 01 | 10 | 00 | 11 | 00 | 11 | 01 | 10 |
| G    | 10 | 01 | 11 | 00 | 11 | 00 | 10 | 01 |

In the process of image encryption, the gray value of each 8bit pixel can be represented by 4 coded DNA sequences. For example, A, T, C and G are used to represent 00, 11, 10 and 01 respectively. Then, the point with a pixel gray value of 121 and the binary sequence are represented as [01111001], the DNA sequence encoded according to code rule 0 in Table 1 is represented as [CTGC].

3.2 Addition and subtraction rule of DNA

With the rapid development of DNA computing, biological and algebraic operations based on DNA sequences have emerged. The addition and subtraction of DNA sequences is similar to that of traditional algebra, such as 01+11 = 00, 01-10 = 11. When using the encoding scheme 0 in Table 1, 00, 11, 01 and 10 respectively represent A, T, C and G, and the detailed corresponding addition and subtraction operations are shown in Table 2.

Table 2 Addition and subtraction of DNA

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

It can be seen from Table 2 that DNA plus operation shows double helix structure, which conforms to Watson Crick complementary rule. DNA subtraction is the opposite of addition, but does not conform to the double helix structure.

3.3 DNA variation rule

DNA mutation refers to the abnormal changes in the structure, replication or phenotypic functions of individual dNMP (deoxynucleoside monophosphate) residues or even fragments of DNA, also known as DNA
damage. According to the type of gene structure change, mutations can be divided into four types: base replacement, transcoding, deletion and insertion. In this paper, we selected base replacement mutations for application in image encryption algorithms. To get a better idea of how base replacement works, a diagram of base replacement mutations is shown in Fig.7.

Fig.7 Diagram of base replacement mutations.

3.4 DNA complementary rule

For the DNA complementary rule, it meets the following principles:

\[
\begin{align*}
F(x) &\neq F(F(x)) \\
&= F(F(F(x)))
\end{align*}
\]

where \( F(x) \) represents the base pair of \( x \), it is a injective mapping to guarantee the DNA complementary rules. There are six groups of DNA complementary rules as follows.

\[
\begin{align*}
F_1(A) &= T, F_1(T) = C, F_1(C) = G, F_1(G) = A \\
F_2(A) &= T, F_2(T) = G, F_2(G) = C, F_2(C) = A \\
F_3(A) &= C, F_3(C) = T, F_3(T) = G, F_3(G) = A \\
F_4(A) &= G, F_4(G) = C, F_4(C) = T, F_4(T) = A' \\
F_5(A) &= G, F_5(G) = T, F_5(T) = C, F_5(C) = A \\
F_6(A) &= C, F_6(C) = G, F_6(G) = T, F_6(T) = A
\end{align*}
\]

where \( F_i \) is the \( i \) complementary rule, \( i=1, 2, 3, 4, 5, 6. \)

4 Image encryption and decryption algorithm based on chaotic system and DNA

4.1 The secret key structure

Table.3 The secret key structure

| \( \alpha_1 \) | \( \alpha_2 \) | \( \alpha_3 \) | \( \beta \) | \( \gamma \) | \( a \) | \( b \) | \( x_0 \) | \( y_0 \) | \( z_0 \) | \( u_0 \) | \( r \) | \( c_0 \) |
|---|---|---|---|---|---|---|---|---|---|---|---|---|

For the designed image encryption algorithm, it’s the secret key structure is shown in Table.3. In the Table.3, \( \alpha_1, \alpha_2, \alpha_3, \beta, \gamma, a \) and \( b \) are parameters of the new memristor chaotic system, \( x_0, y_0, z_0 \) and \( u_0 \) represent initial values of the new memristor chaotic system, \( r \) is DNA coding rule in Table.1, \( c_0 \) means the initial nucleic acid bases.
4.2 Image encryption algorithm

In this section, an image encryption algorithm is designed based on the new memristor chaotic system and DNA operations. The algorithm mainly includes the row and column scrambling, DNA transition, DNA complementary and DNA addition operation. The flowchart of encryption algorithm is shown in Fig.8. The corresponding of specific step is described as follows.

**Fig. 8 Design of encryption algorithm flowchart.**

Step 1 Inputting a plain image $I$, its size is $H\times W$.

Step 2 Setting the parameters $\alpha_1=16.4$, $\alpha_2=6.56$, $\alpha_3=16.4$, $\beta=15$, $\gamma=0.5$, $a=0.2$, $b=0.4$, initial value $(x, y, z, u)=(0.2, 0.1, 0.1, 0.1)$, then based on four order Runge-Kutta algorithm, the new memristor chaotic system (7) is iterated $(m+N)$ times, here $N=\max(H, W)$. The chaotic sequences $x, y, z$ and $u$ are disposed as

$$
\begin{align*}
br & = \text{mod}(\text{floor}(\text{abs}(\frac{(x(m+1:m+H)) \times 10^16)}{W}),2) \\
bc & = \text{mod}(\text{floor}(\text{abs}(\frac{(y(m+1:m+H)) \times 10^16)}{H}),2) \\
x_i & = z(m+1:m+H) \\
y_i & = u(m+1:m+H)
\end{align*}
$$

where $br$, $bc$, $x_1$ and $y_1$ are used to image scrambling algorithm.

Step 3 According to $br$ and $x_1$, the plain image $I$ is scrambled by

$$
\begin{align*}
x_i(i)>0 & \quad \Rightarrow T_i(i,\text{end-br}(i)+1:\text{end})=I(i,1:\text{br}(i)) \\
x_i(i)<0 & \quad \Rightarrow T_i(i,\text{br}(i)+1:\text{end})=I(i,1:\text{end-br}(i)) \\
x_i & = z(m+1:m+H) \\
y_i & = u(m+1:m+H)
\end{align*}
$$

where $T_i$ is the row scrambling result, $i=1, 2, \ldots, H$.

Step 4 According to $bc$ and $y_1$, the row scrambled result $T_i$ is scrambled as

$$
\begin{align*}
y_i(j)>0 & \quad \Rightarrow T(\text{end-bc}(j)+1:\text{end},j)=T_i(1:bc(j),j) \\
y_i(j)<0 & \quad \Rightarrow T(1:bc(j),j)=T_i(\text{bc}(j)+1:\text{end},j) \\
y_i & = z(m+1:m+H) \\
y_i & = u(m+1:m+H)
\end{align*}
$$

where $T$ is the final scrambling result, $j=1, 2, \ldots, W$.

Step 5 Setting the parameters and initial values as Step 2, on the base of four order Runge-Kutta algorithm, the new system memristor system (7) is iterated $(n+H\times W)$ times. The chaotic sequences $x, y,$
$z$ and $u$ are disposed by
\[
\begin{align*}
    p(4^*i-3) &= x(i+n) \\
    p(4^*i-2) &= y(i+n) \\
    p(4^*i-1) &= z(i+n) \\
    p(3^*i) &= w(i+n)
\end{align*}
\]
\[K = \text{mod}(\text{floor}(p^*\text{pow2}(16)), 256)\] (19)

where $K$ is the new sequence.

Step 6 Selected DNA coding rule 1 in Table.1, then the new sequence $K$ is coded, a ($H$, $4\times W$) DNA matrix $K_1$ is obtained.

Step 7 Based on DNA coding rule 1 in Table.1, the scrambled result $T$ is coded, then a ($H$, $4\times W$) DNA matrix $T_2$ is generated.

Step 8 According to DNA base replacement mutations in section 2.3, the DNA matrix $T_2$ is transited by
\[
\begin{align*}
    A &\rightarrow G \\
    T &\rightarrow C
\end{align*}
\]
(20)

Step 9 For the DNA base replacement mutations result of DNA matrix $T_3$, selected initial nucleic acid bases is G, then based on DNA complementary rule in section 2.4, a DNA complementary result $T_3$ is obtained.

Step 10 For the DNA complementary result $T_3$ and DNA matrix $K_1$, according to DNA addition rule in section 2.2, then a new DNA matrix $C_1$.

Step 11 The DNA addition result $C_1$ is decoded as decimalism ($H\times W$) matrix, then the cipher image $C$ is generated.

### 4.3 Image decryption algorithm

The decryption algorithm is similar to encryption algorithm, which the inverse of encryption algorithm. In this paper, decryption algorithm mainly includes DNA subtraction, DNA inverse of complementary, DNA inverse of base replacement and row and column inverse scrambling. The design of decryption algorithm flowchart is shown in Fig.9. The corresponding of steps described as follows.

![Design of decryption algorithm flowchart.](Fig.9)

Step 1 Inputting the cipher image $C$, its size is $H\times W$.

Step 2 Selecting the DNA coding rule 1 in section 2.1, then cipher image $C$ is coded ($H$, $4\times W$) DNA matrix $C_1$.

Step 3 Setting the parameters and initial values as Step 2, on the base of four order Runge-Kutta algorithm, the new memristor system (7) is iterated ($n+H\times W$) times. The chaotic sequences $x$, $y$, $z$ and $u$ are disposed by Eq. (19). The new sequence $F$ is obtained.

Step 4 Selecting the DNA coding rule 1 in section 2.1, then the new sequence $F$ is coded ($H$, $4\times W$)
DNA matrix $F_1$.

Step 4 Based on DNA subtraction in section 2.2, DNA matrix $F_1$ and DNA matrix $C_1$ are operated, and then DNA subtraction result $C_2$ is generated.

Step 5 DNA inverse complementary result $C_3$ is obtained by the DNA complementary rules in section 2.4.

Step 6 DNA inverse transition result $C_4$ is obtained based on Eq. (20).

Step 7 DNA inverse transition result $C_4$ is decoded, then obtained decimalism $(H\times W)$ matrix $C_5$.

Step 8 The same as Step 2 in encryption algorithm, getting the inverse scrambling algorithm $br_1$, $bc_1$, $x_2$ and $y_2$.

Step 9 The inverse scrambling result $T_i$ is obtained by

$$\begin{align}
y_j(j) < 0 & \Rightarrow T(j, end-bc_i(j)+1:end) = C_j(1:bc_i(j), j) \\
y_j(j) > 0 & \Rightarrow T(j, bc_i(j)+1:end) = C_j(1:bc_i(j), j) \\
\end{align}$$  \(21\)

$$\begin{align}
x_i(i) < 0 & \Rightarrow T(i, end-br_i(i)+1:end) = T(i, 1:br_i(i)) \\
x_i(i) > 0 & \Rightarrow T(i, br_i(i)+1:end) = T(i, 1:end-br_i(i)) \\
\end{align}$$  \(22\)

Step 10 The inverse scrambling result $T_i$ is restored to plain image $I$.

### 4.4 Simulation test results

In this paper, to verify the designed image encryption algorithm, gray scale images Lena, Camera, Finger and Fruits with the size of 256×256 are selected as the encryption algorithm test images. In the context of MATLABR2018a, given the secret key values $\alpha_1 = 16.4$, $\alpha_2 = 6.56$, $\alpha_3 = 16.4$, $\beta = 15$, $\gamma = 0.5$, $a = 0.2$, $b = 0.4$, $(x_0, y_0, z_0, w_0) = (0.2, 0.1, 0.1, 0.1)$, $r = 1$ and $c = G$. Then according to the proposed algorithm to read-in image, the image is encrypted operation. The corresponding verification results are shown in Fig.10. The results illustrate that the proposed algorithm can effectively encrypt and decrypt the image.
5 Security performances analysis

To verify algorithm performances, in this section, the following experiment is performed, such as the secret key space analysis, histogram distribution analysis, information entropy analysis, correlation analysis, key sensitivity analysis. In addition, for each analysis method is introduced in detail.

5.1 The secret key space analysis

For an encryption algorithm, if its secret key space is large enough, it can resist brute-force attacks. For our algorithm, according to the secret key structure in section 4.1, we have done many experiments, when \( \alpha_1, \alpha_2, \alpha_3, \beta, \gamma, a, b, x_0, y_0, z_0 \) and \( u_0 \) within error \( 10^{-15} \), the cipher image is decrypted. So secret key space is \( 10^{165} \approx 2^{548} \), it is much bigger than \( 2^{100} \). Therefore our designed algorithm has

Fig. 10 Test results of the proposed algorithm
lager enough secret key space to resist brute-force attacks.

5.2 Histogram distribution analysis

Histogram reflects the distribution of each pixel value in the image. If histogram distribution of the encrypted by ideal encryption algorithm more smooth, which indicates that the proposed encryption algorithm is better.

As we can see from Fig.11, the histogram distribution of cipher image is very smooth, and it has no relation with the histogram of plaintext image. So, the proposed algorithm does not allow the attacker to obtain any useful statistical information by analyzing the cipher image histogram. Therefore, it can prevent statistical attacks.
5.3 Correlation analysis

The adjacent pixels of the original image have a high degree of correlation. Reducing the correlation of adjacent pixels is one of the methods to measure the effectiveness of the encryption algorithm. In this experiment, 2000 pairs of adjacent pixels before and after encryption are randomly selected from horizontal, vertical and diagonal directions respectively, and then the correlation coefficient is calculated by

\[
    r_{uv} = \frac{\text{cov}(u, v)}{\sqrt{D(u)}\sqrt{D(v)}},
\]

(23)

\[
    \text{cov}(u, v) = \frac{1}{N} \sum_{i=1}^{N} (u_i - E(u))(v_i - E(v)),
\]

(24)

\[
    D(u) = \frac{1}{N} \sum_{i=1}^{N} (u_i - E(u))^2,
\]

(25)

\[
    E(u) = \frac{1}{N} \sum_{i=1}^{N} u_i,
\]

(26)

where \( u \) and \( v \) are adjacent pixels value, \( r_{uv} \) is correlation coefficient of the adjacent pixels.

Fig. 12 shows the correlation of adjacent pixels between plaintext and cipher images in horizontal, vertical and diagonal directions. Fig. 12 illustrates that the adjacent pixels of the original image are linearly distributed, and the correlation between adjacent pixels of the encrypted image is greatly reduced.

(a) Plaintext Lena in H  
(b) Plaintext Lena in V  
(c) Plaintext Lena in D  
(d) Cipher Lena in H  
(e) Cipher Lena in V  
(f) Cipher Lena in D  
(g) Plaintext Camera in H  
(h) Plaintext Camera in V  
(i) Plaintext Camera in D
Fig. 12 Correlation distribution analysis

Correlation coefficient values of images are listed in Table. 4. The results illustrate that correlation coefficient values of the original images are close to 1, the correlation coefficient values of the cipher images are close to 0. Therefore, correlation of adjacent pixels is reduced by encryption algorithm,
which indicates that the designed algorithm can prevent some level of statistical attack. In addition, Table.5 listed correlation coefficient value comparison of Lena with different encryption algorithms, which further shows that the proposed algorithm has better security performance.

**Table.4 Correlation coefficient values**

| Images | Plaintext | Horizontal | Vertical | Diagonal |
|--------|-----------|------------|----------|----------|
| Lena   |           | 0.9698     | 0.9413   | 0.9157   |
|        | Cipher    | -0.0059    | 0.0013   | 0.0003   |
| Camera |           | 0.9591     | 0.9345   | 0.9085   |
|        | Cipher    | -0.0461    | -0.0091  | -0.0028  |
| Finger |           | 0.6170     | 0.5585   | 0.5090   |
|        | Cipher    | -0.0231    | 0.0002   | 0.0135   |
| Fruits |           | 0.9721     | 0.9733   | 0.9501   |
|        | Cipher    | -0.0086    | 0.0033   | 0.0053   |

**Table.5 Correlation coefficients comparison**

| Direction | Our algorithm | Ref [21] | Ref [26] | Ref [27] | Ref [28] | Ref [36] |
|-----------|--------------|----------|----------|----------|----------|----------|
| Horizontal| -0.0059      | 0.0023   | 0.0063   | 0.0020   | 0.0124   | -0.0061  |
| Vertical  | 0.0013       | -0.0085  | 0.0062   | -0.0029  | 0.0141   | 0.0014   |
| Diagonal  | 0.0003       | 0.0402   | 0.0069   | -0.0083  | 0.0115   | 0.0062   |

**5.4 Information entropy analysis**

Information entropy is used to measure system complexity, and also used to evaluate performance of encryption algorithm. According to information entropy definition, the information entropy of image is

$$H(m) = - \sum_{i=0}^{L-1} p(m_i) \log_2 p(m_i).$$

where $m_i$ is pixel value, $p(m_i)$ represent the probability of each pixel value appearing. Information entropy of image reflects pixel distribution. The information entropy value is closer to ideal value of 8, which show that the more consistent the distribution of pixel values in the cipher image.

**Table.6 Information entropy results**

| Images | Lena | Camera | Finger | Fruits |
|--------|------|--------|--------|--------|
| Plaintext | 7.4442 | 7.0097 | 7.1075 | 7.3406 |
| Cipher | 7.9978 | 7.9971 | 7.9970 | 7.9976 |

**Table.7 Information entropy comparison**

| Our algorithm | Ref [22] | Ref [23] | Ref [24] | Ref [28] | Ref [29] | Ref [36] |
|---------------|----------|----------|----------|----------|----------|----------|
| 7.9978        | 7.9973   | 7.9970   | 7.7841   | 7.9972   | 7.9972   | 7.9973   |

Table.6 shows that information entropy of cipher image is closer to 8, and also indicates that the pixel values of cipher images are uniformly distributed. Information entropy of Lena comparison results with others algorithms are listed in Table. 7, the results illustrate that the proposed algorithm has a better advantage in information entropy.
5.5 Key sensitivity analysis

![Key sensitivity analysis images](image1.png)

**Fig. 13** The secret key sensitivity analysis

For the secret key structure in section 4.1, the \( \alpha_1, \beta, \gamma, x_0, y_0 \) and \( u_0 \) are respectively changed \( 10^{-15} \), then changed secret key to decrypt Lena cipher image, which test the secret key sensitivity. The corresponding results are shown in Fig.13. The results demonstrate that the algorithm is very sensitive to the secret key, it protects against malicious attacks on the secret key.

5.6 Data loss analysis

![Data loss analysis images](image2.png)

**Fig. 14** The data loss analysis

To verify the encryption algorithm’s ability to resist data loss, in this test, the Lena cipher image are lost data of different degrees, then by using decryption algorithm to decrypt the corresponding
cipher images. Test results are shown in Fig. 14. The analysis results indicate that the designed encryption algorithm can prevent some degrees data loss attacks.

### 5.7 Noise attack analysis

![Images of noise attack analysis](image)

**Fig. 15** The noise attack analysis

Noise attack is a common attack mode in the process of information transmission. To test the proposed algorithm has ability to prevent noise attack, different intensity of Gaussian noise and Salt & Pepper are added to the Lena cipher image, then using the decryption algorithm to decrypt cipher image, the results are shown in Fig. 15. The results illustrate that the proposed algorithm has ability to prevent some degrees noise attacks.

### 6 Conclusions

In this paper, a new memristor chaotic system is obtained, red and blue 3D glasses is used to obverse chaotic trajectory. The dynamic performance of the new memristor chaotic system is analyzed by Lyapunov exponent spectrum, SE complexity and C0 complexity. The results show that using red and blue 3D glasses not only sees immersive 3D chaotic attractors, but also has significant effects. Dynamic analysis illustrates that the new memristor chaotic system has rich dynamic characteristic, and chaos state is distributed over a large parameter range, which indicates that it is more suitable for image encryption application. More significantly, the designed encryption algorithm based on new memristor chaotic system and DNA variation to ensure the safe transmission and storage of image information. In this algorithm, the rows and columns shifts are used to scrambling pixel position, DNA transition, DNA complementary and DNA addition are used to diffuse pixel values. The security analysis illustrates that the new memristor chaotic system and DNA variation are used in image encryption algorithm, it improve security of the image encryption algorithm.
Acknowledgement

This work was supported by the Innovation fund project of colleges and universities in Gansu Province in 2020 (Grant No. 2020B-204); the Natural Science Foundation of Liaoning province (2020-MS-274); the National Natural Science Foundation of China (Grant Nos. 62061014)

Author contributions

Li Xiong and Yingqian Zhang carried out experiments, data analyzed and manuscript wrote. Peng Li made the theoretical guidance for this paper. Feifei Yang and Chenguang Ma improved the algorithm. All authors reviewed the manuscript.

Conflicts of Interest

No conflicts of interests about the publication by all authors.

References

[1] Dmitri, Strukov, Gregory, Snider, Duncan, Stewart, The missing memristor found, Nature, 453, 80-83, (2008).
[2] Q. Xia, W. Robinett, M.W. Cumbie, N. Banerjee, T.J. Cardinali, J.J. Yang, W. Wu, X. Li, W.M. Tong, D.B. Strukov, Memristor?CMOS Hybrid Integrated Circuits for Reconfigurable Logic, Nano Letters, 9,3640-3645 (2009).
[3] M.D. Ventra, Y.V. Pershin, L.O. Chua, Circuit elements with memory: memristors, memcapacitors and meminductors, Proceedings of the IEEE, 97,1717-1724(2009).
[4] J. Borghetti, Z. Li, J. Straznicky, X. Li, D.A.A. Ohlberg, W. Wu, D.R. Stewart, R.S. Williams, A hybrid nanomemristor/transistor logic circuit capable of self-programming, Proceedings of the National Academy of Sciences of the United States of America, 106 ,1699-1703 (2009).
[5] B. Muthuswamy, L.O. Chua, Simplest Chaotic Circuit, International Journal of Bifurcation & Chaos, 20,1002707-(2010).
[6] X. Ye, J. Mou, C. Luo, Z. Wang, Dynamics analysis of Wien-bridge hyperchaotic memristive circuit system, Nonlinear Dynamics, 92(3), 923-933 (2018).
[7] F.Y. Yang, J.L. Leng, Q.D. Li, The 4-dimensional hyperchaotic memristive circuit based on Chua's circuit, Acta Physica Sinica, 63(8): 080502 (2014).
[8] J. Leng, Y. Cao, K. Zhao, Dynamics Analysis of Hyperchaotic Circuit, Applied Physics Frontier, 2(2), 8-11 (2014).
[9] B. Bao, W. Ning, X. Quan, H. Wu, Y. Hu, A Simple Third-Order Memristive Band Pass Filter Chaotic Circuit, IEEE Transactions on Circuits & Systems II Express Briefs, 64,977-981(2017).
[10] X. Ye, J. Mou, C. Luo, F. Yang, Y. Cao, Complexity Analysis of a Mixed Memristive Chaotic Circuit, Complexity, 2018, 8639470, (2018).
[11] J. Mou, K. Sun, H. Wang, R. Jingya, Characteristic Analysis of Fractional-Order 4D Hyperchaotic Memristive Circuit, Mathematical Problems in Engineering, 2017(8), 80502, (2017).
[12] D. Ding, S. Li, N. Wang, Dynamic Analysis of Fractional-Order Memristive Chaotic System, Journal of Harbin Institute of Technology, 25, 54-62 (2018).

[13] Y. Song, F. Yuan, Y. Li, Coexisting Attractors and Multistability in a Simple Memristive Wien-Bridge Chaotic Circuit, Entropy, 21(7), 678 (2019).

[14] B.C. Bao, P.Y. Wu, H. Bao, Q. Xu, M. Chen, Numerical and experimental confirmations of quasi-periodic behavior and chaotic bursting in third-order autonomous memristive oscillator, Chaos Solitons & Fractals, 106, 161-170(2018).

[15] F. Yang, P. Li, Characteristics Analysis of the Fractional-Order Chaotic Memristive Circuit Based on Chua's Circuit, Mobile Networks and Applications, 2019(5), 1-9, 2019.

[16] L. Xiong, Y. Lu, Y. Zhang, X. Zhang, A Novel Memductor-Based Chaotic System and Its Applications in Circuit Design and Experimental Validation, Complexity, 2019, 3870327, (2019).

[17] F. Yu, L. Liu, H. Shen, Z. Zhang, Y. Huang, C. Shi, S. Cai, X. Wu, S. Du, Q. Wan, Dynamic Analysis, Circuit Design, and Synchronization of a Novel 6D Memristive Four-Wing Hyperchaotic System with Multiple Coexisting Attractors, Complexity, 2020, 5904607, (2020).

[18] F. Yu, L. Liu, B. He, Y. Huang, C. Shi, S. Cai, Y. Song, S. Du, Q. Wan, Analysis and FPGA Realization of a Novel 5D Hyperchaotic Four-Wing Memristive System, Active Control Synchronization, and Secure Communication Application, Complexity, 2019, 4047957 (2019).

[19] F. Yu, H. Shen, L. Liu, Z. Zhang, Y. Huang, B. He, S. Cai, Y. Song, B. Yin, S. Du, Q. Xu, CCII and FPGA Realization: A Multistable Modified Fourth-Order Autonomous Chua’s Chaotic System with Coexisting Multiple Attractors, Complexity, 2020, 5212601 (2020).

[20] Q. Lai, Z. Wan, P.D. Kamdem Kuate, H. Fotsin, Coexisting attractors, circuit implementation and synchronization control of a new chaotic system evolved from the simplest memristor chaotic circuit, Communications in nonlinear science & numerical simulation, 89,105341(2020).

[21] Z. Hua, Y. Zhou, C.M. Pun, C.L.P. Chen, 2D Sine Logistic modulation map for image encryption, Information Sciences, 297,80-94(2015).

[22] C. Cao, K. Sun, W. Liu, A novel bit-level image encryption algorithm based on 2D-LICM hyperchaotic map, Signal Processing, 78, 17-25, (2017).

[23] X.Y. Wang, Y.Q. Zhang, X.M. Bao, A novel chaotic image encryption scheme using DNA sequence operations, Optics & Lasers in Engineering, 73,53-61(2015).

[24] X. Zhang, X. Wang, Multiple-image encryption algorithm based on mixed image element and chaos, Computers & Electrical Engineering, 11(1):1–13 32,(2017).

[25] M. Ge, R. Ye, A novel image encryption scheme based on 3D bit matrix and chaotic map with Markov properties, Egyptian Informatics Journal, 2019(20), 45-54, (2019).

[26] X. Wang, K. Guo, A new image alternate encryption algorithm based on chaotic map, Nonlinear Dynamics, 76,1943-1950(2014).

[27] W. Zhang, H. Yu, Y.L. Zhao, Z.L. Zhu, Image encryption based on three-dimensional bit matrix permutation, Signal Processing, 118 ,36-50 (2016).

[28] L. Xu, Z. Li, J. Li, W. Hua, A novel bit-level image encryption algorithm based on chaotic maps, Optics & Lasers in Engineering, 2016(78), 17-25, (2016).

[29] X. Wang, S. Wang, N. Wei, Y. Zhang, A Novel Chaotic Image Encryption Scheme Based on Hash Function and Cyclic Shift, Iete Technical Review, 36, 39-48(2019).

[30] H. Liu, A. Kadir, J. Liu, Color pathological image encryption algorithm using arithmetic over Galois field and coupled hyper chaotic system, Optics & Lasers in Engineering, 2019(122) ,123-133 (2019).
[31] Y. Huang, L. Huang, Y. Wang, Y. Peng, F. Yu, Shape synchronization in driver-response of 4-D chaotic system and its application in image encryption, IEEE Access, 2020(8), 135308-135319, (2020).
[32] Q. Lai, B. Norouzi, F. Liu, Dynamic analysis, circuit realization, control design and image encryption application of an extended Lü system with coexisting attractors, Chaos, solitons and fractals, 114,230-245 (2018).
[33] H. Liu, A. Kadir, P. Gong, A fast color image encryption scheme using one-time S-Boxes based on complex chaotic system and random noise, Optics communications, 338,340-347(2015).
[34] H. Liu, Y. Zhang, A. Kadir, Y. Xu, Image encryption using complex hyper chaotic system by injecting impulse into parameters, Applied mathematics and computation, 360,83-93 (2019).
[35] F. Yang, J. Mou, C. Ma, Y. Cao, Dynamic analysis of an improper fractional-order laser chaotic system and its image encryption application, Optics and Lasers in Engineering, 129,106031(2020).
[36] F. Yang, J. Mou, J. Liu, C. Ma, H. Yan, Characteristic analysis of the fractional-order hyperchaotic complex system and its image encryption application, Signal Processing, 169, 107373 (2020).
[37] X. Chai, X. Zheng, Z. Gan, D. Han, Y. Chen, An image encryption algorithm based on chaotic system and compressive sensing, Signal Processing, 148 124-144, 2018.
[38] X.J. Tong, M. Zhang, Z. Wang, A new image encryption algorithm based on the high-dimensional chaotic map, Journal of Photographic Science, 63,263-272(2015).
[39] F. Yang, J. Mou, H. Yan, J. Hu, Dynamical analysis of a novel complex chaotic system and application in image diffusion, IEEE Access, 7(1), 118188-118202, (2019).
[40] Q. Xu, K. Sun, C. Cao, C. Zhu, A fast image encryption algorithm based on compressive sensing and hyperchaotic map, Optics and Lasers in Engineering, 121, 203-214, (2019).
[41] X. Chai, Z. Gan, Y. Chen, Y. Zhang, A visually secure image encryption scheme based on compressive sensing, Signal Processing, 2017(134), 35-51, (2017).
[42] P. Li, J. Xu, J. Mou, F. Yang, Fractional-order 4D hyperchaotic memristive system and application in color image encryption, EURASIP Journal on Image and Video Processing, 2019, 22, (2019).
[43] H. Liu, X. Wang, A. Kadir, Image encryption using DNA complementary rule and chaotic maps, Applied Soft Computing, 2012(12), 1457-1466, 2012.
[44] Q. Zhang, L. Liu, X. Wei, Improved algorithm for image encryption based on DNA encoding and multi-chaotic maps, AEU - International Journal of Electronics and Communications, 68,186–192, (2014).
[45] Q. Zhang, Q. Wang, X. Wei, A Novel Image Encryption Scheme Based on DNA Coding and Multi-Chaotic Maps, 3,447-451, (2010).
[46] K. Xuejing, G. Zihui, A new color image encryption scheme based on DNA encoding and spatiotemporal chaotic system, Signal Processing Image Communication, 2020(80), 115670, (2019).
[47] X. Chai, Z. Gan, K. Yang, Y. Chen, X. Liu, An image encryption algorithm based on the memristive hyperchaotic system, cellular automata and DNA sequence operations, Signal Processing Image Communication, 52, 6-19, (2017).
[48] X. Ouyang, Y. Luo, J. Liu, L. Cao, Y. Liu, A color image encryption method based on memristive hyperchaotic system and DNA encryption, International Journal of Modern Physics B, 34(4), 2050014, (2020).
[49] X. Chai, Z. Gan, L. Yang, Y. Chen, D. Han, A novel image encryption algorithm based on chaotic system and DNA computing, International Journal of Modern Physics C, 28(5), 1750069, (2017).
[51] F. Yang, J. Mou, C. Luo, Y. Cao, An improved color image encryption scheme and cryptanalysis based on a hyperchaotic sequence, Physica Scripta, 94, 85206, (2019).
[51] Y. Liu, J. Zhang, A Multidimensional Chaotic Image Encryption Algorithm based on DNA Coding, 79, 21579–21601, (2020).

[52] Ting, Liu, Ye, Gong, Li-Hua, Guo, Shao-Feng, Yuan, Hong-Mei., Chaotic image cryptosystem using DNA deletion and DNA insertion, Signal Processing, 2017(134), 234-243, (2017).