EURASIP Journal on Image and Video Processing

RESEARCH Open Access

Fractional-order 4D hyperchaotic memristive system and application in color image encryption

Peng Li, Ji Xu, Jun Mou* and Feifei Yang

Abstract

In this paper, some properties of the fractional-order four-dimensional (4D) hyperchaotic memristive system are analyzed by the phase diagram, Lyapunov exponent spectrum and bifurcation diagram according to the Adomian decomposition method. Based on the chaotic system, a color image encryption scheme is proposed through combining the DNA sequence operation. The algorithm simulation results and security feature analysis show that the encryption scheme has good encryption effect and high safety performance, which provides an experimental basis and theoretical guidance for the safe transmission of image information.

Keywords: Color image encryption, Security analysis, DNA sequence operations, Fractional-order 4D hyperchaotic memristive system

1 Introduction

Nowadays, digital image is an improtant carrier of information, because of the inherent performance of digital images, including bulk data capacity, high redundancy and extremely strong correlation in adjacent pixels, which make digital image processing a research hotspot. For example, prediction error preprocessing for image compression [1], histogram equalization of images [2], image compression and reconstruction [3], and so on. To achieve the requirement of digital image safety transmission, researchers are interested in an encryption algorithm based on a chaotic system. Chaos is a random or uncertain movement in a particular system. It has inherent properties of ergodicity, sensitivity of initial value and parameters, and complex dynamic characteristic [4, 5]. Especially, chaotic attractors coexist [6, 7]. Therefore, a chaos system could be used in the image encryption fields.

Up to now, all kinds of image encryption algorithms through chaotic system are proposed [1, 8–13]. For example, Hua et al. [8] proposed an image encryption scheme using 2D Logistic-adjusted-Sine map. Yang et al. [9] presented novel quantum image encryption through 1D quantum cellular automata. Because low-dimensional chaotic maps have fewer system parameters, the structures are simple. The system parameters and initial value may be predicted by using chaotic signal estimation technologies. On the contrary, high-dimensional chaotic maps, especially hyperchaotic maps, possess excellent chaotic performance and complex structure. Therefore, Natiq et al. [10] designed a new hyperchaotic map and its application for image encryption. Luo Y and his research team [11] proposed a parallel image encryption algorithm through two chaotic maps.

Recently, an encryption scheme using DNA addition in combination with chaotic system was proposed by Zhang et al. [14]. Soon afterwards, some cryptosystems were applied to DNA sequence operations and chaotic systems [2–5, 7, 15–27]. These schemes applied DNA encoding and DNA sequence operation to encrypt images. An idea of DNA subsequence operation, rather than complex biological operation of image encryption scheme, was introduced by Zhang et al. [25]. Liu and his research team [26] employed a chaotic map and the DNA complementary rule in an image encryption algorithm. SaberiKamarposhti et al. [27] proposed hybrid image encryption algorithm through DNA sequences and a logistic map. However, compared with the general chaotic system, the fractional-order system has nonlocal

* Correspondence: moujun@csu.edu.cn
School of Information Science and Engineering, Dalian Polytechnic University, Dalian, China

character and high nonlinearity, and the encryption algorithm of fractional-order chaotic has higher security features [20, 28]. Compared with the general chaotic system, dynamic features of the memristor chaotic system depend not only on system parameters but also on the initial conditions of memristor retention internal state variables [29, 30]. However, the memristor chaotic systems are not widely used for image and data encryption algorithms. Therefore, to improve the safety performance of image encryption algorithm, in this paper, a color image encryption using a fractional-order 4D hyperchaotic memristive system and DNA sequence operations is proposed.

The following is the architecture of this paper. Preliminary materials are described in Section 2. The encryption and decryption scheme and the simulation results are presented in Section 3. In Section 4, security performance is analyzed. Finally, the conclusion is given in Section 5.

2 Preliminary materials

2.1 Adomian decomposition method

For a certain fractional-order differential equation ${}^{*}Dq\ to(t) = f(x(t))$, here $x(t) = [x_1(t), x_2(t), \ldots, x_n(t)]^{T}$, ${}^{*}Dq\ to$ are variables and ${}^{*}Dq\ to$ is the Caputo derivative operator of order $q((m-1) < q \le m,\ m \in N)$. The following initial value is obtained by making $f(x(t))$ been separated into three parts [31, 32]:

$$\begin{cases} {}^{*}D^{q}_{to}x(t) = Lx(t) + Nx(t) + g(t) \\ x^{(k)}(t_0^{+}) = b_k, k = 0, 1, \ldots, m-1 \end{cases} \tag{1}$$

Here, L and N are linear and nonlinear parts of system functions, $g(t) = [g_1(t), g_2(t), \ldots, g_n(t)]^{T}$ are constants for autonomous systems, and b_k is a specified constant. On both sides of Eq. (3) perform $Jq\ to$ operators, the following equation is obtained [33]:

$$x = J^{q}_{t0}Lx + J^{q}_{t0}Nx + J^{q}_{t0}g + \sum_{k=0}^{m-1} b_k \frac{(t-t_0)^k}{k!} \tag{2}$$

$Jq\ to$ is fractional integral operator of order q based on Riemann-Liouville. For $t \in [t_0, t_1]$, $q \ge 0$, $r \ge 0$, $\gamma > -1$ and real constant C, the fundamental properties of $Jq\ to$ are described by [34]:

$$J^{q}_{t0}(t-t_0)^{\gamma} = \frac{\Gamma(\gamma+1)}{\Gamma(\gamma+1+q)}(t-t_0)^{\gamma+q} \tag{3}$$

$$J^{q}_{t0}C = \frac{C}{\Gamma(q+1)}(t-t_0)^{q} \tag{4}$$

$$J^{q}_{t0}J^{r}_{t0}x(t) = J^{q+r}_{t0}x(t) \tag{5}$$

Based on ADM, the nonlinear terms of Eq. (4) are decomposed according to

$$\begin{cases} A^{i}_{j} = \frac{1}{i!}\left[\frac{d^{i}}{d\lambda^{i}}N\left(v^{i}_{j}(\lambda)\right)\right]_{\lambda=0} \\ v^{i}_{j}(\lambda) = \sum_{k=0}^{i}(\lambda)^{k}x^{k}_{j} \end{cases} \tag{6}$$

where $i = 0,1,\ldots,\infty$, $j = 1,2,\ldots n$. Then the nonlinear terms are expressed as

$$Nx = \sum_{i=0}^{\infty} A^{i}\left(x^{0}, x^{1}, \ldots, x^{i}\right) \tag{7}$$

So the solution of Eq. (3) $x = \sum\infty\ i = 0$ is derived from

$$\begin{cases} x^{0} = J^{q}_{t0}g + \sum_{k=0}^{m-1} b_k \frac{(t-t_0)^k}{k!} \\ x^{1} = J^{q}_{t0}Lx^{0} + J^{q}_{t0}A^{0}\left(x^{0}\right) \\ x^{2} = J^{q}_{t0}Lx^{1} + J^{q}_{t0}A^{1}\left(x^{0}, x^{1}\right) \\ \ldots \\ x^{i} = J^{q}_{t0}Lx^{i-1} + J^{q}_{t0}A^{i-1}\left(x^{0}, x^{1}, \ldots, x^{i-1}\right) \\ \ldots \end{cases} \tag{8}$$

2.2 Fractional-order 4D hyperchaotic memristive system

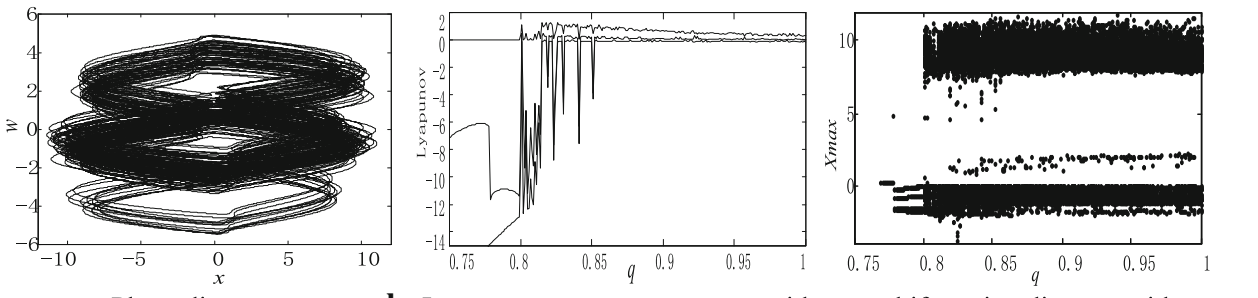
The fractional-order 4D hyperchaotic memristive system is described by [30]:

$$\begin{cases} D^{*q}_{t0}x = \alpha(y-x) \\ D^{*q}_{t0}y = -xz + \beta y - \rho W(w)x \\ D^{*q}_{t0}z = xy - \gamma z \\ D^{*q}_{t0}w = x \end{cases} \tag{9}$$

where x, y, z and w are the stateful variables of chaotic system, $q(0 < q \le 1)$ is the order of fractional-order differential equation, where $W(w)$ is defined as $W(w) = a + 3bw^2$, and a, b, α, β, γ, and ρ are the system parameters.

In order to evaluate the chaotic system for image encryption, the dynamic characteristics of the fractional-order 4D hyperchaotic memristive system by the phase diagram, Lyapunov exponent spectrum, and bifurcation diagram are analyzed according to Adomian decomposition method.

Let parameters $a = 4$, $b = 0.01$, $\alpha = 36$, $\beta = 20$, $\gamma = 3$, $q = 0.85$ and $\rho = 3$, the initial value of the Eq. (9) is (1, 0, 1, 0). We get the phase diagram shown Fig. 1a. Then make parameters $a = 4$, $b = 0.01$, $\alpha = 36$, $\beta = 20$, $\gamma = 3$, $\rho = 3$ and versus $q \in [0.75, 1]$. The Lyapunov exponent spectrum and bifurcation diagram of the fractional-order 4D hyperchaotic memristive system are obtained as shown in Fig. 1b and c. Obviously, the phase diagram, Lyapunov exponent spectrum and bifurcation diagram of the fractional-order 4D hyperchaotic memristive system distribute in a large region. This means that the system has good randomness, large key space and pseudorandom sequence generator.



a Phase diagram

b Lyapunov exponent spectrum with a=4, b=0.01, α=36, β=20, γ=3, ρ=3

c bifurcation diagram with a=4, b=0.01, α=36, β=20, γ=3, ρ=3

Fig. 1 Dynamic analysis of 4D hyperchaotic memristive system. **a** Phase diagram; **b** Lyapunov exponent spectrum with $a = 4$, $b = 0.01$, $\alpha = 36$, $\beta = 20$, $\gamma = 3$, $\rho = 3$, versus $q \in [0.75,1]$; **c** bifurcation diagram with $a = 4$, $b = 0.01$, $\alpha = 36$, $\beta = 20$, $\gamma = 3$, $\rho = 3$, versus $q \in [0.75,1]$

2.3 DNA encoding and decoding rules

A DNA sequence is composited of four nuclear acid bases ATCG (adenine, thymine, cytosine, guanine); here, A and T are complementary, and C and G are complementary. The information is represented binary in the current generation theory of the electronic computer, and in the DNA coding theory, all information is represented by four nuclear acid bases A, T, C, G. According to complementary rules of binary 0 and 1, the 00 and 11 are complementary, and 01 and 10 are complementary. Therefore, acid bases A, T, C and G are encoded 00, 01, 10 and 11. Obviously, the coding rules has 4! = 24 kinds, but only 8 kinds of coding rules are satisfied with Watson-Crick mutual complement rule [35], as shown in Table 1. DNA decoding is the opposite of DNA encoding. For instance, if the value of image pixel is 152, we can get the corresponding binary sequence "10011000," and it can be encoded as "TCGA" based on Rule 1. If the encoded sequence is "TGCA," it can be decoded "00100111" by Rule 3, the final DNA decoding result is decimal value 39.

2.4 DNA addition and subtraction rules

On the basis of traditional binary addition and subtraction, the DNA addition and subtraction are obtained. Thus, according to the eight kinds of DNA encoding rules, we can get the corresponding eight kinds of DNA addition and subtraction rules. For example, on the basis of DNA encoding rule 1, DNA addition rule 1 and subtraction rule 1 are shown in Table 2.

2.5 DNA complementary rule

The DNA complementary rule [26] must satisfy Eq. (10) for each nucleotide x_i.

$$\begin{cases} x_i \neq L(x_i) \neq L(L(x_i)) \neq L(L(L(x_i))) \\ x_i = L(L(L(L(x_i)))) \end{cases} \tag{10}$$

where $L(x_i)$ and x_i are basic pairs and they are complementary, the basic pairs are satisfied with the injective map.

On the basis of (12), there are six kinds of reasonable combination of complementary base pairs, as shown below:

(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,...,6) represents the ith complement rule.

In the diffusion of pixels, used DNA complementary rule bases complementary replacement, and we can randomly select one of the six kinds of complementary combination rules are complementary to replace, which achieve the goal of pixel diffusion.

3 Method - image encryption and decryption algorithm

3.1 The key design

The key design of the proposed color image encryption algorithm is shown in Fig. 2. It consists of five

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	T	A
10	G	C	G	C	A	T	A	T
11	T	T	A	A	C	C	G	G

Table 2 Addition rules 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

a	b	w_0	x_0	y_0	z_0	m	m	c_0	α	β	γ	q	ρ	$\alpha 1$	$\beta 1$

Fig. 2 Key format

parts, chaotic system initial values(x_0,y_0,z_0,w_0), parameters a, b, α, β, γ, q, ρ, cycle numbers m, n, starting acid base c_0($c_0 \in$A, T, C, G) and DNA encoding rules in Table 1 $\alpha 1$, $\beta 1$($\alpha 1$, $\beta 1 \in$ [1, 8]).

3.2 Image encryption algorithm

3.2.1 Pixel position scrambling

The pixel location is scrambled in order to destroy correlation of the original image, and an image is rearranged, which makes the image become disturbed. The random sequences through the fractional-order 4D hyperchaotic memristive system are generated, and the image is permutated. The detailed confusion process can be presented as the following steps.

***Step* 1.** The input is color original image I with the size of $M \times N \times 3$. Setting secret key values a, b, α, β, γ, q, ρ, x_0, y_0, z_0, w_0. New initial conditions of the fractional-order 4D hyperchaotic memristive system are generated by

$$s = \frac{\left[\sum_{i=1}^{M}\sum_{j=1}^{N}\sum_{k=1}^{3} I(i,j,k)\right]}{10^{10}} \tag{11}$$

$$\begin{cases} x_0^{'} = x_0 + s \\ y_0^{'} = y_0 + s \\ z_0^{'} = z_0 + s \\ w_0^{'} = w_0 + s \end{cases} \tag{12}$$

***Step* 2.** Setting the $L = \max(M, N)$. Let the chaotic system (9) iterate for $(m + L)$ times based on new initial conditions, and then throw out the former m values to improve initial value sensitivity. The four chaotic sequences $\{x_i\}L\ i = 1$, $\{y_i\}L\ i = 1$, $\{z_i\}L\ i = 1$ and $\{w_i\}L\ i = 1$ are obtained by Eq. (9). The following shift step numbers are used for scrambling:

$$Bri = \mod\left(\left\lfloor |x_i| \times 10^{16} \right\rfloor, \frac{N}{2}\right) \tag{13}$$

$$Bcj = \mod\left(\left\lfloor \left|y_j\right| \times 10^{16} \right\rfloor, \frac{M}{2}\right) \tag{14}$$

where Bri means that the cyclic step size of row i, and Bcj is the cyclic step number of column j. Here, $i = 1,2,...,M$, $j = 1,2,...,N$.

***Step* 3.** Color image I is decomposed into R, G, B parts, and then R, G, B parts are converted into three matrices and the rows are shifted. The shift results $TR1$, $TG1$ and $TB1$ are obtained by the following rules. Assumption $x_i > 0$, let the row i of R would be moved to left and step number is Bri; otherwise, the row i of R would be moved to the right with step number Bri, where $i = 1,2,...,M$. The same rules are used as in the G and B channels.

***Step* 4.** The columns shift results TR, TG and TB are obtained as follows. When $y_j > 0$, the column j of $TR1$ would be moved up with the size of step is Bcj, or else the column j of $TR1$ would be moved down with the size of step is Bcj, where $j = 1,2,...,N$. The same rules are used as in the $TG1$ and $TB1$.

3.2.2 DNA sequence operation

The pixel values are diffused according to DNA operations and include addition and complementary operations. Specific steps are as follows.

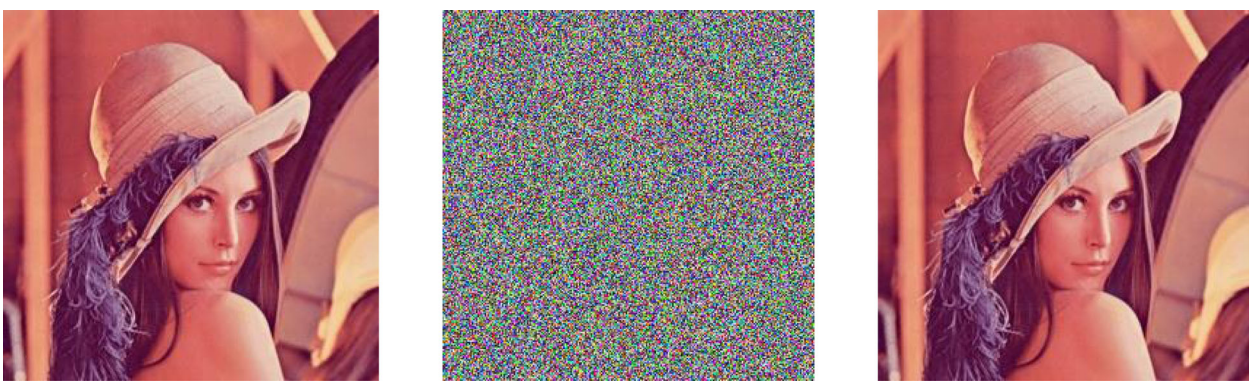


Fig. 3 Encryption and decryption results. **a** Original Lena image; **b** encrypted Lena image; **c** decrypted Lena image

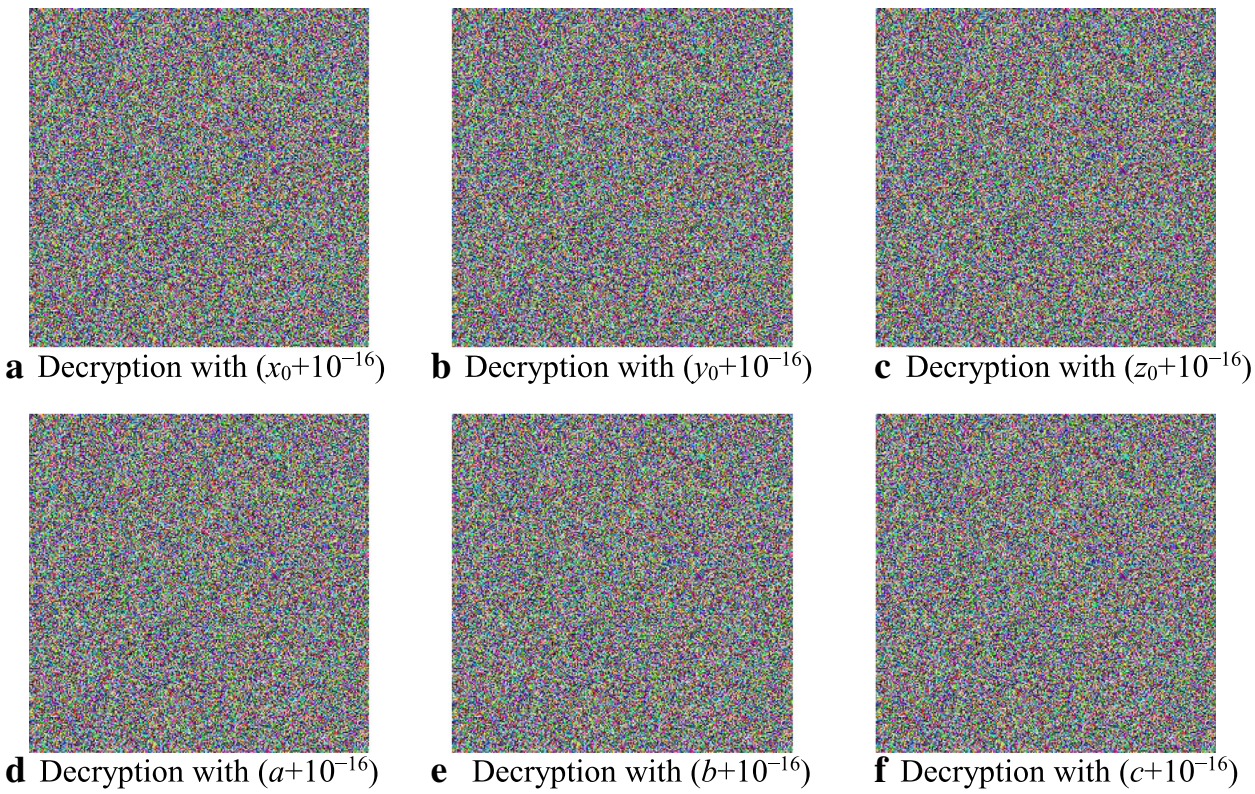


Fig. 4 Key sensitivity test results. **a** Decryption with ($x_0 + 10^{-16}$); **b** decryption with ($y_0 + 10^{-16}$); **c** decryption with ($z_0 + 10^{-16}$); **d** decryption with ($a + 10^{-16}$); **e** decryption with ($b + 10^{-16}$); **f** decryption with ($c + 10^{-16}$)

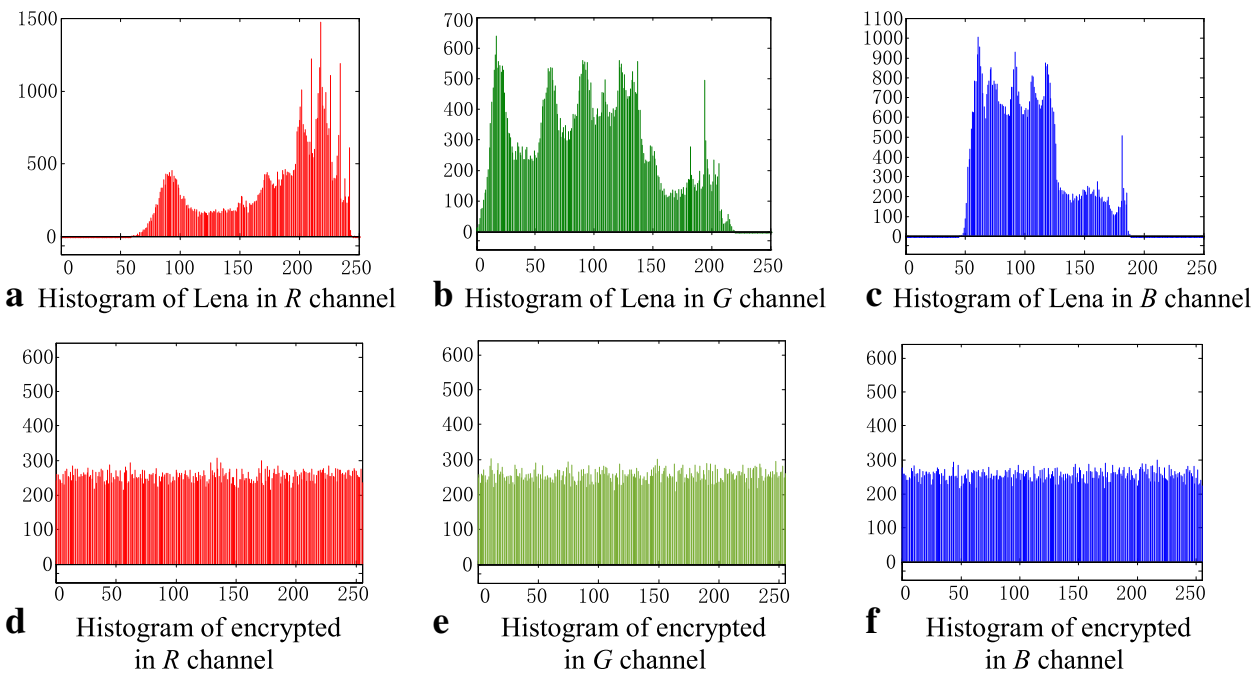


Fig. 5 Histogram of the color Lena image and cipher image. **a** Histogram of Lena in *R* channel; **b** histogram of Lena in *G* channel; **c** histogram of Lena in *B* channel; **d** histogram of encrypted in *R* channel; **e** histogram of encrypted in *G* channel; **f** histogram of encrypted in *B* channel

Table 3 Correlation coefficients in *R*, *G*, *B* channels

Channels	Direction	Original Lena image	Our Algorithm	Ref [12]	Ref [20]
R channel	Horizontal	0.9556	− 0.0025	0.0032	0.0031
	Vertical	0.9780	0.0913	0.0058	− 0.0009
	Diagonal	0.9434	0.0011	0.0133	0.0027
G channel	Horizontal	0.9443	0.0058	0.0068	− 0.0018
	Vertical	0.9711	− 0.0372	0.0042	0.0079
	Diagonal	0.9301	− 0.0014	0.0130	− 0.0002
B channel	Horizontal	0.9280	− 0.0058	0.0014	0.0033
	Vertical	0.9575	0.0036	0.0035	− 0.0049
	Diagonal	0.9030	2.1180e-04	0.0091	0.0015

***Step* 1.** The $M \times 8N$ binary matrices R, G and B are obtained by TR, TG and TB. Then the matrices R, G and B are encoded through the DNA encoding Rule α, and then the $M \times 4N$ DNA matrix $S1$, $S2$ and $S3$ are obtained.

***Step* 2.** Setting the chaotic system initial values of x_0, y_0, z_0, w_0 and getting chaotic sequences $\{x_i\}MN\ i = 1$, $\{y_i\}MN\ i = 1$, $\{z_i\}MN\ i = 1$, $\{w_i\}L\ i = 1$ by iterating system (1) ($n + M \times N$) times and discarding the former n values. Three sequences $k1$, $k2$ and $k3$ are obtained by

$$\begin{cases} k1 = \mod(\lfloor |x_i| \rfloor) \times 10^{16}, 256) \\ k2 = \mod(\lfloor |y_i| \rfloor) \times 10^{16}, 256) \\ k3 = \mod(\lfloor |z_i| \rfloor) \times 10^{16}, 256) \end{cases} \quad (15)$$

where $i = 1,2,\ldots,MH$.

***Step* 3.** The sequence $k1$, $k2$ and $k3$ are transformed into binary matrix, and the matrixes are encoded according to the same DNA rule α to get three $M \times 4N$ matrixes $K1$, $K2$ and $K3$.

***Step* 4.** According to the DNA complementary rule, the middle encryption result of DNA formulation matrix $C = \{c_i\}4MN\ i = 1$ is obtained as follows:

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

Table 4 Identical position with *R*, *G*, *B*

Images	*R*, *G*	*R*, *B*	*G*, *B*
Fig. 5a	0.8849	0.7013	0.9326
Fig. 5b	− 0.0060	− 0.0035	0.0076
Ref [20]	0.0001	− 0.0019	0.0029

***Step* 5.** The encrypted image of DNA sequence $D = \{d_i\}4MN\ i = 1$ is calculated by

$$d_i = c_i + K(i) + d_{i-1} \quad (16)$$

Here, $i = 1,2,\ldots,MH$. "+" means that the DNA addition operation, and $d_0 = c_{4MN}$. Three DNA matrices $D1$, $D2$ and $D3$ are obtained by Eq. (18).

***Step* 6.** The matrices $D1$, $D2$, and $D3$ are decoded by DNA Rule β and then recovering three binary formulations $C1$, $C2$ and $C3$. Finally, the encrypted image C by combination $C1$, $C2$ and $C3$ is obtained.

3.3 Decryption algorithm

The decryption algorithm is a process of restoring the original image. First, the encryption image C is decomposed $C1$,$C2$ and $C3$, and then $C1$,$C2$ and $C3$ are encoded as matrices $D1$, $D2$ and $D3$ through DNA rule β, and then the middle encryption result of DNA formulation matrix $C = \{c_i\}4MH\ i = 1$ is recovered as

$$c_i = d_i - K(i) - d_{i-1} \quad (17)$$

where $i = 1,2,\ldots,MH$. "−" is the DNA subtraction, and $d_0 = c_{4MH}$. The matrices $K1$, $K2$ and $K3$ are generated by doing Step 3 of the DNA sequence operation. Second, the image of DNA sequence matrices $S1$, $S2$ and $S3$ is recovered. The same iteration as Step 3 and Step 4 of pixel position scrambling is performed. Finally, the encrypted image is recovered.

3.4 Simulation result

The color Lena image with the size of 256 × 256 is used for an algorithm simulation test, resulting in the Lena image as shown in Fig. 3a. The key $a = 4$, $b = 0.01$, $\alpha = 36$, $\beta = 20$, $\gamma = 3$, $q = 0.855$, $\rho = 2.67$, $x_0 = 1$, $y_0 = 0$, $z_0 = 1$, $w_0 = 0$, $m = 1000$, $n = 5000$, $c_0 = A$, $\alpha = 1$, $\beta = 3$. The encrypted Lena image can be obtained as in Fig. 3b and the corresponding decryption image as shown in Fig. 3c.

Table 5 Adjacent position with *R*, *G*, *B*

Images	*R*, *G*	*R*, *B*	*G*, *B*
Fig. 5a	0.8570	0.6700	0.8934
Fig. 5b	− 0.0093	0.0072	2.4163e-04
Ref [20]	− 0.0038	0.0018	0.0053

4 Results and discussion

4.1 Key space

As a good image encryption algorithm, it should have large enough key space to resist the brute-force attack. In our encryption scheme, the keys are x_0, y_0, z_0, w_0, a, b, α, β, γ, q, ρ; if the calculation precision is 10^{-15}, the key space will be 2^{548}. For the other part of key c_0, $\alpha 1$, $\beta 1$, b_1, b_2,...b_8, because DNA has four acid base, eight kinds of encoding and decoding rules and six DNA complementary rules, and get the key space $2^2 \times 2^6 \times 2^{20} = 2^{28}$. So, all the key space would be 2^{576}, which shows that the algorithm key space is large enough and can resist the brute-force attack.

4.2 Key sensitivity analysis

The restored image will be completely different from its original image when the key has a tiny change, which means that the encryption algorithm is well and should also be extremely sensitive with its key. In this paper, we respectively used six slightly changed keys, $(x_0 + 10^{-16})$, $(y_0 + 10^{-16})$, $(z_0 + 10^{-16})$, $(a + 10^{-15})$, $(b + 10^{-15})$ and $(c + 10^{-15})$, to decrypt the encrypted Lena image shown in Fig. 3b and the sensitivity test shown in Fig. 4. Obviously, these restored images are completely different from the correct decrypted image in Fig. 3c. Therefore, the proposed algorithm is very sensitive to its key.

4.3 Statistical analysis

4.3.1 Histogram analysis

The distribution of pixel values in the image is shown by the histogram. The histogram of the encrypted image is flat and can well resist statistical attacks. The histograms of original color Lena image and its encrypted image are shown in Fig. 5. It can be seen that the cipher image histogram is very smooth, which indicates that the proposed encryption algorithm is well. So, in this paper, the encryption algorithm is proposed that will not make the attacker by analyzing the ciphertext to get any image with statistical information; thus, it can prevent the attacker from doing a statistical attack.

4.3.2 Correlation coefficient analysis

For the original image, it has extremely strong correlation in adjacent pixels. A good of image encryption algorithm should break the correlation between neighboring pixels. The correlation coefficients r_{xy} of pixels x and y is calculated as:

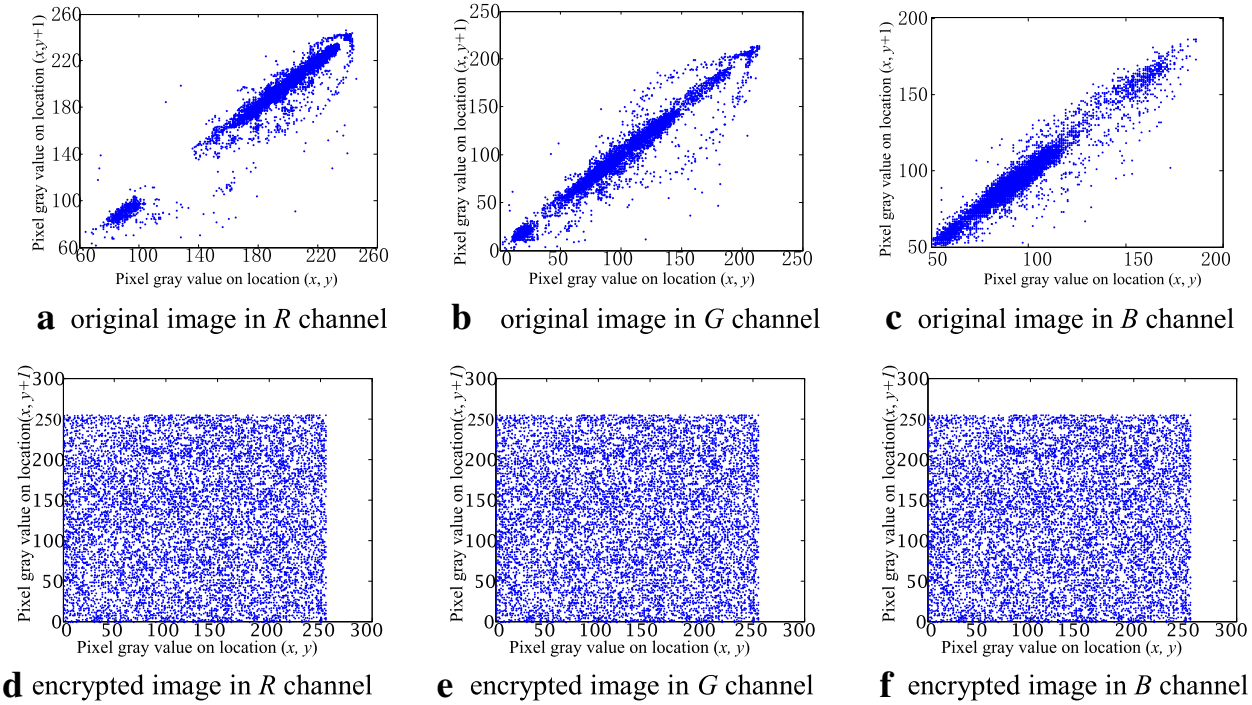


Fig. 6 Correlation distributions between two horizontal different pixels. **a** Original image in *R* channel; **b** original image in *G* channel; **c** original image in *B* channel; **d** encrypted image in *R* channel; **e** encrypted image in *G* channel; **f** encrypted image in *B* channel

Table 6 Information entropy of encryption image

Images	*R*	*G*	*B*	*S*
Lena	7.9991	7.9973	7.9967	7.9974
Ref [20]	7.9967	7.9974	7.9973	7.9970

$$r_{xy} = \frac{\mathrm{cov}(x,y)}{\sqrt{D(x)D(y)}} \tag{18}$$

$$\mathrm{cov}(x,y) = E\{[x - E(x)][y - E(y)]\} \tag{19}$$

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i \tag{20}$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N} [x_i - E(x)]^2 \tag{21}$$

where x and y are the pixel values of different image pixels, cov (x, y) represents the covariance, and $D(x)$ means that the variance of x. Similarly, $E(x)$ is the average, and N represents the number of all pixels. Correlation coefficients of the original Lena image and encrypted image in R, G, and B channels are listed in Table 3. The correlation coefficients of the encrypted image with identical positions in R, G, B components are listed in Table 4. Table 5 lists the correlation coefficients of the encrypted image with adjacent positions in R, G, B components. The tabular data indicate that the original images have significant correlation, whereas encrypted images are very small, which shows the encryption algorithm effect is up to the mustard.

To clearly see the correlation of the original and encrypted images, the correlation distributions of horizontally adjacent pixels for the Lena image are shown in Fig. 6. Obviously, the original image has extremely strong correlation between adjacent pixels as shown in Fig. 6a, b and c. In the figure, we can see that all the pixel dots of the original image are congregated along the diagonal. However, the encrypted image pixel dots are scattered over the entire plane as shown Fig. 6d, e and f. This indicates that the correlations of different pixels in the encrypted image are greatly reduced in the encrypted image. Therefore, the image encryption algorithm has the ability to resist statistical attack.

Table 7 Mean values number of pixels change rates and unified average changing intensities of encryption image

Images	Mean NPCR%			Mean UACI%		
	R	*G*	*B*	*R*	*G*	*B*
Lena	99.6016	99.6205	99.6095	33.2483	33.4977	33.3877
Ref [12]	99.5712	99.6187	99.6922	33.3415	33.3523	33.3581
Ref [19]	99.5926	99.6017	99.5912	33.3386	33.3595	33.1250
Ref [20]	99.6268	66.6025	99.5878	33.3181	33.3107	33.3731

NPCR Number of pixels change rate, *UACI* Unified average changing intensity

4.4 Information entropy

Information entropy is an important gray value for image random, and it is defined as

$$H(m) = \sum_{i=0}^{L-1} p(m_i)\ \log\frac{1}{p(m_i)} \tag{22}$$

where $p(m_i)$ means that the probability of occurrence for symbol m_i, and L represents all the number of symbols m_i. Because there are 2^8 states of the 256 gray-level images, so the theoretical value of information entropy is 8. The information entropy values of encryption image in R, G, B channels, and the combination of R, G, B components S, are listed Table 6. It can be seen clearly from Table 6 that calculation of the values of the new algorithm is close to 8. Therefore, randomness of the encrypted images is good.

4.5 Differential attack

The attacker makes a subtle change in the original image. Then the original image is encrypted and changed by encryption methods, and then attacker can be compared with two encrypted images to find the original image and the encrypted image correlation to attack image information. Therefore, researchers usually use the number of pixels change rate (NPCR) and unified average changing intensity (UACI) to evaluate whether the encryption algorithm can resist differential attack. NPCR and UACI are calculated as follows:

$$\mathrm{NPCR} = \frac{\sum_{i,j} D(i,j)}{L} \times 100\% \tag{23}$$

$$\mathrm{UACI} = \frac{1}{L}\sum_{i,j} \frac{|C(i,j) - C_1(i,j)|}{255} \times 100\% \tag{24}$$

where L is the number of all image pixels. C and C_1 are pixel values before and after the same position change, respectively, and $D(i, j)$ is obtained through the following rules. If $C(i, j) \neq C_1(i, j)$, then $D(i, j) = 1$, if $C(i, j) = C_1(i, j)$, then $D(i, j) = 0$.

In this experimental test, we just change the one random pixel of the original image and carry out the test ten times with one round of encryption to obtain the average values NPCRs and UACIs are listed in Table 7. The results illustrate that the mean values NPCRs and UACIs of the proposed algorithm are over 99.6% and 33.3%, respectively, which means the value is large enough to resist the differential attack.

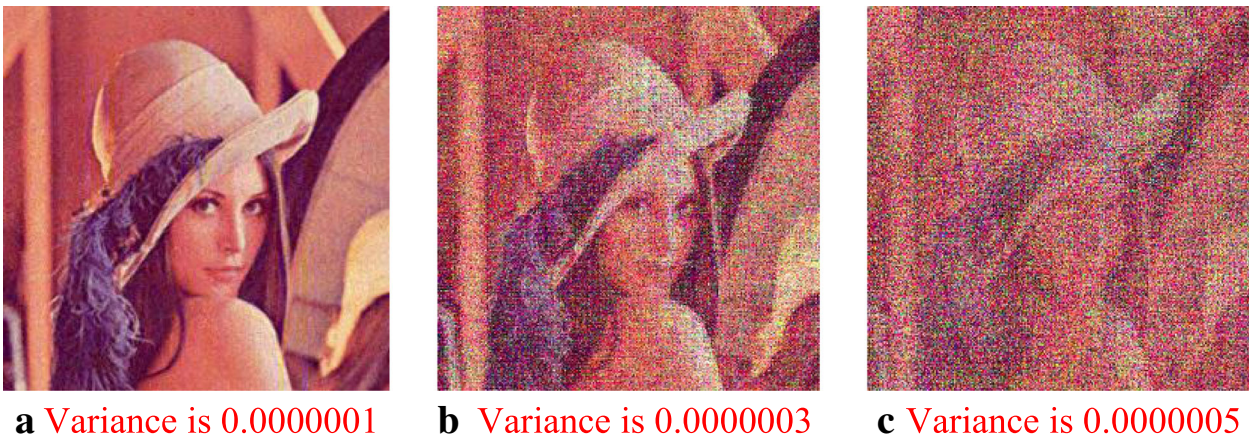


Fig. 7 Noise attack analysis. **a** Variance is 0.0000001; **b** variance is 0.0000003; **c** variance is 0.0000005

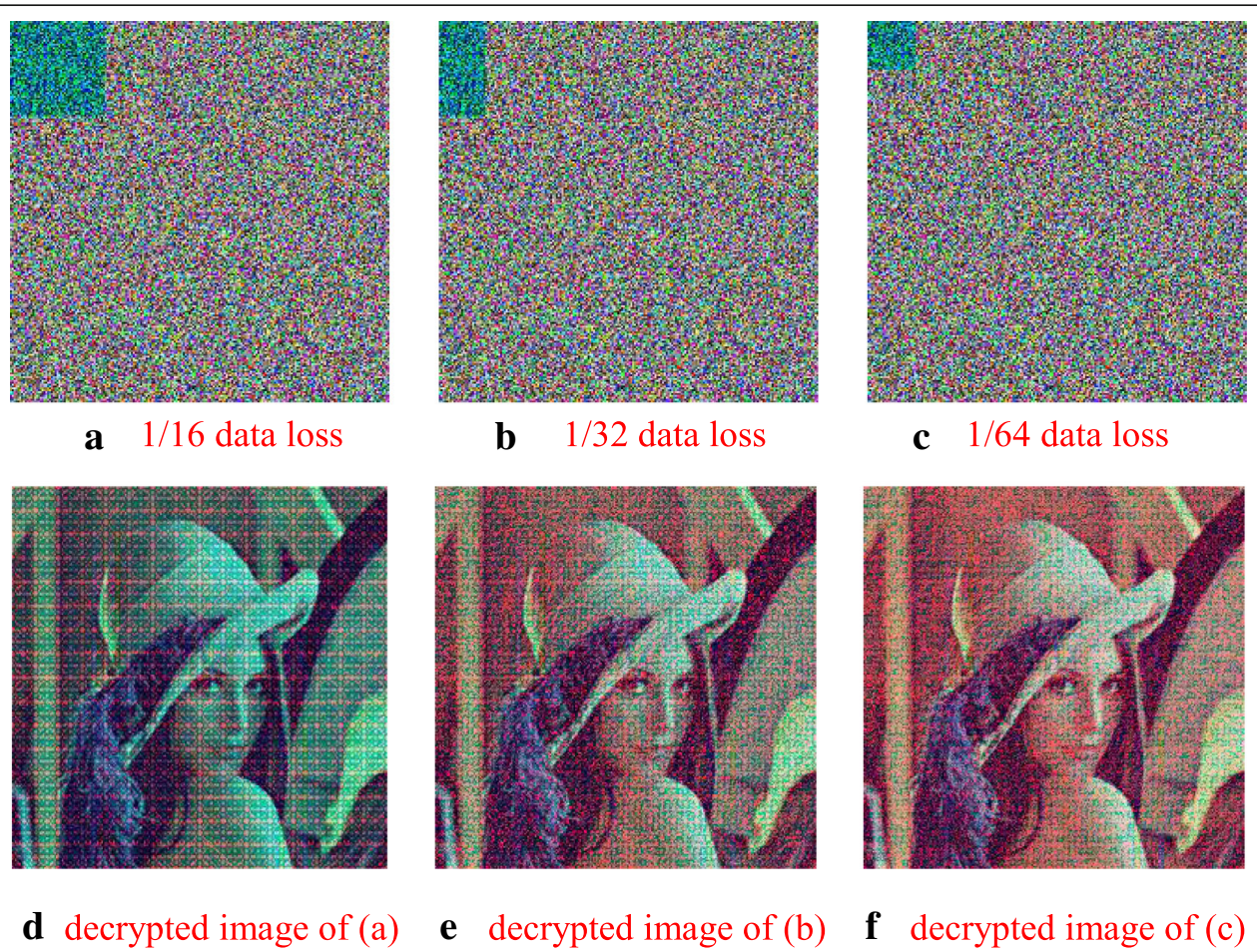


Fig. 8 Cropping attack analysis results. **a** 1/16 data loss; **b** 1/32 data loss; **c** 1/64 data loss; **d** decrypted image of (**a**); **e** decrypted image of (**b**); **f** decrypted image of (**c**)

4.6 Robustness analysis

4.6.1 Noise attack

The encrypted image is disturbed by noise in the transmission process. So we added the Gaussian noise to the encrypted image to carry out antinoise test. Three different variances of Gaussian noise are added to the encrypted Lena image, and corresponding recovery results are shown in Fig. 7a, b and c. Among them, the quality of the decrypted images becomes increasingly worse with the increase of noise variance. However, the main image information can be obtained. This proves that the proposed encryption scheme has strong antinoise capability.

4.6.2 Cropping attack

The cropping attack is an important standard of evaluating the cryptosystem in order to test resistance of cropping attack of the proposed algorithm. The encrypted Lena image with three different data losses is shown in Fig. 8a, b and c, and the decrypted images are shown in Fig. 8d, e and f, respectively. In Fig. 8, we can see that even though the encrypted image is cropped, the main information of the image can be recovered. Moreover, our algorithm could resist cropping attack to a certain degree.

5 Conclusion

In this paper, we focus on studying a color image encryption algorithm through a fractional-order 4D hyperchaotic memristive system and DNA sequence operations. The dynamic analysis results show that the fractional-order 4D hyperchaotic memristive system has more complexity in dynamic characteristics and randomness; moreover, it is more suited for image encryption. Algorithm simulation test and security performance analysis indicate that our algorithm not only can effectively to encrypt image but also has excellent safety features. Therefore, image encryption algorithm based on the fractional-order 4D hyperchaotic memristive system can effectively encrypt images and has more efficiency, which provides the related theoretical basis and practical application foundation applied to cryptography, secure communication and information security and other fields.

Abbreviations

4D: 4-Dimensional; ADM: Adomian decomposition method; AES: Advanced encryption standard; ATCG: Adenine, thymine, cytosine, guanine; DES: Data encryption standard; DNA: Deoxyribonucleic acid; NPCR: Number of pixels change rate; UACI: Unified average changing intensity

Acknowledgements

The authors thank the editor and anonymous reviewers for their helpful comments and valuable suggestions.

Funding

The research presented in this paper was supported by Provincial Natural Science Foundation of Liaoning (Grant No. 20170540060), Basic Scientific Research Projects of Colleges and Universities of Liaoning Province (Grant Nos. 2017 J045 and 2017 J046).

Availability of data and materials

Please contact author for data requests.

Authors' contributions

PL made a theoretical guidance for this paper. JX designed and performed experiments. JM wrote this manuscript. FY analyzed data. All authors carefully read and approved the final manuscript.

Competing interests

The authors declare that they have no competing interests.

Publisher's Note

Received: 22 October 2018 Accepted: 21 December 2018
Published online: 28 January 2019

References

1. K.C. Liu, Prediction error preprocessing for perceptual color image compression. EURASIP J. Image Video Process. **2012**(1), 3 (2012)
2. T. Huynh-The, B.V. Le, S. Lee, et al., Using weighted dynamic range for histogram equalization to improve the image contrast. EURASIP J. Image Video Process. **2014**(1), 44 (2014)
3. Y. Wang, H. Bai, L. Zhao, et al., Cascaded reconstruction network for compressive image sensing. EURASIP J. Image Video Process. **2018**, 77 (2018)
4. J. Liu, K. Liu, S. Liu, Adaptive control for a class of nonlinear complex dynamical systems with uncertain complex parameters and perturbations. PLoS One **12**(5), e0175730 (2017)
5. J. Liu, S. Liu, C. Yuan, Adaptive complex modified projective synchronization of complex chaotic (hyperchaotic) systems with uncertain complex parameters. Nonlinear Dyn. **79**(2), 1035–1047 (2015)
6. C. Li, J.C. Sprott, H. Xing, Constructing chaotic systems with conditional symmetry. Nonlinear Dyn. **87**, 1351–1358 (2017)
7. C. Li, J.C. Sprott, Y. Mei, An infinite 2-D lattice of strange attractors. Nonlinear Dyn. **89**(4), 2629–2639 (2017)
8. Z. Hua, Y. Zhou, Image encryption using 2D logistic-adjusted-sine map. Inf. Sci. **339**, 237–253 (2016)
9. Y.G. Yang, J. Tian, H. Lei, et al., Novel quantum image encryption using one-dimensional quantum cellular automata. Inf. Sci. **345**, 257–270 (2016)
10. H. Natiq, N.M.G. Al-Saidi, M.R.M. Said, et al., A new hyperchaotic map and its application for image encryption. Eur. Phys. J. Plus **133**(1), 6 (2018)
11. Y. Luo, R. Zhou, J. Liu, et al., A parallel image encryption algorithm based on the piecewise linear chaotic map and hyper-chaotic map. Nonlinear Dyn. **93**(3), 1165–1181 (2018)
12. X.J. Tong, M. Zhang, Z. Wang, et al., An image encryption scheme based on a new hyperchaotic finance system. Optik **126**(20), 2445–2452 (2015)
13. W. Liu, K. Sun, C. Zhu, A fast image encryption algorithm based on chaotic map. Opt. Lasers Eng. **84**, 26–36 (2016)
14. Q. Zhang, L. Guo, X. Wei, Image encryption using DNA addition combining with chaotic maps. Math. Comput. Modell. **52**(11–12), 2028–2035 (2010)
15. A. Girdhar, V. Kumar, A RGB image encryption technique using Lorenz and Rossler chaotic system on DNA sequences. Multimed. Tools Appl. **77**(20), 27017–27039 (2018)
16. X. Fu, B. Liu, Y.Y. Xie, et al., Image encryption-then-transmission using DNA encryption algorithm and the double chaos. IEEE Photonics J. **10**(3), 3900515 (2018)
17. Y. Zhang, The image encryption algorithm based on chaos and DNA computing. Multimed. Tools Appl. **77**(16), 21589–21615 (2018)
18. X. Li, C. Zhou, N. Xu, A secure and efficient image encryption algorithm based on DNA coding and spatiotemporal chaos. Int. J. Netw. Secur. **20**(1), 110–120 (2018)
19. R. Guesmi, M.A.B. Farah, A. Kachouri, et al., A novel chaos-based image encryption using DNA sequence operation and secure hash algorithm SHA-2. Nonlinear Dyn. **83**(3), 1123–1136 (2016)
20. L.M. Zhang, K.H. Sun, W.H. Liu, et al., A novel color image encryption scheme using fractional-order hyperchaotic system and DNA sequence operations. Chin. Phys. B **26**(10), 98–106 (2017)

21. X. Chai, Z. Gan, Y. Lu, et al., A novel image encryption algorithm based on the chaotic system and DNA computing. Int. J. Mod. Phys. C **28**(5), 1750069 (2017)
22. X. Wu, K. Wang, X. Wang, et al., Lossless chaotic color image cryptosystem based on DNA encryption and entropy. Nonlinear Dyn. **90**(2), 855–875 (2017)
23. T. Hu, Y. Liu, L.H. Gong, et al., An image encryption scheme combining chaos with cycle operation for DNA sequences. Nonlinear Dyn. **87**(1), 51–66 (2016)
24. W. Liu, K. Sun, Y. He, et al., Color image encryption using three-dimensional sine ICMIC modulation map and DNA sequence operations. Int. J. Bifurcation Chaos **27**(11), 1750171 (2017)
25. Q. Zhang, X.L. Xue, X.P. Wei, A novel image encryption algorithm based on DNA subsequence operation. Sci. World J. **2012**, 286741 (2012)
26. H.J. Liu, X.Y. Wang, A. Kadir, Image encryption using DNA complementary rule and chaotic maps. Appl. Soft Comput. **12**(5), 1457–1466 (2012)
27. M. SaberiKamarposhti, I. AlBedawi, D. Mohamad, A new hybrid method for image encryption using DNA sequence and chaotic logistic map. Aust. J. Basic Appl. Sci. **6**(3), 371–380 (2012)
28. E.S.A. Shahri, A. Alfi, J.A.T. Machado, Stability analysis of a class of nonlinear fractional-order systems under control input saturation. Int. J. Robust Nonlinear Control **28**(3), 2887–2905 (2018)
29. X. Ye, J. Mou, C. Luo, et al., Dynamics analysis of Wien-bridge hyperchaotic memristive circuit system. Nonlinear Dyn. **92**(3), 923–933 (2018)
30. J. Mou, K. Sun, H. Wang, et al., Characteristic analysis of fractional-order 4D hyperchaotic memristive circuit. Math. Probl. Eng. **2017**, 2313768 (2017)
31. S. Momani, K. Al-Khaled, Numerical solutions for systems of fractional differential equations by the decomposition method. Appl. Math. Comput. **162**(3), 1351–1365 (2005)
32. V. Daftardar-Gejji, H. Jafari, Adomian decomposition: a tool for solving a system of fractional differential equations. J. Math. Anal. Appl. **301**(2), 508–518 (2005)
33. N.T. Shawagfeh, Analytical approximate solutions for nonlinear fractional differential equations. Appl. Math. Comput. **131**(2–3), 517–529 (2002)
34. R. Gorenflo, F. Mainardi, *Fractal and fractional calculus in continuum mechanics* (Springer-Verlag, New York, 1997)
35. A.N. Demaria, A structure for deoxyribose nucleic acid. J. Am. Coll. Cardiol. **42**(2), 373–374 (2003)