The Visual Computer (2022) 38:1509–1526
https://doi.org/10.1007/s00371-021-02085-7

ORIGINAL ARTICLE

The image compression–encryption algorithm based on the compression sensing and fractional-order chaotic system

Ji Xu[1] · Jun Mou[1] · Jian Liu[1] · Jin Hao[1]

Accepted: 5 February 2021 / Published online: 20 March 2021

Abstract

In this paper, a novel image encryption algorithm based on the fractional-order chaotic system and compression sensing algorithm is proposed. Firstly, the dynamical characteristics of the fractional-order chaotic system are analyzed. The hardware circuit is designed in and realized on the DSP. Secondly, the block feedback diffusion algorithm is applied to this encryption scheme. The elements of the cipher block are decided by the front of the cipher block and the plain-text block. In this algorithm, it needs to be emphasized that the scrambling calculation and the diffusion operation are carried out simultaneously. The simulation results show that the algorithm can effectively encrypt digital images. Finally, the security analysis demonstrates the security and the effectiveness of the proposed encryption algorithm.

Keywords Image encryption · Compression sensing · Fractional-order chaotic system

1 Introduction

Because of the wide application of the streaming media, many multimedia data are delivered in the two different terminals. Those multimedia data include the image, video, and audio. Especially, the image data is an important data format in militarily, medical, and industrial areas. For example, a personal picture can illustrate the secret information of this person like health condition and personal habit [18,46]. Therefore, the image files have the risk of unauthorized access. The protection scheme of the image files has become a serious problem. The image files are different with the text message. It is a typical two-dimensional data. Therefore, the data capacity of image is huge and the spatial distribution is complex. It is a disputed question that the encryption standard of text message is whether suitable to protect image data [5,6,18]. Besides, the image files without compression operation can occupy a huge resource of communication channels. These situations make the encryption algorithm needs to improve the security level of multimedia data transmission.

The chaotic systems have the properties of unpredictability, ergodicity, and sensitivity to their parameters. Therefore, chaotic systems have been widely used in different applications. In the security application area, most research objects are adopted different kinds of chaotic systems. These encryption schemes have wonderful security performance with a low calculation complexity [1,4,18,23,26,27,45]. Moreover, the DNA encode theory is applied to the chaotic-based encryption scheme [2,22,24,39,43]. The fractional-order chaotic system has more complex dynamical characteristics compared with the integer-order chaotic system [11,16,17,25,31,32]. In the encryption algorithm, the order of the system can expend the key space of the algorithm. Also, the chaotic sequences of fractional-order chaotic system are random and the high-randomness sequence can cover the plain-text information more effectively. The related research can prove the fractional-order chaotic system has flexible and good characteristics in the encryption algorithm [21,22,34–36,43].

The other problem is the size of the multimedia files. Firstly, the number of multimedia files in real-time transmitting is large. Secondly, it has to strictly comply with the law of sampling for the uncompressed multimedia data. Therefore, the resource of the signal channel is short and the transmitting cost is huge. The compression sensing technology is a

The Natural Science Foundation of Liaoning Province (2020-MS-274) and the National Nature Science Foundation of China (No. 61773010).

✉ Jun Mou
moujun@csu.edu.cn

[1] School of Information Science and Engineering, Dalian Polytechnic University, Dalian 116000, China

new approach in the signal sampling theory. This scheme can generate the measured result by the measurement matrix. The size of the result is less than the original signal. It can save the storage space in the signal channel and reduce the transmitting cost. Moreover, the chaotic system is applied to build the measured matrix in the compressive sensing algorithm. This method can improve the security of transmission and compress the image file at the same time [7,13,30,38,40].

Based on the advantages of compression sensing, an image encryption algorithm based on the fractional-order chaotic system and compression sensing is proposed. The encryption algorithm is a combination of compression and encryption, the discrete chaotic system is applied to compress the image. The encryption scheme depends on the fractional-order chaotic system. The sequences of the fractional-order chaotic system are obtained by the CADM algorithm [15,20,25]. The contributions of this algorithm are listed as follows

1. Two different and independent chaotic systems are applied into the flow of compression and encryption. The final cipher image cannot be decoded without the complete initial condition.
2. The scrambling operation and diffusion calculation are carried out simultaneously. The purpose of this structure is to cover the statistical information of the plain-text image and change the arrangement of the pixel at the one round operation.
3. The secret key has two parts: the public key and the private key. The compression rate (CR) is public in the processing of transmission. The parameters of the chaotic system are the private key in this algorithm.
4. The new critical scores of the difference attack analyses are adopted in the security analyses [3,10,14,42,44].

The rest parts of this paper are structured as follows. The basic theory of compression sensing and the dynamical characteristics analyses of a fractional-order chaotic system are carried out in Sect. 2. The detail of the encryption algorithm and decryption workflow is described in Sect. 3. The encryption and decryption image is shown in Sect. 4. The results of performance analyses are given in Sect. 4 too. The important conclusion is given in Sect. 5.

2 Preliminaries

2.1 The basic theory of compression sensing

The basic structure of the compression sensing includes the three parts: the measurement matrix, the method of sparse signal, and the reconstruction algorithm. The complete flow of compression sensing can be presented as

$$y = \phi \cdot x = \phi \cdot \psi \cdot x, \tag{1}$$

where x represents the original signal. The matrix ψ is the orthogonal transform matrix. This matrix is applied to the sparse the original signal matrix. Therefore, this matrix can be called the sparse base matrix. The common sparse method includes the discrete cosine transform (DCT) algorithm and the discrete wavelet transform (DWT) algorithm. The matrix ϕ is called the measurement matrix. The size of the measurement matrix is $M \times N$ and M is less than the pixel amount N in the row or column.

The reconstruction algorithm can present the solution of the optimization l_0 problem. This problem can be denoted as

$$\begin{cases} \hat{x} = argmin\|S\|_0; \\ y = \hat{\Theta}x; \end{cases} \tag{2}$$

where $\Theta = \phi \cdot \psi$. The common reconstruction algorithms are orthogonal matching pursuit (OMP) algorithm, subspace pursuit (SP) algorithm and smoothed ℓ_0 norm (SL0) algorithm. The smoothed ℓ_0 (SL0) algorithm is applied in this encryption algorithm. The sparsest solutions are obtained by an under determined system of linear equations $As = x$. Moreover, this algorithm tries to directly minimize the ℓ_0 norm [28,29].

In this encryption algorithm, the sparse method is adopted the DWT scheme. The measurement matrix is constructed by the discrete chaotic system. To reduce the relevance among the column vectors, the first element of column vector is set $\Phi(\hat{i}, 1) = \lambda \cdot \Phi(i-1, 1)$. The final measurement matrix is generated by

$$\begin{cases} \hat{\Phi}(i, 1) = \lambda \cdot \Phi(i-1, 1) \\ \hat{\Phi}(i, 2:end) = \lambda \cdot \Phi(i-1, 1:end-1) \end{cases}. \tag{3}$$

2.2 The dynamical characteristics of fractional-order chaotic system

The design concept of random-number generator in this encryption algorithm is based on the fractional-order Jerk chaotic system. The chaotic sequences are obtained by the CADM algorithm. Firstly, the integer-order Jerk chaotic system is present in Eq. (4)

$$\begin{cases} \dot{x}_1 = x_2 \\ \dot{x}_2 = ax_3 \\ \dot{x}_3 = -bx_1 \cdot cx_3 - d(e^{kx_2} - e^{-x_2}) \end{cases}. \tag{4}$$

Based on the Caputo definition [15], the fractional-order system can be rewritten as

$$\begin{cases} D_t^q x_1 = x_2 \\ D_t^q x_2 = a x_3 \\ D_t^q x_3 = -b x_1 \cdot c x_3 - d(e^{k x_2} - e^{-x_2}) \end{cases}. \tag{5}$$

At the first, Eq. (5) needs to be divided into the two blocks: the linear terms and the nonlinear terms

$$\begin{bmatrix} Lx_1 \\ Lx_2 \\ Lx_3 \end{bmatrix} = \begin{bmatrix} x_2 \\ a x_3 \\ -b x_1 - c x_3 \end{bmatrix}, \begin{bmatrix} Nx_1 \\ Nx_2 \\ Nx_3 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ -d(e^{k x_2} - e^{-x_2}) \end{bmatrix}. \tag{6}$$

According to the calculation flow of CADM, the first five Adomian polynomials of the nonlinear term are calculated as follows:

$$\begin{aligned} A_3^0 &= e^{k x_2^0} - e^{-x_2^0} \\ A_3^1 &= k x_2^1 e^{k x_2^0} + x_2^1 e^{-x_2^0} \\ A_3^2 &= [k x_2^2 + \tfrac{1}{2} k^2 (x_2^1)^2] e^{k x_2^0} - [-x_2^2 + \tfrac{1}{2}(x_2^1)^2] e^{-x_2^0} \\ A_3^3 &= [k x_2^3 + k^2 x_2^1 x_2^2 + \tfrac{1}{6} k^3 (x_2^1)^3] e^{k x_2^0} - [-x_2^3 + x_2^1 x_2^2 - \tfrac{1}{6}(x_2^1)^3] \\ A_3^3 &= A_3^3 \cdot e^{-x_2^0} - [-x_2^3 + x_2^1 x_2^2 - \tfrac{1}{6}(x_2^1)^3] e^{-x_2^0} \\ A_3^4 &= [k x_2^4 + k^2 (x_2^3 x_2^1 + \tfrac{1}{2}(x_2^2)^2) + \tfrac{1}{2} k^3 (x_2^1)^2 x_2^2 + \tfrac{1}{24} k^4 (x_2^1)^4] \\ A_3^4 &= e^{k x_2^0} A_3^4 - [-x_2^4 + (x_2^3 x_2^1 + \tfrac{1}{2}(x_2^2)^2) - \tfrac{1}{2}(x_2^1)^2 x_2^2 \\ &\quad + \tfrac{1}{24}(x_2^1)^4] e^{-x_2^0} \end{aligned}. \tag{7}$$

The initial conditions x_0 is equal to $[x_1(t_0^+)\ x_2(t_0^+)\ x_3(t_0^+)]$. Therefore, the first item is:

$$\begin{cases} x_1^0 = x_1(t_0^+) \\ x_2^0 = x_2(t_0^+) \\ x_3^0 = x_3(t_0^+) \end{cases}. \tag{8}$$

Letting $x^0 = c^0 = [c_1^0 c_2^0 c_3^0]$. The second term is:

$$\begin{cases} x_1^1 = c_2^0 \frac{h^q}{q} \\ x_2^1 = a c_3^0 \frac{h^q}{q} \\ x_3^1 = (-b c_1^0 - c c_3^0 - d(e^{k c_2^0} - e^{-c_2^0})) \frac{h^q}{q} \end{cases}, \tag{9}$$

where the step size $h = t - t_0$. Setting

$$\begin{cases} c_1^1 = c_2^0 \\ c_2^1 = a c_3^0 \\ c_3^1 = -b c_1^0 - c c_3^0 - d(e^{k c_2^0} - e^{-c_2^0}) \end{cases}, \tag{10}$$

then x^1 will be represented as $x_i^1 = \frac{c^1 h^q}{q}$ $(i = 1, 2, 3)$. Similarly, the other four coefficients of the rest terms are:

$$\begin{cases} c_1^2 = c_2^1 \\ c_2^2 = a c_3^1 \\ c_3^2 = -b c_1^1 - c c_3^1 - d(k c_2^1 e^{k c_2^0} + c_2^1 e^{-c_2^0}) \end{cases}, \tag{11}$$

$$\begin{cases} c_1^3 = c_2^2 \\ c_2^3 = a c_3^2 \\ c_3^3 = -b c_1^2 - c c_3^2 - d((k c_2^2 + (k c_2^1)^2) e^{k c_2^0} \\ \quad + (c_2^2 - (c_2^1)^2) e^{-c_2^0}) \end{cases}, \tag{12}$$

$$\begin{cases} c_1^4 = c_2^3 \\ c_2^4 = a c_3^3 \\ c_3^4 = -b c_1^3 - c c_3^3 - d((k c_2^3 + 3k^2 c_2^1 c_2^2 + k^3 (c_2^1)^3) e^{k c_2^0} \\ \quad + (c_2^3 - 3k^2 c_2^1 c_2^2 + k^3 (c_2^1)^3) e^{-c_2^0}) \end{cases}, \tag{13}$$

$$\begin{aligned} c_1^5 &= c_2^4 \\ c_2^5 &= a c_3^4 \\ c_3^5 &= -b c_1^4 - c c_3^4 - d((k c_2^4 + k^2 (4 c_2^3 c_2^1 + 3(c_2^2)^2) \\ &\quad + 6k^3 (c_2^1)^2 c_2^2 + k^4 (c_2^1)^4) e^{k c_2^0} - (-c_2^4 + 4 c_2^3 c_2^1 + 3(c_2^2)^2 \\ &\quad - 6(c_2^1)^2 c_2^2 + (c_2^1)^4) e^{-c_2^0}) \end{aligned}. \tag{14}$$

So, the numerical solution of the FONJCS with six terms is

$$\begin{aligned} \tilde{x}_j &= c_j^0 + c_j^1 \frac{h^q}{q} + c_j^2 \frac{h^{2q}}{2q^2} + c_j^3 \frac{h^{3q}}{6q^3} \\ &\quad + c_j^4 \frac{h^{4q}}{24q^4} + c_j^5 \frac{h^{5q}}{120q^5}. \end{aligned} \tag{15}$$

The system initial conditions are [1.9,0,0]; the system parameters are $[a\ c\ d\ k\ q] = [1, 0.5, 2.72165 * 10^{-4}, 1, 0.9]$. The phase diagrams are shown in Fig. 1. Set the system parameters as $a = 1$, $c = 0.5$, $k = 1$, $q = 0.9$. The variable $b \in [0.85, 2.85]$. The Lyapunov exponent spectrum and the bifurcation diagram are shown in Fig. 2. This system suddenly transforms into two coexisting attractors when the parameter $b = 0.965$. Therefore, the curves of the max Lyapunov exponent and bifurcation diagram show the properties of two coexisting attractors. The widely chaotic range can be illustrated by Fig. 2a. Figure 2b can prove that this system has widely chaotic range from the max Lyapunov direction.

The DSP development board is selected as hardware platform to implement the fractional-order system in this paper. The parameters of six different type attractors are listed in Table 1. The experiment suit and the application environment are shown in Fig. 3. The simulation results are shown in Fig. 4.

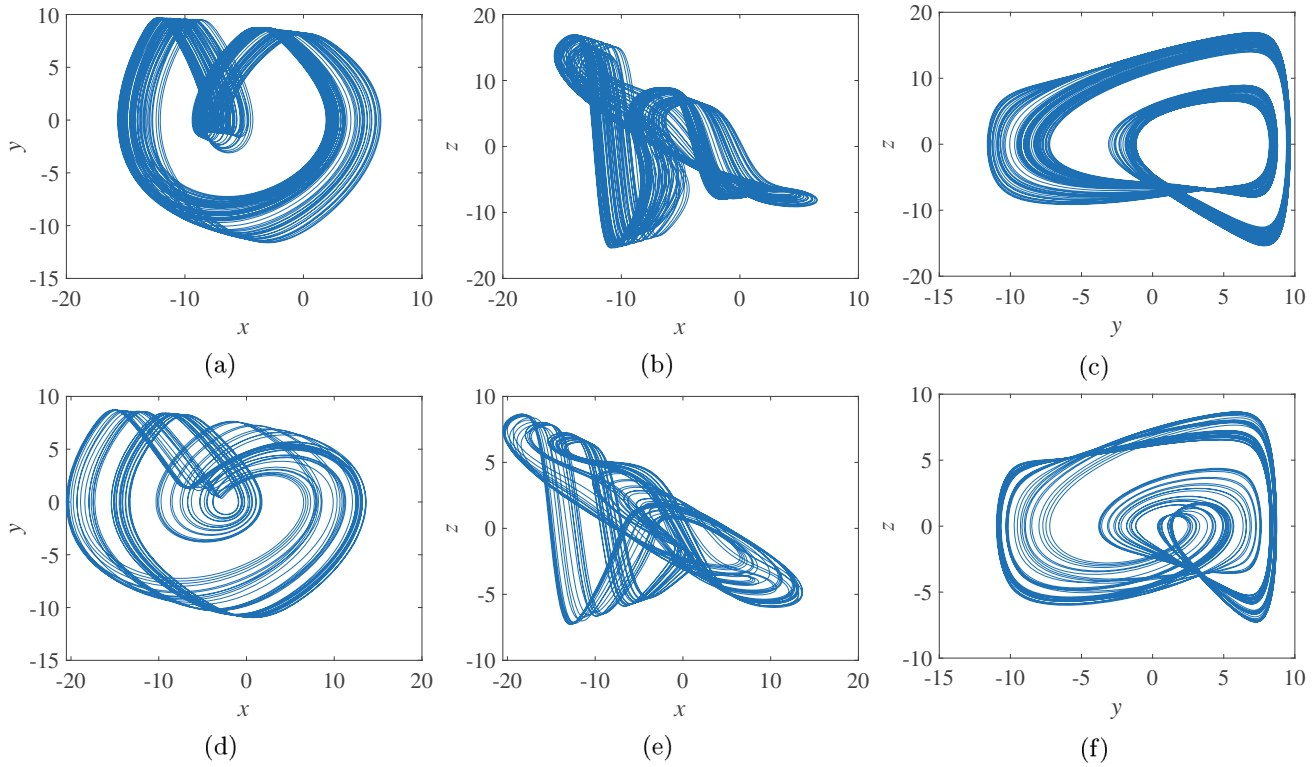


Fig. 1 The phase diagram: **a** $x - y$ ($b = 0.3$), **b** $x - z$ ($b = 0.3$), **c** $y - z$ ($b = 0.3$), **d** $x - y$ ($b = 1$), **e** $x - z$ ($b = 1$), and **f** $y - z$ ($b = 1$)

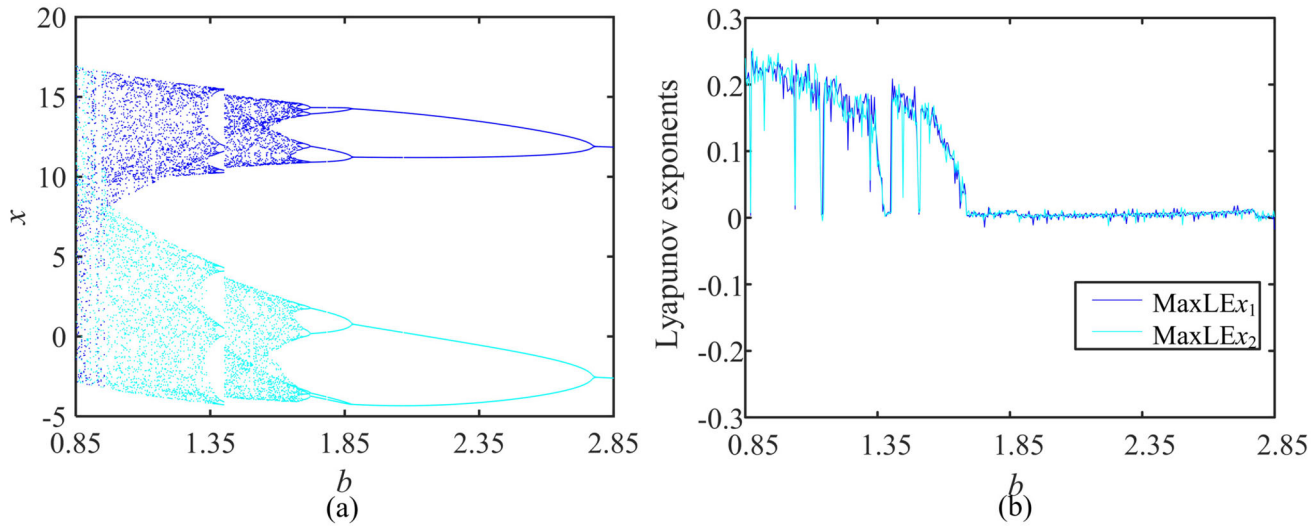


Fig. 2 The dynamical characteristics of the FONJCS. **a** Coexisting bifurcation diagram and **b** coexisting maximum Lyapunov exponent spectrum

2.3 The dynamical characteristics of the discrete chaotic system

The measurement matrix is obtained by the discrete chaotic system. Firstly, the size of the measurement matrix needs to control in a certain size. This measure can save the resource of the signal channel. The discrete chaotic system has low calculation cost and complex dynamical behaviors. It can satisfy this request. Moreover, the sequences of the discrete chaotic system have uniform distribution and zero correlation. Therefore, the discrete chaotic system has good promising applications in the encryption algorithm [4,9,44].

Table 1 Attractor's type

Attractor type	$[b, k, q]$
Type VIII	[1.01, 1.41, 0.9]
Type IX	[1.01, 1.51, 0.9]
Type X	[1.01, 1.51, 0.9]
Type XI	[1.44, 2.31, 0.9]
Type XII	[3.01, 2.62, 0.9]
Type V	[1.6, 1.19, 0.691]

The 3D-SIMM system is a high-dimension (HD) discrete chaotic system. The mathematical model is

$$\begin{cases} x_{i+1} = a_1 \cdot \sin(b_1 z_i) \cdot \sin(\frac{c_1}{x_i}) \\ y_{i+1} = a_1 \cdot \sin(b_1 x_{i+1}) \cdot \sin(\frac{c_1}{y_i}) \\ z_{i+1} = a_1 \cdot \sin(b_1 y_{i+1}) \cdot \sin(\frac{c_1}{z_i}) \end{cases} . \tag{16}$$

The phase diagram is shown in Fig. 5a. When the system parameters $[a, b, c]$=[1,2π,11.5], this system is in chaotic state. The 3D-SIMM has a wide hyper-chaotic range when variable $a \in [0.33, 5]$. The Lyapunov spectrum and bifurcation diagram are shown in Fig. 5b, c. It is obvious that this

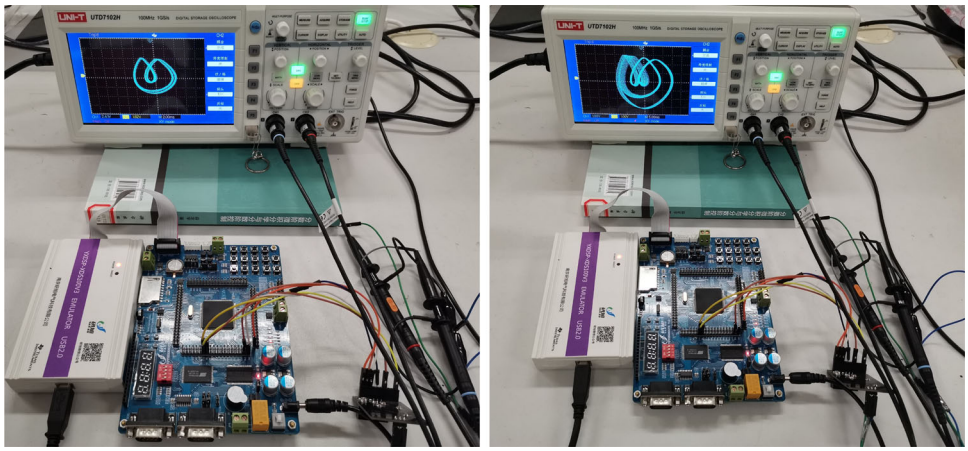


Fig. 3 DSP experimental platform

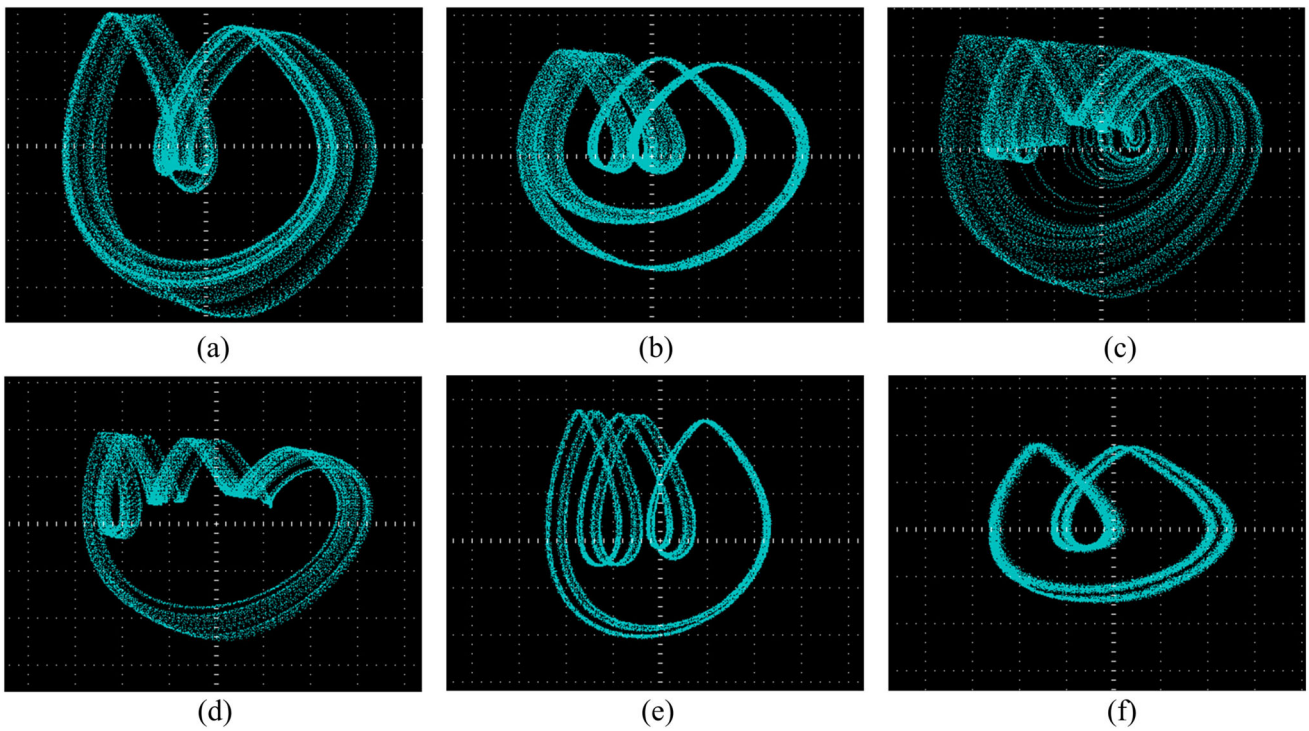


Fig. 4 Simulation results on the oscilloscope with different parameters $[b, k, q]$: **a** [1.01, 1, 41, 0.9], **b** [1.01, 1.51, 0.9], **c** [1.01, 1.51, 0.9], **d** [1.44, 2.31, 0.9], **e** [3.01, 2.62, 0.9], and **f** [1.6, 1.19, 0.691]

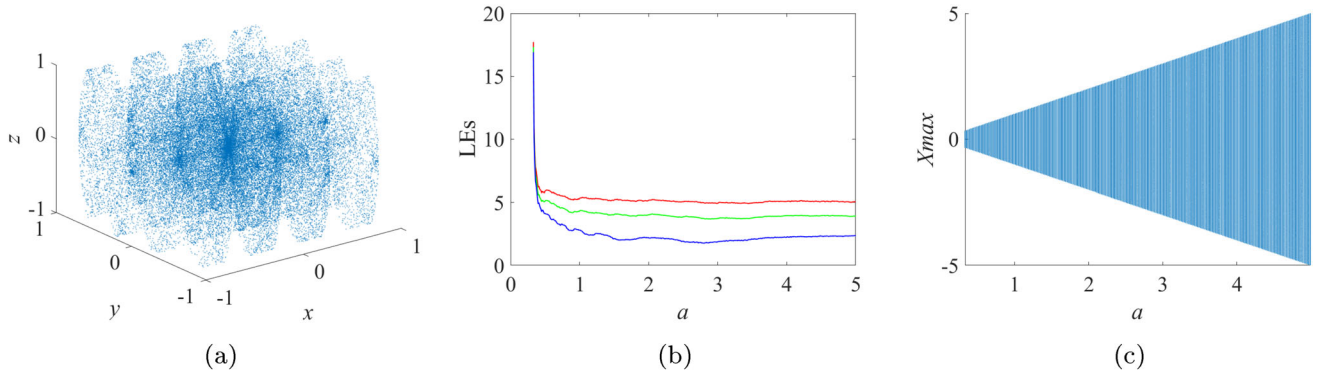


Fig. 5 The dynamical behaviors of 3D-SIMM: **a** The phase diagram, **b** the Lyapunov spectrum, and **c** the bifurcation diagram

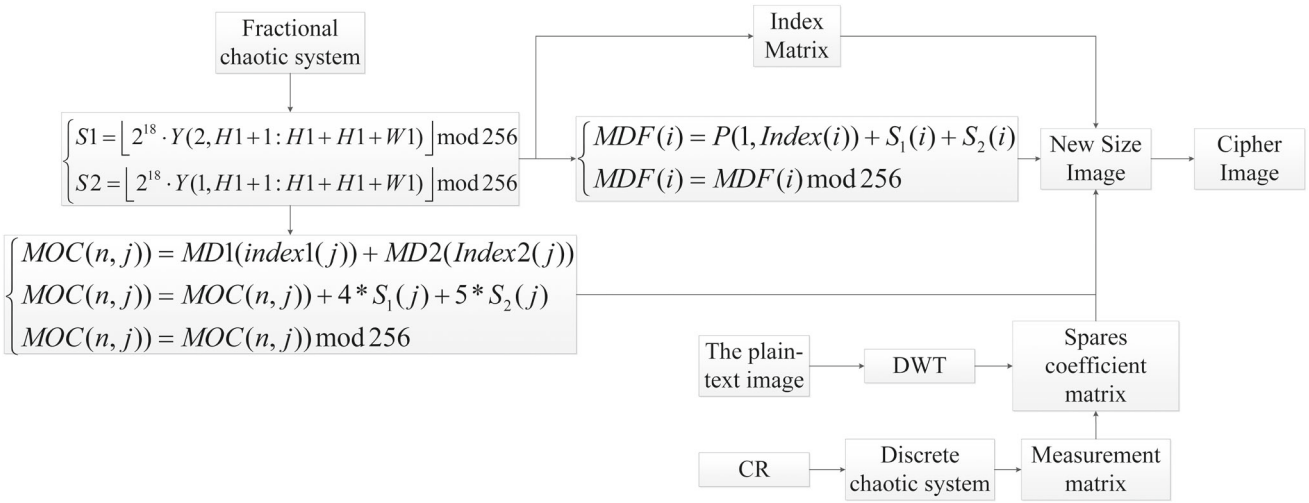


Fig. 6 The flow of encryption

system has complex dynamical characteristics and a wide chaotic range [23]. Firstly, the hyper-chaotic state can maintain in the whole parameter range. This property is illustrated by Fig. 5c. Secondly, Fig. 5b can prove that this assumption is correct from other side. Therefore, the sequences of this system are applied to construct the measurement matrix.

3 The description of encryption algorithm

The discussion point of this section is the concrete steps of the encryption algorithm. The flow is shown in Fig. 6.

The order of encryption is subject to the compression–encryption. In the encryption operation, the scrambling operation and the diffusion calculation are going at the same time. Besides, the encryption algorithm is based on the block cipher theory. Therefore, the length of the secret sequence is certain. It can reduce the time cost in chaotic sequences calculation. Moreover, the elements of the cipher block are dependent on the front of the cipher block, the plain-text block, and the chaotic sequences.

3.1 The flow of encryption algorithm

1. Sparse the image matrix. The sparse signal matrix is come from the plain-text image by DWT algorithm. The size of sparse signal matrix is equal to $H \times W$, where H presents the number of rows, W is the number of columns.
2. Set the compression rate (CR). The measurement matrix is generated by the discrete chaotic system. The size of the measurement matrix is subject to the number of CR. The final measurement matrix is obtained by Eq. (3). This equation is used to reduce the relevance among the column vectors.
3. Compress the image matrix. The size of the new image matrix is equal to $M \times W$, where the number of M is equal to $CR \times H$. The elements of the new image matrix need to uniformization. The method of uniformization is

$$\begin{cases} Max = max(max(P) \\ Min = min(min(P)) \\ Q = round(255 * (P - Min)/(Max - Min)) \end{cases} \tag{17}$$

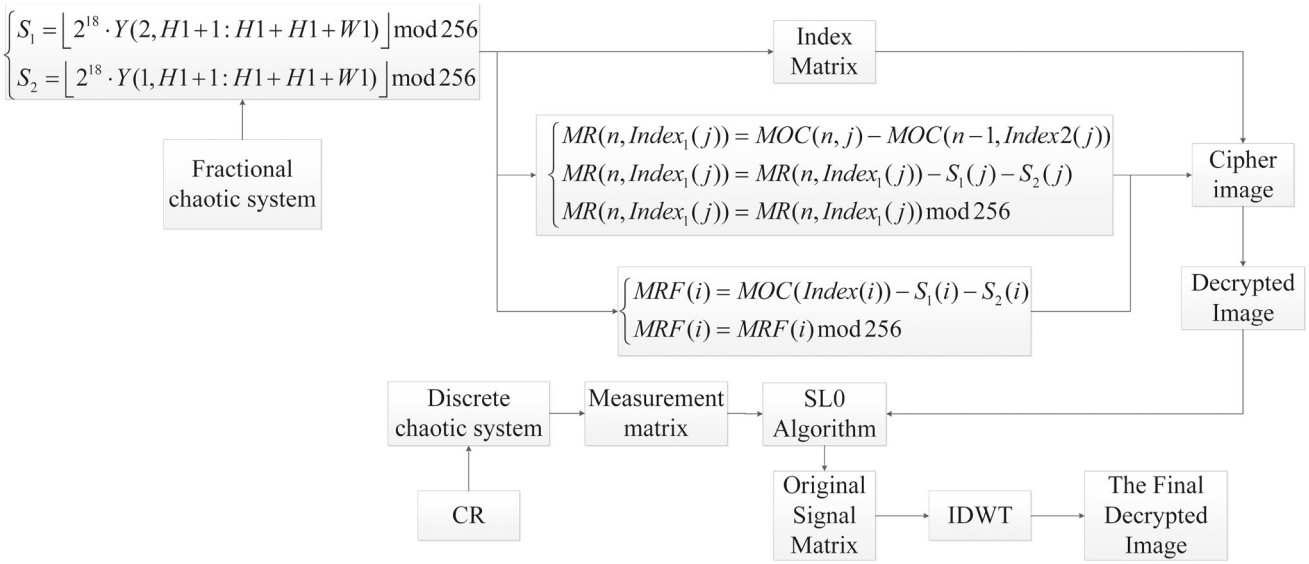


Fig. 7 The flow of decryption algorithm

where P is the new image matrix, Q is the compressed image.

4. The secret sequence is generated by the fractional-order Jerk chaotic system. The length of sequence is equal to the row vectors. The secret sequence is obtained by

$$S = \lfloor (pow2(16) * Y) \rfloor \bmod L, \tag{18}$$

where the L is present for the max gray level in the image matrix. Y is a chaotic sequence obtained by the fractional-order Jerk chaotic system. Besides, the scrambling matrix is generated by a sort chaotic sequence.

5. The size of cipher image is equal to $H1 \times W1$. The encryption operation contains two directions: the blockchain diffusion and the elements scrambling in the group. These directions can be presented by one equation group as follows

$$\begin{cases} MDF(i) = P(Index1(i)) + S1(i) + S2(i) \\ MDF(i) = MDF(i) \bmod L \\ Cipherimage(n, :) = MDF \qquad n = 1 \end{cases}. \tag{19}$$

The front matrix of diffusion (MDF) is start block in the chain diffusion. The secret sequences $S1$ and $S2$ respond to the change value of the pixel. The Index1 is generated by sorting the chaotic sequence. This sequence is applied to disorder the arrangement of pixel in group. The final results of MDF are embed into the first row of cipher image.

$$\begin{cases} MD(i) = MD1(Index1(i)) + MD2(Index2(i)) \\ MD(i) = MD(i) + 4 * S1(i) + 5 * S2(i) \\ MD(i) = MD(i) \bmod L \\ Cipherimage(n, :) = MD \qquad n \in [2, \cdots, H1] \end{cases}. \tag{20}$$

The matrix of diffusion (MD) is a basic unit in the encryption operation. The size of MD is equal to the column vector of plain-text image. The plain-text sequences P are named as MD1. The front cipher blocks C are named as MD2. Therefore, the value of the cipher group depends on the plain-text block, the secret sequence, and the front block of cipher image. The pixel of plain-text and the front cipher sequence are selected randomly. The select principle is subject to the Index matrix.

3.2 The flow of decryption algorithm

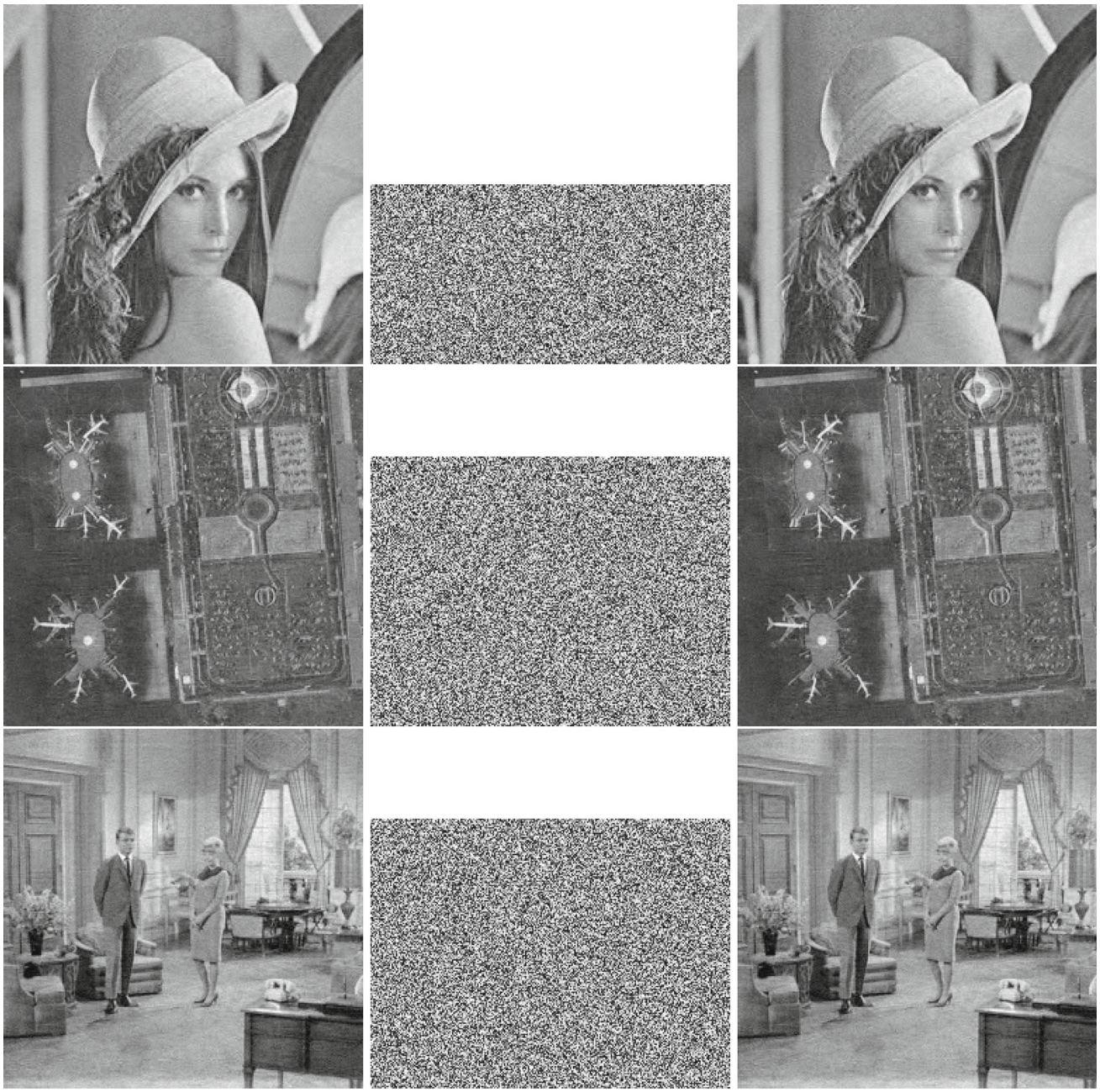
The decryption algorithm is inverse flow compare with the encryption algorithm. The flow is shown in Fig. 7.

Firstly, the value and order of the cipher matrix are recovered by the block diffusion and the elements scrambling. The recovered matrix is regrouped by the divide algorithm. The reconstructed image is obtained by the smoothed ℓ_0 algorithm and the inverse DWT transform.

1. Recover the value of pixel. The principle of recovery is subject to Eqs. (21–22).

Table 2 The parameters of encryption algorithm

Item	Parameter	Value
System parameters of fractional-order chaotic system	a, b, c, d, k, q	$[1, 1, 0.5, 2.72165 * 10^{-4}, 1, 0.9]$
Initial conditions of fractional-order chaotic system	x, y, z	[1.9, 0, 0]
System parameters of discrete chaotic system	$a_1, b_1, c_1,$	$[2^{32\times(1-CR),}, 8\pi, round(CR \times H)]$
Initial conditions of discrete chaotic system	x, y, z	[0.8, 0.9, 0.6]



(a) (b) (c)

Fig. 8 The simulation result: **a** plain-text image, **b** cipher image, and **c** recover image

$$\begin{cases} MRF(Index1(i)) = MDF(i) - S1(i) - S2(i) \\ MRF(Index1(i)) = MRF(Index1(i)) \bmod L \end{cases}, \quad (21)$$

Equation (21) is inverse algorithm of Eq. (19). The inverse algorithm of Eq. (20) as follows

$$\begin{cases} MR(Index1(i)) = MR1(i) - MR2(Index2(i)) \\ -(4 * S1(i) + 5 * S2(i)) \\ MR(Index1(j)) = MR(Index1(j)) \bmod L \end{cases}. \quad (22)$$

2. Inverse uniformization of image matrix. The method of inverse uniformization as follows

$$R = (Q * (Max - Min))/255 + Min, \quad (23)$$

where the matrix R is recover image matrix.
3. Reconstruct the original image pixel. The smoothed ℓ_0 (SL0) algorithm is applied to reconstruct pixel of image matrix.
4. Inverse the DWT and obtain the final decrypted image.

4 The performance analysis

4.1 Simulation result

This section to test the decoded image is similar to the plain-text image, where some classical images are selected as the test images. The encryption parameters contain two parts: (1) the parameters of the chaotic system; (2) the initial parameters of the chaotic system. The structure of the secret key is listed in Table 2. The encryption and decryption results are shown in Fig. 8.

4.2 The key analyses

The secret key is decided the decoded image is correct. Also, the secret key can affect the security of the cipher image. Therefore, the security of secret key is an important character of encryption algorithm. This subsection has two directions need to discuss.

4.2.1 The key space analysis

The first discussion point is the key space. The space of secret key should approach or larger than 2^{100} [5,8,12]. The large key space makes sure the cipher image has the ability to resist the brute-force attack. The key space of the proposed algorithm can approach 2^{448}. This result is satisfied with the request for key space. Table 3 demonstrates that the comparison result with another encryption scheme. Firstly, the proposed algorithm has enough key space to resist the brute-force attack. Secondly, compared with other algorithms, the key space of the proposed algorithm is large.

Table 3 Key space

The encryption scheme	Key space
Proposed algorithm	2^{747}
Ref. [33]	2^{256}
Ref. [19]	2^{224}
Ref. [37]	2^{240}

4.2.2 The key sensitivity analysis

The second discussion point is the sensitivity of the secret key. The image applied to test key sensitivity is Lena (256×256). Set the change value Δ equal to $\pm 10^{-15}$; the new parameters encode the plain-text image. The test result is shown in Fig. 9. The difference between the two cipher images can be calculated by the number of pixels change rate (NPCR). The calculation method is shown as follows

$$NPCR = \frac{\sum_{i,j} D(i,j)}{H \times W} \times 100\%. \quad (24)$$

Equation 25 is represented the symbolic function $D(i,j)$.

$$D(i,j) = \begin{cases} 1 & C(i,j) \neq C_1(i,j) \\ 0 & C(i,j) = C_1(i,j) \end{cases}, \quad (25)$$

where C (i, j) is the original cipher matrix and C1 (i, j) is the new cipher matrix. The size of image matrix can be considered as $W \times H$. Besides, the new cipher matrix has come from the different parameters of encryption algorithm.

Table 4 shows the test results of NPCR with difference cipher image. It is obviously that the new cipher image is a different image compare with the original cipher image. The error key can't recover the cipher image. In the encryption phase, the little change of secret key can obtain the difference cipher image.

4.3 The anti-statistical attack ability analyses

The discussion point in this subsection is the anti-statistical attack ability. The discussion direction has three indexes, the histogram, the information entropy, and the adjacent point correlation analysis. These indexes can present the randomness of cipher image.

4.3.1 The histogram analysis

The purpose of histogram analysis proves that the distribution of pixels is the uniform distribution. This hypothesis can be illustrated by χ^2-value. The different critical values with

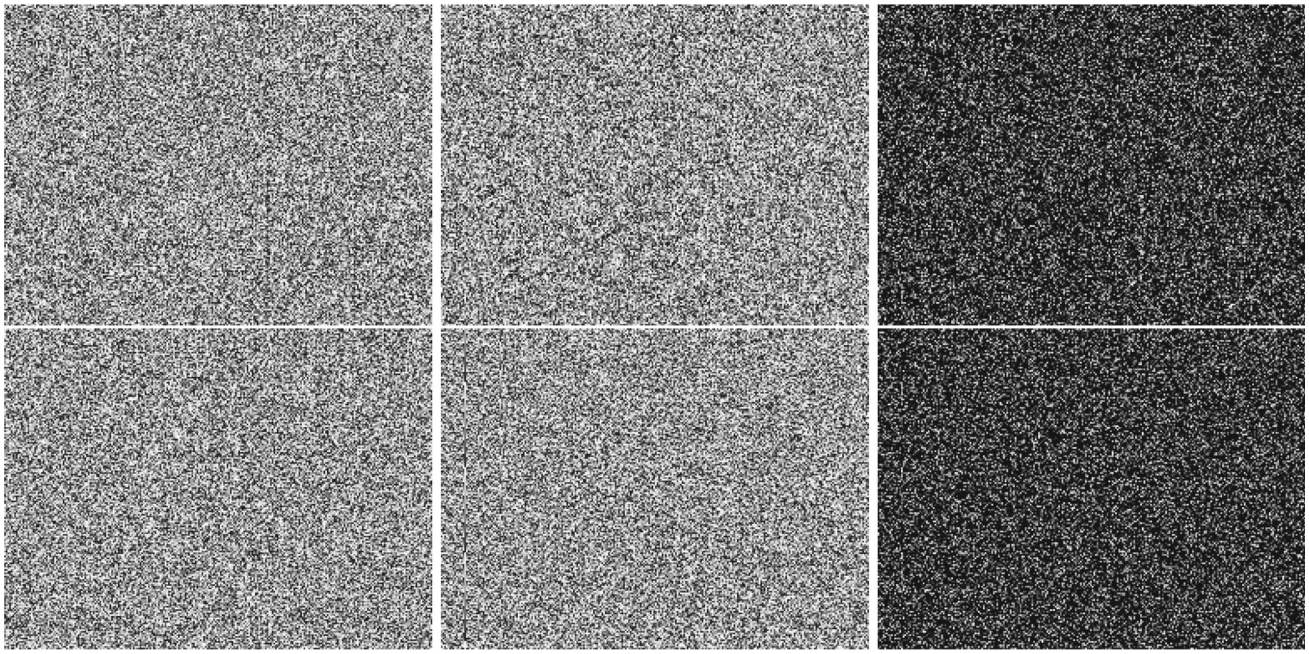


Fig. 9 The analysis result of key sensitivity: **a** The original cipher image, **b** the new cipher image, and **c** the result of image subtraction

Table 4 NPCR between the new cipher image and the original cipher image

The image name	NPCR (%)
Lena (256 × 256)	99.6053
Couple (256 × 256)	99.6012
Lake (256 × 256)	99.6358
Lax (256 × 256)	99.6134

10%, 5%, and 1% probability are 284.3360, 293.2478, and 310.4574, respectively. The analysis result is listed in Table 5. The values of χ^2 can prove that the distribution cipher image is uniform. The histogram of the cipher image and the plain-text image is shown in Fig. 10.

4.3.2 Correlation analysis

The correlation analysis is aim to measure the correlation of adjacent pixel in different directions. The calculation equation of correlation coefficients is shown in Eq. (26–29).

$$\gamma_{xy} = \frac{cov(x, y)}{\sqrt{D(X)D(Y)}}; \tag{26}$$

$$cov(x, y) = E(X - E(X)) - (Y - E(Y)); \tag{27}$$

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i; \tag{28}$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N}[(x_i - E(x))]^2. \tag{29}$$

This equation group has calculated the value of correlation coefficients of the image. The correlation coefficients of the

Table 5 χ^2-value for different images

The image name	χ^2-value (plain-text)	χ^2-value (cipher)	Critical Value		
			$\chi^2_{0.1}$ (255)	$\chi^2_{0.05}$ (255)	$\chi^2_{0.01}$ (255)
Lena (256*256)	40483.4453	246.0703	Pass	Pass	Pass
Lena (512*512)	439826.9414	237.8184	Pass	Pass	Pass
Couple (256*256)	54616.9531	277.7813	Pass	Pass	Pass
Lake (256*256)	48805.5156	231.2917	Pass	Pass	Pass
Lax (256*256)	134336.7109	249.5833	Pass	Pass	Pass

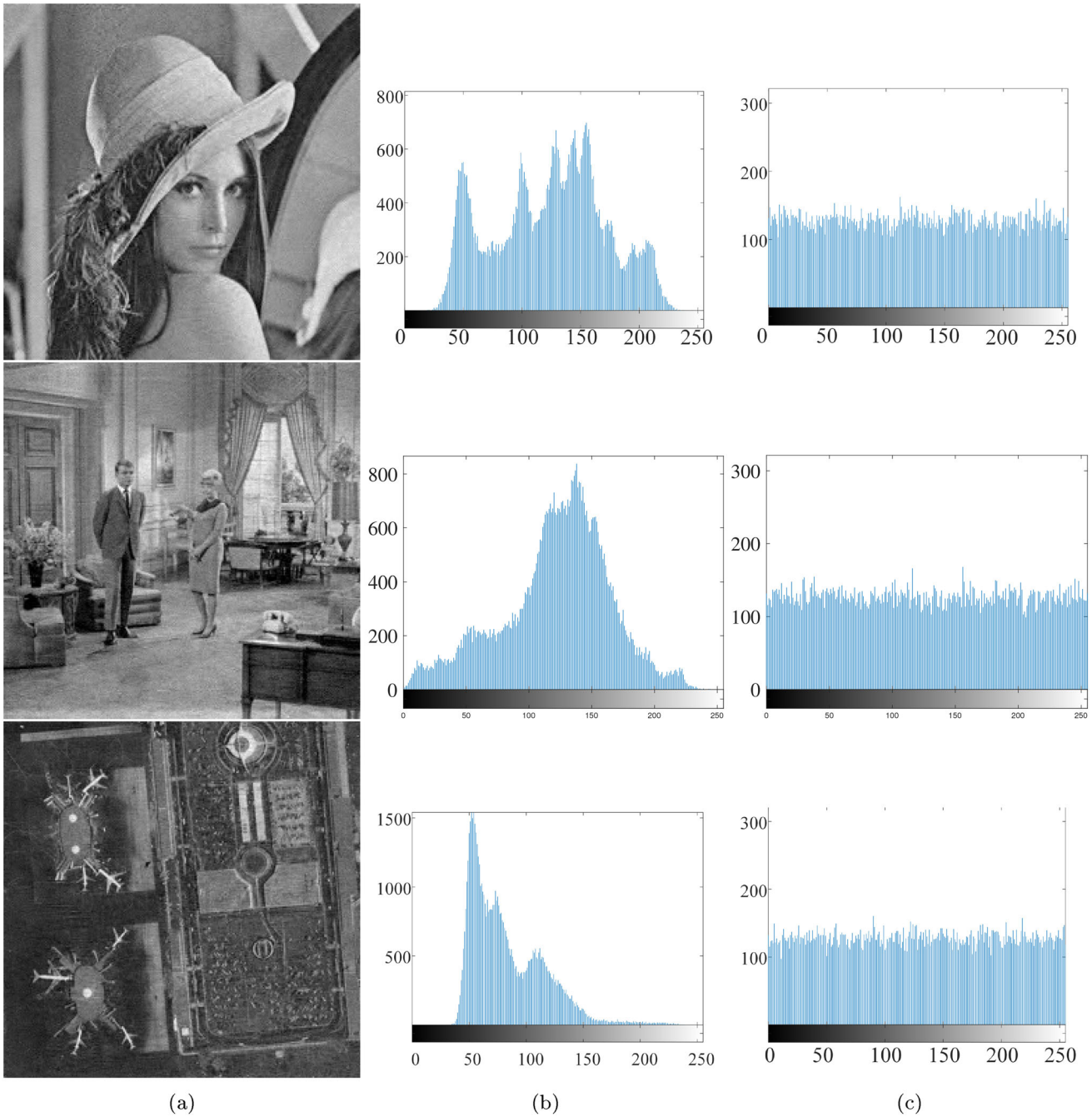


Fig. 10 The analysis result of histogram: **a** the test image, **b** the histogram of plain-text image, and **c** the histogram of cipher image

cipher image are close to 0. It can prove that the adjacent pixel is not correlated. The adjacent pixel point distribution is shown in Fig. 11. The correlation coefficient results are listed in Table 6. The comparison results are shown in Table 7

Figure 11d–f illustrates that the correlation of adjacent pixels is reduced. The correlation coefficient with different directions can prove that the assumption is correct.

4.4 The compression ratio analyses

In this subsection, the mean structural similarity (MSSIM) and peak signal-to-noise ratio (PSNR) are applied to measure the quality of decode image with difference compression ratios.

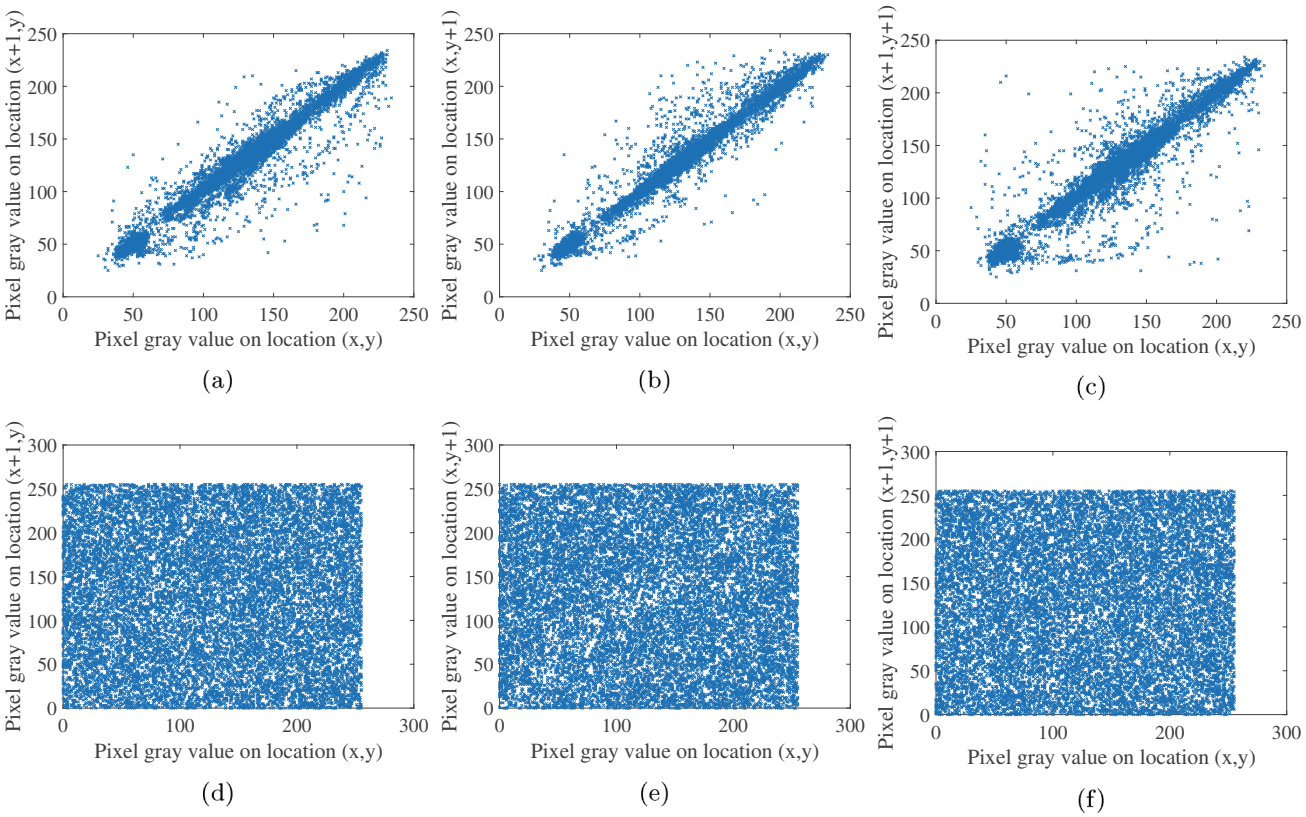


Fig. 11 The analysis result of pixel point distribution: **a** plain-text horizontal direction, **b** plain-text vertical direction correlation, **c** plain-text diagonal direction correlation, **d** ciphertext horizontal direction correlation, **e** ciphertext vertical direction correlation, and **f** ciphertext diagonal direction correlation

4.4.1 The mean structural similarity (MSSIM) analysis

The structural similarity (SSIM) is used to measure the similarity between two images. The mean structural similarity (MSSIM) is applied to evaluate the performance of the encryption algorithm. The calculation method is defined as

$$\begin{cases} I(X,Y) = \frac{2\mu_x\mu_y+C_1}{\mu_x^2+\mu_y^2+C_1} \\ c(X,Y) = \frac{2\sigma_x\sigma_y+C_2}{\sigma_x^2+\sigma_y^2+C_2} \\ s(X,Y) = \frac{\sigma_{xy}+C_3}{\sigma_x\sigma_y+C_3} \\ SSIM(X,Y) = I(X,Y) \times c(X,Y) \times s(X,Y) \\ MSSIM(X,Y) = \frac{1}{M}\sum_{k=1}^{M} SSIM(x_k, y_k) \end{cases}, \quad (30)$$

where μ_x and μ_y represent the average values of plain image X and the decode image Y. σ_x and σ_y denote the variance values of X and Y. σ_{xy} is the covariance of X and Y. $C1$, $C2$ and $C3 = [(K_1 \times 255)^2, (K_2 \times 255)^2, \frac{C_2}{2}]$ are constants, where $k_1 = 0.01$ and $k_2 = 0.03$. The total number of image blocks M is equal to 64. Table 8 lists the different images at the different compression.

The bigger MSSIM value can prove two different images have a good similarity. For the decrypted image, the value of MSSIM is bigger than 0.9. The analysis results illustrated that the decrypted image is similar to the plain-text image.

4.4.2 The peak signal-to-noise ratio (PSNR) analysis

The anti-noise attack ability is discussion point in this section. The cipher image might be disturbed by noise signal during transmission. Mean squared error (MSE) and peak signal-to-noise ratio (PSNR) are adopted to calculate the quality of decrypted image. The formula of MSE and PSNR is as follows:

$$\begin{cases} MSE = \frac{\sum_{i=1}^{n}(y_i - x_i)^2}{H*W} \\ PSNR = 10\lg\frac{255^2}{MSE} \end{cases}, \quad (31)$$

where x_i and y_i are the pixel value of plain-text image and decrypted image, respectively. The high score of PSNR can illustrate the high quality of decode image. On the contrary, the value of MSE has a low degree. The diagrams of MSE and PSNR are shown in Fig. 12a, b. The simulation condition

Table 6 Correlation coefficients with different directions

The test image name	Horizontal		Vertical		Diagonal	
	Plain-text	Cipher	Plain-text	Cipher	Plain-text	Cipher
Lena (256*256)	0.9412	− 0.0031	0.9699	0.0029	0.9267	5.8684e-05
Lena (512*512)	0.98254	0.0060	0.98575	− 0.0016	0.9600	− 0.0002

Table 7 Correlation coefficients with different algorithms

The image name	Horizontal		Vertical		Diagonal	
	Plain-text	Cipher	Plain-text	Cipher	Plain-text	Cipher
Proposed algorithm	0.9412	− 0.0031	0.9699	0.0029	0.9267	5.8684e-05
Ref. [46]	0.9577	0.0034	0.9226	− 0.0003	0.9019	− 0.0011
Ref. [4]	0.9654	0.0019	0.9326	0.0012	0.9071	0.0009
Ref. [2]	0.9750	− 0.0002	0.9230	− 0.0015	0.9102	− 0.0008
Ref. [10]	0.9646	0.0022	0.9342	0.0013	0.9075	0.0008

Table 8 The compression results of MSSIM values with difference CR

Images	CR	Proposed algorithm	Ref. [7]	Ref. [30]
	0.2	0.9141		0.3368
*Lena (256 × 256)	0.4	0.9513		0.4547
	0.8	0.9831		0.7012
	0.25	0.7878	0.9633	
*Baboon (256 × 256)	0.5	0.8992	0.9823	
	0.75	0.9417	0.9892	

is that the encrypted image is attacked by Gaussian white noise with the variance within the range of $(10^{-7}, 10^{-5})$. The distribution of MSE and PSNR displays that the noise signal could affect the quality of the decrypted image.

The other function of PSNR is to judge the quality of the recovered image. The Lean (256 × 256) image is selected as the test image in this section. The comparison result is shown in Table 9.

The other index about image quality is cosine similarity. This index is applied to calculate the similarity between the decrypted image and the original image. The equation of cosine similarity is

$$\cos\theta = \frac{\sum_{i=1}^{n}(x_i, y_i)}{\sqrt{\sum_{i=1}^{n} x_i} \cdot \sqrt{\sum_{i=1}^{n} y_i}}, \tag{32}$$

where x_i and y_i are present for the decrypted image with Gaussian noise signal and plain-text image, respectively. In the ideal conditions, the result of cosine similarity should be 1. The value of cosine similarity decrease when the cipher image is affected by the noise signal. The results of cosine similarity are shown in Fig. 12c.

The analysis results can prove that the encryption algorithm can resist the effect of the noise signal. The quality of the decrypted image is shown clearly. The similarity of cosine can prove that the cipher image is similar to the plain-text image.

4.5 The anti-difference attack ability

The NPCR (number of pixels change rate) and UACI (unified average changing intensity) are important index for measuring the ability for anti-difference attack. The equation of NPCR is present in Eq. (24–25). The calculation method of UACI is shown as follows

$$UACI = \frac{1}{L}\sum_{i,j}\frac{|C(i,j) - C_1(i,j)|}{256} \times 100\%, \tag{33}$$

where C (i,j) is the cipher matrix and C1 (i,j) is the new cipher matrix. In this subsection, the pixel original plain-text image is changed randomly. The new plain-text image is obtained. Therefore, the new plain image is applied to encryption and obtained the new cipher image C1.

The criteria values of NPCR and UACI are applied to test the encryption algorithm. The critical score of NPCR is

$$N_a^* = \frac{G - \Phi^{-1}(a)\sqrt{\frac{G}{L}}}{G+1}, \tag{34}$$

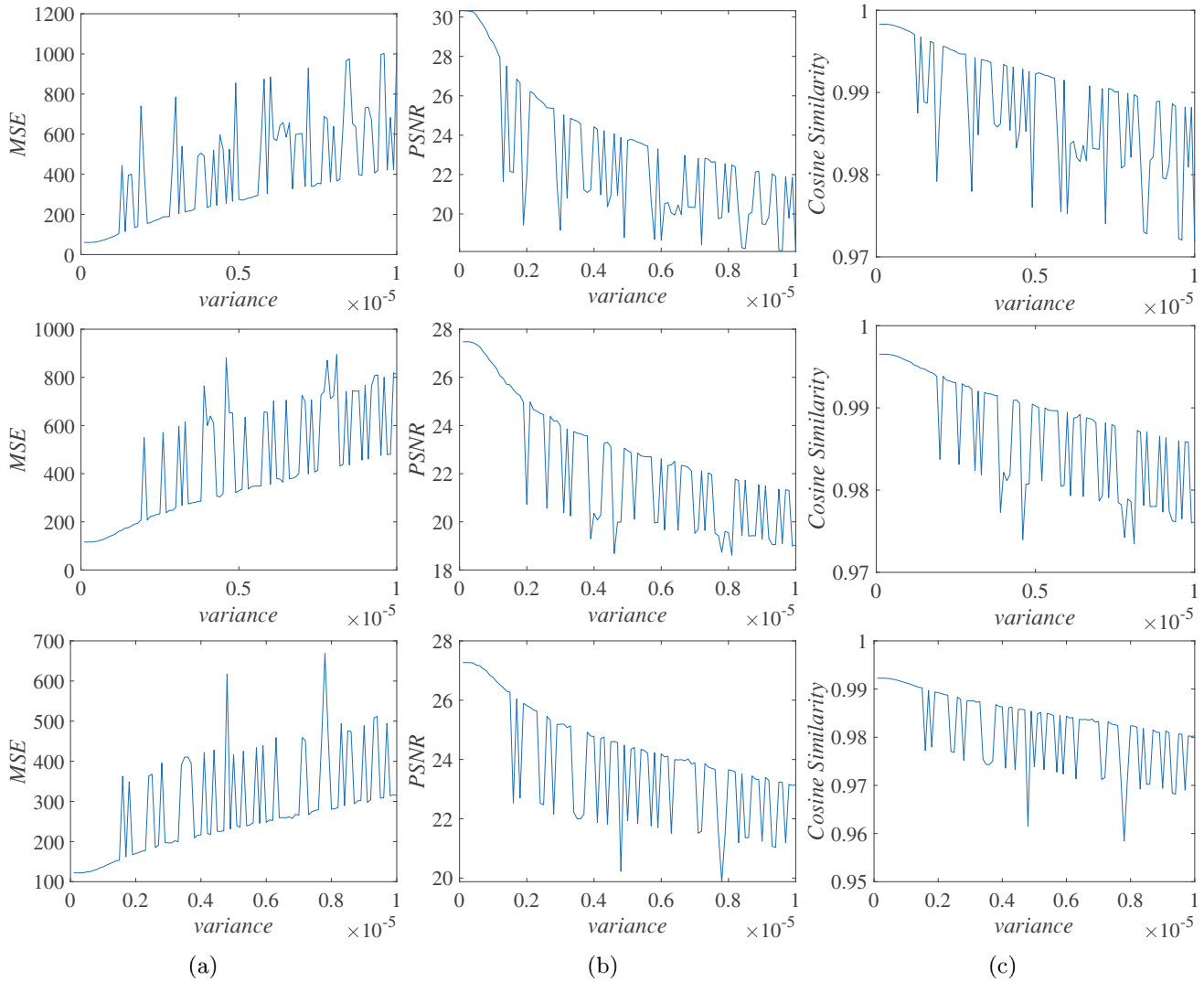


Fig. 12 The analysis result of anti-noise attack: **a** MSE, **b** PSNR, and **c** cosine similarity

Table 9 The compression results of PSNR with difference CR

Images	CR	Proposed algorithm	Ref. [7]	Ref. [30]
*Lena 256 (256 × 256)	0.2	25.4763		28.7059
	0.25	25.1769	26.0600	28.0900
	0.4	28.2450		29.6826
	0.5	30.3211	29.8200	29.8500
	0.75	32.1803		32.2200
	0.8	32.7317	29.5600	32.6120

where G is the number of pixel points or coordinates in a plain matrix, L indicates the value of the gray level. Setting the significance level α, the NPCR value of the cipher image is greater than N_*^a. It means that the encryption scheme can resist difference attack effectively. The critical range of UACI is obtained from Eq. (35)

$$\begin{cases} u_a^{*-} = \mu_u - \Phi^{-1}(\frac{\alpha}{2})\sigma_u \\ u_a^{*+} = \mu_u + \Phi^{-1}(\frac{\alpha}{2})\sigma_u \end{cases}, \tag{35}$$

where

$$\mu_u = \frac{G+2}{3G+4}, \tag{36}$$

Table 10 The NPCR result of different images

The image name	NPCR (mean)	Critical Value		
		$N^*_{0.05}$ (255) =99.5696%	$N^*_{0.01}$ (255) =99.5527%	$N^*_{0.001}$ (255) =99.5341%
Lena (256*256)	99.6007%	Pass	Pass	Pass
Lena (512*512)	99.6162%	Pass	Pass	Pass
Couple (256*256)	99.6022%	Pass	Pass	Pass
Lax (256*256)	99.6034%	Pass	Pass	Pass

Table 11 The UACI result of different images

The image name	UACI (mean) (%)	Critical value		
		$u^{*+}_{0.05}$ (255) =33.6447% $u^{*-}_{0.05}$ (255) =33.2824%	$u^{*+}_{0.01}$ (255) =33.7016% $u^{*-}_{0.01}$ (255) =33.2255%	$u^{*+}_{0.001}$ (255) =33.7677% $u^{*-}_{0.001}$ (255) =33.1594%
Lena (256*256)	33.5381	Pass	Pass	Pass
Lena (512*512)	33.4645	Pass	Pass	Pass
Couple (256*256)	33.4346	Pass	Pass	Pass
Lax (256*256)	33.6926	Pass	Pass	Pass

Table 12 Comparison results between other algorithms

The image name	NPCR (%)	UACI (%)
Proposed scheme	99.60	33.54
Ref. [46]	99.61	33.45
Ref. [10]	99.61	33.46
Ref. [41]	99.60	33.46

and

$$\sigma_u = \frac{(G+2)(G^2+2G+3)}{18(G+1)^2GL}. \tag{37}$$

The UACI score of cipher images should fall into the interval of (u_a^{*-}, u_a^{*+}). It can prove that the encryption algorithm passes the UACI test. The test results of NPCR and UACI are listed in Tables 10 and 11.

The test results can prove that the encryption algorithm has a high sensitivity of pixels change. It means that the encryption algorithm can resist the difference attack. The comparison result of other encryption schemes is shown in Table 12.

4.6 The anti-choose plain-text and Known plain-text attack analysis

In this section, the known plain-text attack and chosen plain-text attack are used to evaluate the security performance of the encryption algorithm. Based on the description in Ref. [14], the attacker can choose the random matrix to obtain the corresponding cipher and speculate the construction of the secret key. For measuring the algorithm performance of resisting the known plain-text attack and chosen plain-text attack, all-white and all-black pictures are selected as encryption object. The performance of anti-known plain-text and chosen plain-text attacks ability are shown in Fig. 13 and Table 13.

The encryption result and histogram are shown in Fig. 13a–c. Figure 13c can illustrate that the cipher picture is the uniform distribution. Besides, the χ^2 value is 251.0833. It is satisfied with the critical stander of different freedom. It can prove that the proposed algorithm can resist known plain-text attack and chosen plain-text attack more effectively.

5 Conclusion

This paper provided a novel image encryption algorithm. This algorithm is based on the fractional-order Jerk system, the discrete chaotic system and compression sensing theory. Firstly, the analysis of the dynamical characteristics shows that this chaotic system has a wide chaotic range. Therefore, the analysis results can prove that this system is suitable to apply to the encryption algorithm. Secondly, the block cipher theory is applied to the encryption algorithm. Therefore, the size of secret code sequences is small. It can reduce the time cost of chaotic sequences calculation. In the encryption operation, the value of the plain-text matrix and the arrangement of pixels are changed simultaneously. It can permute the pixels arrangement more effectively. Moreover,

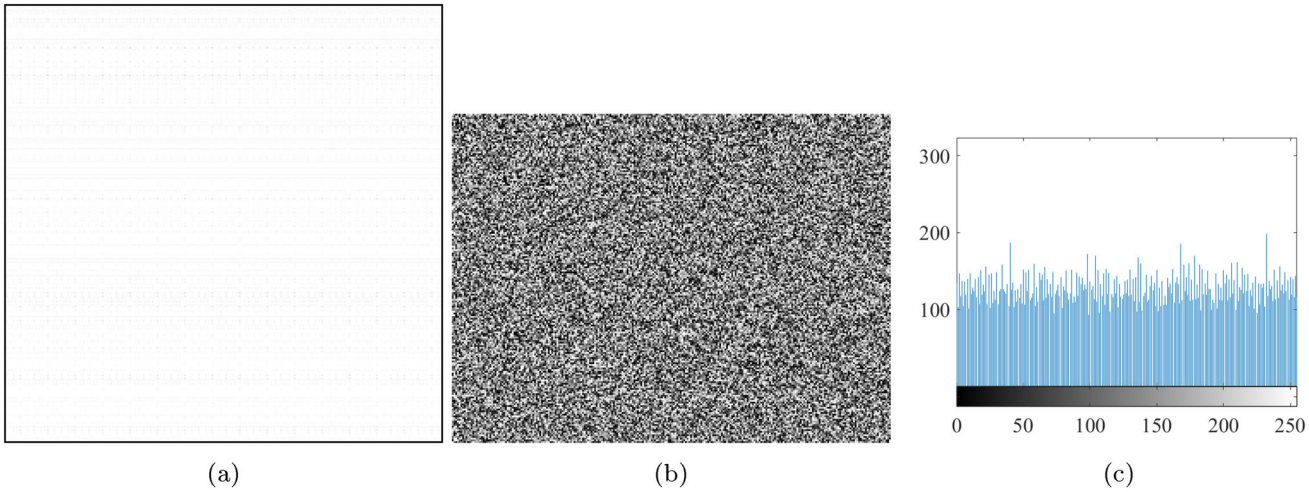


Fig. 13 The analysis result: **a** the plain-text image, **b** the cipher image, and **c** the histogram of cipher image

Table 13 The performance of anti-known plain-text attack

Encryption scheme	Image	NPCR	UACI	χ^2-value	Correlation coefficients		
					Horizontal	Vertical	Diagonal
Proposed scheme	All-white (256 × 256)	99.5605%	33.4350%	251.0833	−0.0026	0.0019	−0.0019

the current elements of the cipher block are based on the front cipher block and plain-text block. At the end, the security analyses show that this algorithm has good performance in resisting common attacks such as statistical, brute-force, and anti-differential attacks. Therefore, this encryption algorithm has good encryption properties and protects the plain information more effectively. Also, this algorithm provided another realization way for image security.

However, this algorithm still has few questions that need to be improved. The limitations of this algorithm are summarized as follows,

1. The one-dimensional measurement matrix is applied in the current algorithm. Therefore, the image size is only reduced in the row direction. The channel resource occupied problem cannot be overcome completely.
2. The two chaotic system can expend key space of secret key. Besides, these systems can provide different chaotic sequences. However, the calculation cost is bigger than the encryption algorithm based on the one chaotic system.

Therefore, the measurement matrix is two-dimensional in compression operation in the future. It can reduce the image size from two directions. The performance of compression has improved. On the other hand, the new chaotic sequence generator scheme is a new focus point in the future. The time cost of chaotic sequences calculation needs to decrease in the new scheme. This is an important index of new encryption algorithm.

Acknowledgements This subject is supported by the Natural Science Foundation of Liaoning Province (2020-MS-274) and the National Nature Science Foundation of China (No.61773010).

Declarations

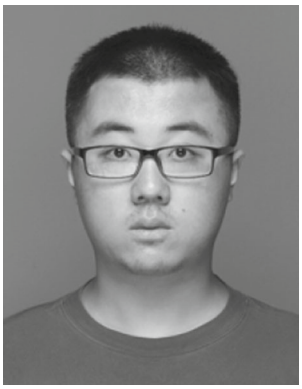
Conflict of interest No conflicts of interests in the publication by all authors.

References

1. Alvarez, G., Li, S.: Some basic cryptographic requirements for chaos-based cryptosystems. Int. J. Bifurcat. Chaos **16**(08), 2129–2151 (2006)
2. Aqeelurrehman, L.X., Hahsmi, M.A., Haider, R.: An efficient mixed inter-intra pixels substitution at 2bits-level for image encryption technique using dna and chaos. Optik **153**, 117–134 (2018)
3. Belazi, A., El-Latif, A.A.A., Belghith, S.: A novel image encryption scheme based on substitution-permutation network and chaos. Sig. Process. **128**, 155–170 (2016)
4. Cao, C., Sun, K., Liu, W.: A novel bit-level image encryption algorithm based on 2d-licm hyperchaotic map. Sig. Process. **143**, 122–133 (2018). https://doi.org/10.1016/j.sigpro.2017.08.020
5. Chai, X., Chen, Y., Broyde, L.: A novel chaos-based image encryption algorithm using dna sequence operations. Opt. Lasers Eng. (2017a). (**88(Complete):197–213**)

6. Chai, X., Gan, Z., Lu, Y., Chen, Y., Han, D.: A novel image encryption algorithm based on the chaotic system and dna computing. Int. J. Mod. Phys. C **28**(05), 1750069 (2017b)
7. Chai, X., Zheng, X., Gan, Z., Han, D., Chen, Y.: An image encryption algorithm based on chaotic system and compressive sensing. Sig. Process. **148**, 124–144 (2018). https://doi.org/10.1016/j.sigpro.2018.02.007
8. Chai, X., Wu, H., Gan, Z., Zhang, Y., Chen, Y.: Hiding cipher-images generated by 2-d compressive sensing with a multi-embedding strategy. Sig. Process. (2020). https://doi.org/10.1016/j.sigpro.2020.107525
9. Chen, C., Sun, K., He, S.: A class of higher-dimensional hyper-chaotic maps. Eur. Phys. J. Plus (2019). https://doi.org/10.1140/epjp/i2019-12776-9
10. Chen, C., Sun, K., He, S.: An improved image encryption algorithm with finite computing precision. Sig. Process. (2019b). https://doi.org/10.1016/j.sigpro.2019.107340
11. Chen, L.P., Yin, H., Yuan, L.G., Lopes, A.M., Machado, J.T., Wu, R.C.: A novel color image encryption algorithm based on a fractional-order discrete chaotic neural network and dna sequence operations. Front. Inf. Technol. Electron. Eng. **21**(6), 866–879 (2020)
12. Gan, Z., Chai, X.L., Han, D.J., Chen, Y.R.: A chaotic image encryption algorithm based on 3-d bit-plane permutation. Neural Comput. Appl. **31**(11), 7111–7130 (2018). https://doi.org/10.1007/s00521-018-3541-y
13. Gong, L., Deng, C., Pan, S., Zhou, N.: Image compression-encryption algorithms by combining hyper-chaotic system with discrete fractional random transform. Opt. Laser Technol. **103**, 48–58 (2018). https://doi.org/10.1016/j.optlastec.2018.01.007
14. Gong, L., Qiu, K., Deng, C., Zhou, N.: An optical image compression and encryption scheme based on compressive sensing and rsa algorithm. Opt. Lasers Eng. **121**, 169–180 (2019). https://doi.org/10.1016/j.optlaseng.2019.03.006
15. He, S., Sun, K., Banerjee, S.: Dynamical properties and complexity in fractional-order diffusionless Lorenz system. Eur. Phys. J. Plus **131**(8), 254 (2016)
16. He, S., Sun, K., Mei, X., Yan, B., Xu, S.: Numerical analysis of a fractional-order chaotic system based on conformable fractional-order derivative. Eur. Phys. J. Plus (2017a). https://doi.org/10.1140/epjp/i2017-11306-3
17. He, S., Sun, K., Wang, H., Mei, X., Sun, Y.: Generalized synchronization of fractional-order hyperchaotic systems and its dsp implementation. Nonlinear Dyn. **92**(1), 85–96 (2017b). https://doi.org/10.1007/s11071-017-3907-1
18. Hua, Z., Zhou, Y.: Image encryption using 2d logistic-adjusted-sine map. Inf. Sci. **339**, 237–253 (2016). https://doi.org/10.1016/j.ins.2016.01.017
19. Jin, X., Wu, Z., Song, C., Zhang, C., Li, X.: 3d point cloud encryption through chaotic mapping. In: Pacific Rim Conference on Multimedia, pp. 119–129. Springer (2016)
20. Khalil, R., Al Horani, M., Yousef, A., Sababheh, M.: A new definition of fractional derivative. J. Comput. Appl. Math. **264**, 65–70 (2014)
21. Li, G., Wang, L.I.: Double chaotic image encryption algorithm based on optimal sequence solution and fractional transform. Vis. Comput. **35**(9), 1267–1277 (2019)
22. Li, P., Xu, J., Mou, J., Yang, F.: Fractional-order 4d hyperchaotic memristive system and application in color image encryption. Eur. J. Image Video Process. **1**, 22 (2019)
23. Liu, W., Sun, K., He, S.: Sf-simm high-dimensional hyperchaotic map and its performance analysis. Nonlinear Dyn. **89**, 2521–2532 (2017a)
24. Liu, W., Sun, K., He, Y., Yu, M.: Color image encryption using three-dimensional sine icmic modulation map and dna sequence operations. Int. J. Bifurcat. Chaos **27**(11), 1750171 (2017b)
25. Ma, C., Jun, M., Cao, Y., Liu, T., Wang, J.: Multistability analysis of a conformable fractional-order chaotic system. Phys. Scr. **95**(7), (2020)
26. Matthews, R.: On the derivation of a chaotic encryption algorithm. Cryptologia **8**(8), 29–41 (1989)
27. Millerioux, G., Amigo, J.M., Daafouz, J.: A connection between chaotic and conventional cryptography. IEEE Trans. Circuits Syst. Regul. Pap. **55**(6), 1695–1703 (2008)
28. Mohimani, G.H., Babaie-Zadeh, M., Jutten, C.: Fast sparse representation based on smoothed l0 norm. In: International Conference on Independent Component Analysis and Signal Separation, pp 389–396. Springer (2007)
29. Mohimani, H., Babaie-Zadeh, M., Jutten, C.: A fast approach for overcomplete sparse decomposition based on smoothed l0 norm. IEEE Trans. Signal Process. **57**(1), 289–301 (2008)
30. Mou, J., Yang, F., Chu, R., Cao, Y.: Image compression and encryption algorithm based on hyper-chaotic map. Mobile Netw. Appl. (2019). https://doi.org/10.1007/s11036-019-01293-9
31. Peng, D., Sun, K.H., Alamodi, A.O.A.: Dynamics analysis of fractional-order permanent magnet synchronous motor and its dsp implementation. Int. J. Mod. Phys. B (2019a). https://doi.org/10.1142/s0217979219500310
32. Peng, Y., Sun, K., He, S., Peng, D.: Parameter identification of fractional-order discrete chaotic systems. Entropy **21**(1), 27 (2019b)
33. Rey, A.M.D.: A method to encrypt 3d solid objects based on three-dimensional cellular automata. In: Hybrid Artificial Intelligence Systems, pp. 427–438 (2015)
34. Sayed, W.S., Radwan, A.G.: Generalized switched synchronization and dependent image encryption using dynamically rotating fractional-order chaotic systems. AEU Int. J. Electron. Commun. **123**, (2020)
35. Talhaoui, M.Z., Wang, X., Midoun, M.A.: A new one-dimensional cosine polynomial chaotic map and its use in image encryption. Vis, Comput (2020a)
36. Talhaoui, M.Z., Wang, X., Talhaoui, A.: A new one-dimensional chaotic map and its application in a novel permutation-less image encryption scheme. Vis, Comput (2020b)
37. Wang, X., Xu, M., Li, Y.: Fast encryption scheme for 3d models based on chaos system. Multimed. Tools Appl. **78**(23), 33865–33884 (2019)
38. Xu, Q., Sun, K., Cao, C., Zhu, C.: A fast image encryption algorithm based on compressive sensing and hyperchaotic map. Opt. Lasers Eng. **121**, 203–214 (2019). https://doi.org/10.1016/j.optlaseng.2019.04.011
39. Yang, F., Mou, J., Luo, C., Cao, Y.: An improved color image encryption scheme and cryptanalysis based on hyperchaotic sequence. Phys. Scr. **94** (2019a)
40. Yang, F., Mou, J., Sun, K., Cao, Y., Jin, J.: Color image compression-encryption algorithm based on fractional-order memristor chaotic circuit. IEEE Access (2019b). https://doi.org/10.1109/ACCESS.2019.2914722
41. Yang, F., Mou, J., Liu, J., Ma, C., Yan, H.: Characteristic analysis of the fractional-order hyperchaotic complex system and its image encryption application. Signal Process. **169**, (2020)
42. Yu, S.S., Zhou, N.R., Gong, L.H., Nie, Z.: Optical image encryption algorithm based on phase-truncated short-time fractional Fourier transform and hyper-chaotic system. Opt. Lasers Eng. (2020). https://doi.org/10.1016/j.optlaseng.2019.105816
43. Zhang, L.M., Sun, K.H., Liu, W.H., He, S.B.: A novel color image encryption scheme using fractional-order hyperchaotic system and dna sequence operations. Chin. Phys. B **26**, 10 (2017)
44. Zhongyun, H., Zhou, Y., Huang, H.: Cosine-transform-based chaotic system for image encryption. Inf. Sci. **480**, 403–419 (2019). https://doi.org/10.1016/j.ins.2018.12.048

45. Zhou, S., Wei, Z., Wang, B., Zheng, X., Zhou, C., Zhang, Q.: Encryption method based on a new secret key algorithm for color images. AEU Int. J. Electron. Commun. **70**(1), 1–7 (2016)
46. Zhu, C., Gan, Z., Lu, Y., Chai, X.: An image encryption algorithm based on 3-d dna level permutation and substitution scheme. Multimed. Tools Appl. (2019). https://doi.org/10.1007/s11042-019-08226-4



Ji Xu He currently pursuing the Ph.D. degree in Dalian polytechnic University. His mainly research interest is chaotic digital image cryptosystem.

Jun Mou He is a professor in Dalian Polytechnic University. His mainly research interest includes the nonlinear system control, secure communication, power system automation and smart grid research.

Jian Liu She is a professor in Jinan University. Her mainly research interest includes the nonlinear system control.

Jin Hao He currently pursuing the master degree in Dalian polytechnic University His mainly research interest is chaotic digital image cryptosystem.