Multimedia Tools and Applications (2023) 82:4343–4369
https://doi.org/10.1007/s11042-022-13414-w

A novel chaotic system with hidden attractor and its application in color image encryption

Haiying Hu[1] · Yinghong Cao[1] · Jin Hao[1] · Xuejun Li[1] · Jun Mou[1]

Received: 6 December 2020 / Revised: 11 May 2022 / Accepted: 2 July 2022 /
Published online: 26 July 2022

Abstract
In this paper, a novel fractional-order no-equilibrium chaotic system with hidden attractor is presented. The dynamical characteristics of the fractional-order system are analyzed by the phase diagram, Lyapunov exponents, bifurcation diagram, complexity, and attractor basin. Based on the above analysis, an image encryption scheme performs discrete cosine transform on the R, G, and B channels of the original color image to get the corresponding sparse coefficient matrices. Then, the measurement matrix generated by the Hadamard matrix and the chaotic pseudo-random sequence is used to compress and perceive the sparse coefficient matrices. In addition, the row and column scrambling and GF (257) domain diffusion algorithm are performed on the compressed pixel matrix to obtain the final cipher image. Experimental results and performance analysis display that the scheme has high compressibility and security. Even if the compression rate is 0.25, the calculated PSNR values are around 30. In addition, the χ^2-value of the encrypted Lena image is 248.2824, and the algorithm has passed the UACI and NPCR tests and can resist differential attacks. Therefore, the proposed algorithm is effectively.

Keywords Fractional-order no-equilibrium chaotic system · Hidden attractor · Color image encryption

1 Introduction

In 2011, Leonov and Kuznetsov put forward the concept of hidden attractor [22, 25]. Generally, chaotic systems with no equilibrium point, stable equilibrium point and infinite number of unstable equilibrium points are classified as chaotic systems with hidden attractors. This kind of chaotic system has some hidden chaotic characteristics, which has potential

✉ Yinghong Cao
caoyinghong@dlpu.edu.cn

✉ Jun Mou
moujun@csu.edu.cn

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

application value in the field of nonlinear terms and engineering applications [18, 20, 23, 24, 37–41, 44, 45, 49]. In 2013, Jafari et al. [18]. listed a series of elementary 3-D chaotic systems without equilibrium points. Research on chaotic systems without equilibrium points has also become a focus. Wang and Chen gave a chaotic system without equilibrium points, on this basis, a chaotic system with any number of equilibrium points was constructed [49]. In 2015, a chaotic system containing nonlinear exponential terms is studied, with no equilibrium point but has rich dynamical characteristics [38]. In 2016, a 4-D hyperchaotic system with hidden attractors and its dynamical characteristics, control, and synchronization are analyzed by Vaidyanathan [45]. Pham et al. [40] discovered a 3-D chaotic system without equilibrium points, analyzed the basic dynamical characteristics of the system, and implemented the circuit of the system. All of the above are studies of some integer order no-equilibrium chaotic systems. However, the properties of the fractional-order chaotic system without equilibrium have not been researched, the dynamical characteristics of the fractional-order no-equilibrium system is analyzed. At present, the methods for solving fractional differential equations mainly include the frequency domain approximation method [19], predictor-corrector method [10], and Adomian decomposition method (ADM). Compared with the other two methods, ADM decomposition method has high calculation accuracy, fast convergence speed, and less computer resource consumption [53]. Therefore, the ADM decomposition algorithm is chosen to solve the fractional chaotic system in this paper. In addition, a very important application field of chaotic system is image encryption, so we not only analyze the chaotic system with no equilibrium point of fractional order, but also study its application.

Nowadays, digital images have become one of the major interactive objects on the Internet, especially in the medical, military and national defense fields, which means that we have hidden security risks when transmitting images [15]. Generally the amount of image data is large and the storage cost is high. Therefore, the image should be compressed and encrypted during the image transmission process. Due to pseudo-random characteristics of chaotic system and the high sensitivity to initial values, image encryption algorithms based on chaotic systems have become a hot spot in information security research [3, 21, 47, 52, 54]. So far, various chaotic image encryption algorithms have been proposed [1, 4, 5, 8, 9, 12–14, 16, 17, 26–28, 30, 35, 51, 55–58]. In 2020, A color image encryption system was proposed by Hu et al. [14], this algorithm uses chaotic pseudo-random sequences and matrix convolution operations to scramble and diffuse the pixel matrix, respectively. In 2019, Hasanzadeh et al. [12] introduced a color image encryption scheme based on the replacement box and Chen hyper-chaotic system, which has a massive secret key space and secret key sensitivity. Based on the coupled hyperchaotic system and Galois field arithmetic operations, Liu et al. proposed a medical image encryption scheme. [28]. Yang et al. [56] introduced a diffusion algorithm using the complex chaotic system and the gravity law model. These algorithms are sufficiently secure, but further research found that there is a considerable storage cost during image transmission. Zhu and Chen used a low-dimensional chaotic system and block compressive sensing to encrypt color image [58]. Mou et al. [35] studied image compression and encryption algorithm that combined 3D hyper-chaotic system and compressive sensing.

Based on the above research background, the dynamic characteristics of fractional order no-equilibrium chaotic system are analyzed, and it is applied in the field of image encryption, and an encryption algorithm with high efficiency and low storage space is designed. This system could complete image encryption and compression simultaneously and has

high compressibility and security. Firstly, a fractional-order no-equilibrium chaotic system is given, which is solved by the ADM decomposition algorithm. Using phase diagram, Lyapunov exponents and bifurcation diagram to analyze the dynamical characteristics of the fractional-order no-equilibrium chaotic system, and obtaining the optimal parameter range for applying the system to the image encryption system. Moreover, the generated chaotic pseudo-random sequences are used in the entire cryptographic system. Secondly, the Hadamard matrix and chaotic pseudo-random sequences are used to construct the measurement matrix of the R, G, and B channels of the color image. Finally, the compressed R, G, and B channels are scrambled separately, and the scrambled channels are diffused based on the GF (257) domain and chaotic pseudo-random sequences to obtain the final cipher image.

The rest of this paper is organized as follows. The dynamical characteristics of the fractional-order no-equilibrium chaotic system are analyzed in Section 2, The color image encryption scheme is introduced in detail in Section 3, the simulation results and the performance analysis of the proposed scheme are illustrated in Section 4. Finally, conclude in Section 5.

2 Fractional-order no-equilibrium chaotic system

2.1 Fractional-order no-equilibrium chaotic system model

The no-equilibrium chaotic system can be defined as

$$\begin{cases} \dot{x} = y \\ \dot{y} = -x - yz \\ \dot{z} = xy + \alpha x^2 + \beta y^2 - \gamma \end{cases}. \tag{1}$$

here α, β, γ are parameters and α, β, $\gamma > 0$, the state variables are represented by x, y, z.

According to the definition of Caputo fractional calculus and the system (1), the mathematical expression of the fractional-order no-equilibrium system is

$$\begin{cases} *D_{t_0}^{q} x = y \\ *D_{t_0}^{q} y = -x - yz \\ *D_{t_0}^{q} z = xy + \alpha x^2 + \beta y^2 - \gamma \end{cases}. \tag{2}$$

here q means the order of the fractional system equation, and $0 < q \leq 1$.

2.2 Solution of the fractional-order no-equilibrium chaotic system

Solving the fractional-order system equation by ADM algorithm, the linear, non-linear and constant terms of the system (2) are

$$\begin{bmatrix} Lx_1 \\ Lx_2 \\ Lx_3 \end{bmatrix} = \begin{bmatrix} x_2 \\ -x_1 \\ 0 \end{bmatrix}, \begin{bmatrix} Nx_1 \\ Nx_2 \\ Nx_3 \end{bmatrix} = \begin{bmatrix} 0 \\ -x_2 x_3 \\ x_1 x_2 + \alpha (x_1)^2 + \beta (x_2)^2 \end{bmatrix}, \begin{bmatrix} g_1 \\ g_2 \\ g_3 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ -\gamma \end{bmatrix} \tag{3}$$

The non-linear term needs further decomposition. As the ADM decomposition algorithm has fast convergence [32], only the first five terms of the non-linear term can be decomposed to ensure the calculation accuracy. The non-linear term is decomposed into

$$\begin{cases} A_2^0 = -x_2^0 x_3^0 \\ A_2^1 = -x_2^1 x_3^0 - x_2^0 x_3^1 \\ A_2^2 = -x_2^2 x_3^0 - x_2^1 x_3^1 - x_2^0 x_3^2 \\ A_2^3 = -x_2^3 x_3^0 - x_2^2 x_3^1 - x_2^1 x_3^2 - x_2^0 x_3^2 \\ A_2^4 = -x_2^4 x_3^0 - x_2^3 x_3^1 - x_2^2 x_3^2 - x_2^1 x_3^3 - x_2^0 x_3^4 \end{cases} \tag{4}$$

$$\begin{cases} A_3^0 = x_1^0 x_2^0 + \alpha (x_1^0)^2 + \beta (x_2^0)^2 \\ A_3^1 = x_1^1 x_2^0 + x_1^0 x_2^1 + 2\alpha x_1^1 x_1^0 + 2\beta x_2^1 x_2^0 \\ A_3^2 = x_1^2 x_2^0 + x_1^1 x_2^1 + x_1^0 x_2^2 + 2a x_1^2 x_1^0 + a x_1^1 x_1^1 \\ \quad +2\beta x_2^2 x_2^0 + \beta x_2^1 x_2^1 \\ A_3^3 = x_1^3 x_2^0 + x_1^2 x_2^1 + x_1^1 x_2^2 + x_1^0 x_2^2 + 2\alpha x_1^3 x_1^0 + 2\alpha x_1^1 x_1^2 \\ \quad +2\beta x_2^3 x_2^0 + 2\beta x_2^1 x_2^2 \\ A_3^4 = x_1^4 x_2^0 + x_1^3 x_2^1 + x_1^2 x_2^2 + x_1^1 x_2^3 + x_1^0 x_2^4 + 2\alpha x_1^4 x_1^0 + 2\alpha x_1^3 x_1^1 \\ \quad +\alpha x_1^2 x_1^2 + 2\beta x_2^4 x_2^0 + 2\beta x_2^3 x_2^1 + \beta x_2^2 x_2^2 \end{cases} \tag{5}$$

The solution of system (2) is defined as

$$\tilde{x}_j(t) = c_j^0 + c_j^1 \frac{(t-t_0)^q}{\Gamma(q+1)} + c_j^2 \frac{(t-t_0)^{2q}}{\Gamma(2q+1)} + c_j^3 \frac{(t-t_0)^{3q}}{\Gamma(3q+1)} + c_j^4 \frac{(t-t_0)^{4q}}{\Gamma(4q+1)} + c_j^5 \frac{(t-t_0)^{5q}}{\Gamma(5q+1)} \tag{6}$$

where $h = t - t_0$ is time step, $j = 1, 2, 3$. And

$$\begin{cases} C_{10} = x_1^0 \\ C_{20} = x_2^0 \\ C_{30} = x_3^0 - \frac{\gamma h^q}{\Gamma(q+1)} \end{cases} \tag{7}$$

$$\begin{cases} C_{11} = C_2^0 \\ C_{21} = -C_1^0 - C_2^0 C_3^0 \\ C_{30} = C_1^0 C_2^0 + \alpha (C_1^0)^2 + \beta (C_2^0)^2 \end{cases} \tag{8}$$

$$\begin{cases} C_{12} = C_2^1 \\ C_{22} = -C_1^1 - C_2^1 C_3^0 - C_2^0 C_3^1 \\ C_{32} = C_1^1 C_2^0 + C_1^0 C_2^1 + 2\alpha C_1^1 C_1^0 + 2\beta C_2^1 C_2^0 \end{cases} \tag{9}$$

$$\begin{cases} C_{13} = C_2^2 \\ C_{23} = -C_1^2 - C_2^2 C_3^0 - C_2^1 C_3^1 \frac{\Gamma(2q+1)}{\Gamma^2(q+1)} - C_2^0 C_3^2 \\ C_{33} = C_1^2 C_2^0 + C_1^1 C_2^1 \frac{\Gamma(2q+1)}{\Gamma^2(q+1)} + C_1^0 C_2^2 + 2\alpha C_1^2 C_1^0 + \alpha C_1^1 C_1^1 \frac{\Gamma(2q+1)}{\Gamma^2(q+1)} \\ \quad +2\beta C_2^2 C_2^0 + \beta C_2^1 C_2^1 \frac{\Gamma(2q+1)}{\Gamma^2(q+1)} \end{cases} \tag{10}$$

$$\begin{cases} C_{14} = C_2^3 \\ C_{24} = -C_1^3 - C_2^3 C_3^0 - (C_2^2 C_3^1 + C_2^1 C_3^2) \frac{\Gamma(3q+1)}{\Gamma(q+1)(2q+1)} - C_2^0 C_3^0 \\ C_{34} = C_1^3 C_2^0 + (C_1^1 C_2^2 + C_1^2 C_2^1) \frac{\Gamma(3q+1)}{\Gamma(q+1)(2q+1)} + C_1^0 C_2^3 + 2\alpha C_1^3 C_1^0 \\ \quad +2\alpha C_1^2 C_1^1 \frac{\Gamma(3q+1)}{\Gamma(q+1)(2q+1)} + 2\beta C_2^3 C_2^0 + 2\beta C_2^1 C_2^2 \frac{\Gamma(3q+1)}{\Gamma(q+1)(2q+1)} \end{cases} \tag{11}$$

$$\begin{cases} C_{15} = C_2^4 \\ C_{25} = -C_1^4 - C_2^4 C_3^0 - C_2^2 C_3^2 \frac{\Gamma(4q+1}{\Gamma^2(2q+1)} - (C_2^3 C_3^1 + C_2^1 C_3^3) \frac{\Gamma(4q+1)}{\Gamma(q+1)(3q+1)} \\ \quad -C_2^0 C_3^4 \\ C_{35} = C_1^4 C_2^0 + (C_1^3 C_2^1 + C_1^1 C_2^3) \frac{\Gamma(4q+1)}{\Gamma(q+1)(3q+1)} + C_1^2 C_2^2 \frac{\Gamma(4q+1}{\Gamma^2(2q+1)} + C_1^0 C_2^4 \\ \quad +2\alpha C_1^4 C_1^0 + \alpha C_1^2 C_1^2 \frac{\Gamma(4q+1}{\Gamma^2(2q+1)} + 2\alpha C_1^1 C_1^3 \frac{\Gamma(4q+1)}{\Gamma(q+1)(3q+1)} + 2\beta C_2^4 C_2^0 \\ \quad +\beta C_2^2 C_2^2 \frac{\Gamma(4q+1}{\Gamma^2(2q+1)} + 2\beta C_2^1 C_2^3 \frac{\Gamma(4q+1)}{\Gamma(q+1)(3q+1)} \end{cases} \tag{12}$$

Selecting the system parameters $\alpha = 0.5$, $\beta = 0.1$, $\gamma = 1.3$ and $q = 0.67$, iteration time step $h = 0.01$, the initial values are $[x_0, y_0, z_0]$ = [0, 0.1, 0]. The phase diagrams of fractional-order no-equilibrium system in different planes are plotted in Fig. 1, the corresponding Lyapunov exponents of the system are $\mathrm{LE}_1 = 0.2306$, $\mathrm{LE}_2 = 0$, $\mathrm{LE}_3 = -13.676$, and Lyapunov dimension $D_L = 2.0167$. Since there is only one Lyapunov exponent greater than 0, it means that the system is chaotic [6, 34], and the calculated maximum Lyapunov exponent of the system is positive, indicating that the system is in a chaotic state.

It is obtained from reference [40] that the Lyapunov exponent of an integer-order no-equilibrium chaotic system is $\mathrm{LE}_1 = 0.0453$, $\mathrm{LE}_2 = 0$, $\mathrm{LE}_3 = -3.2903$. The analysis shows that when the order q is a fraction, the maximum Lyapunov exponent of the system obtained is far much larger than the integer order system, the chaotic performance of the fractional-order no-equilibrium system has been greatly improved compared with the integer-order system, so the fractional-order no-equilibrium chaotic system has more complex dynamic characteristics, the system is more suitable for image encryption.

2.3 Equilibrium point analysis

The equilibrium point of the system can be found by making the equation of fractional-order no-equilibrium chaotic system equal to 0, so

$$y = 0 \tag{13}$$

$$-x - yz = 0 \tag{14}$$

$$xy + \alpha x^2 + \beta y^2 - \gamma = 0 \tag{15}$$

2.4 Dynamical characteristics of the fractional-order no-equilibrium chaotic system

The parameters are set to $\alpha = 0.5$, $\beta = 0.1$, $\gamma = 1.3$, $h = 0.01$, the initial values $x_0 = [0, 0.1, 0]$, when the order $q \in [0.45, 1]$, the LEs and bifurcation diagram of the system are presented in Fig. 2. The bifurcation trajectory enters chaotic state after an obvious

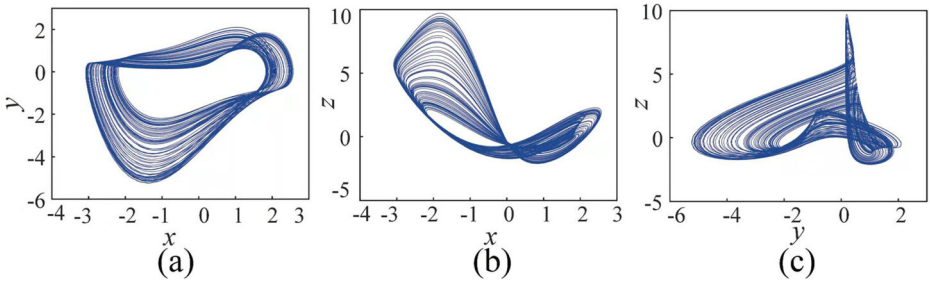

Fig. 1 Chaotic attractor phase diagram (a) $x - y$ plane (b) $x - z$ plane (c) $y - z$ plane

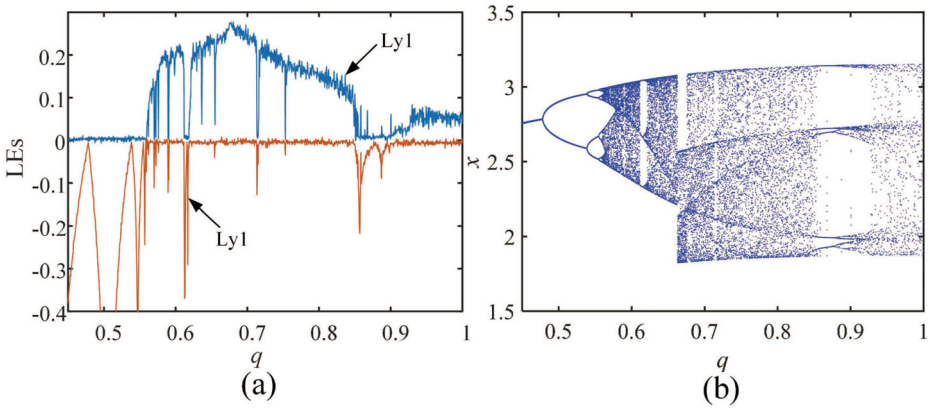

Fig. 2 LEs and bifurcation diagram with order $q \in [0.45, 1]$

period-doubling bifurcation. Besides, the smallest order that can produce chaos is $q = 0.565 \times 3 = 1.695$. A positive Lyapunov exponent indicates that the phase volume of the system continues to expand and fold, causing the originally similar trajectories in the attractors to become increasingly uncorrelated, and the initial value of the system is highly sensitive. It can be seen from Fig. 2 that when $q = 1$, the system is in the form of integer-order, and it can be clearly seen that when $q < 1$, the Lyapunov exponent of the fractional-order chaotic system is significantly higher than that of the integer-order chaotic system, and the initial value of the system is more sensitive.

Fixed $q = 0.67$, $\alpha \in [0.3, 0.7]$, and other parameter values remain unchanged, the LEs and bifurcation diagram are plotted in Fig. 3. From the bifurcation diagram, we can see that the no-equilibrium system has obvious periodic bifurcation and is correspondingly consistent with the Lyapunov exponents. Keeping other parameter values, $\alpha = 0.5$, the LEs and bifurcation diagram of $\beta \in [0, 0.2]$ are shown in Fig. 4. Moreover, setting $\beta = 0.1$, $\gamma \in [1.1, 1.5]$, and other parameter values remain unchanged, the corresponding LEs and bifurcation diagram are presented in Fig. 5. When the order q is a fraction, the maximum LE of the system is much larger than the integer order. Obviously, the dynamical characteristics of the

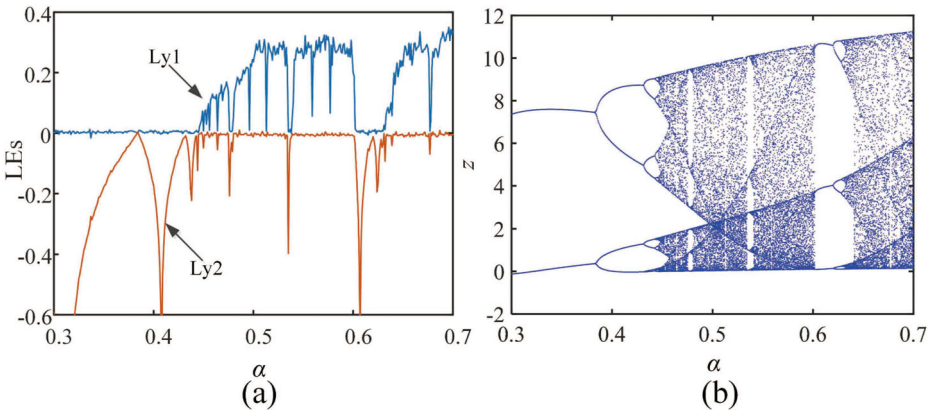

Fig. 3 LEs and bifurcation diagram with parameter $\alpha \in [0.3, 0.7]$

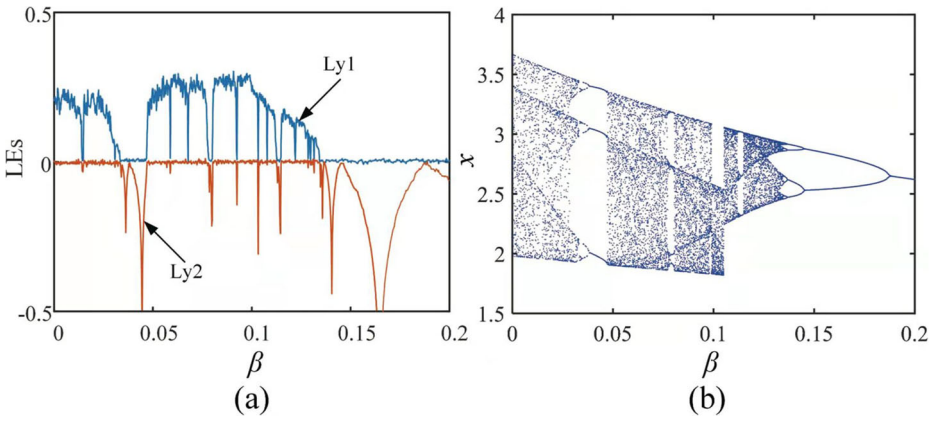

Fig. 4 LEs and bifurcation diagram with parameter $\beta \in [0, 0.2]$

fractional-order no-equilibrium chaotic system are rich. In addition, we refer to a chaotic system with equilibrium points, whose LES and bifurcation diagram are shown in Fig. 6, and compare its LEs and bifurcation diagram with parameters changing with system 2. It can be seen that when parameters change, the LEs value of system 2 is larger than that of reference [42], so the randomness of the system is better.

2.5 Complexity analysis

When chaotic sequences are applied to chaotic secure communication or image encryption, it needs to have high randomness and strong complexity. The LEs and bifurcation diagram can qualitatively analyze the dynamical characteristics of the system, but cannot quantitatively reflect the randomness and complexity of the chaotic sequences. Therefore, spectral entropy (SE) and C_0 complexity algorithms are adopted to analyze the complexity and randomness of fractional-order no-equilibrium system. Taking the system parameters $\beta = 0.1$, $\gamma = 1.3$, $h = 0.01$, and the initial condition is [0, 0.1, 0]. According to the spectral entropy

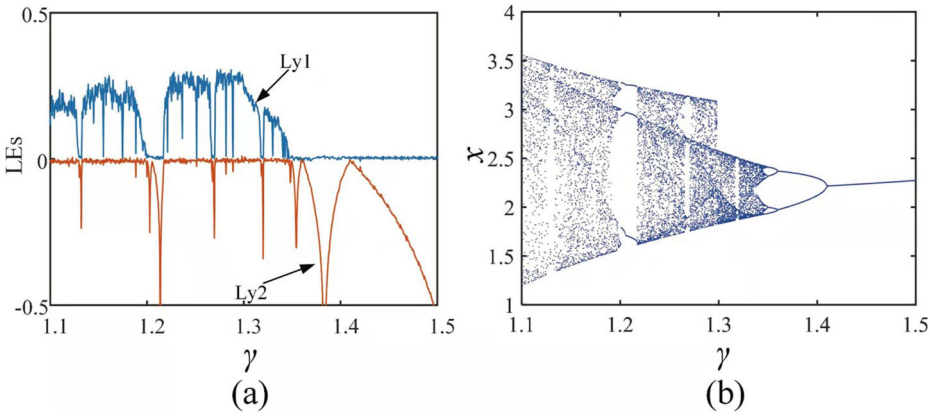

Fig. 5 LEs and bifurcation diagram with parameter $\gamma \in [1.1, 1.5]$

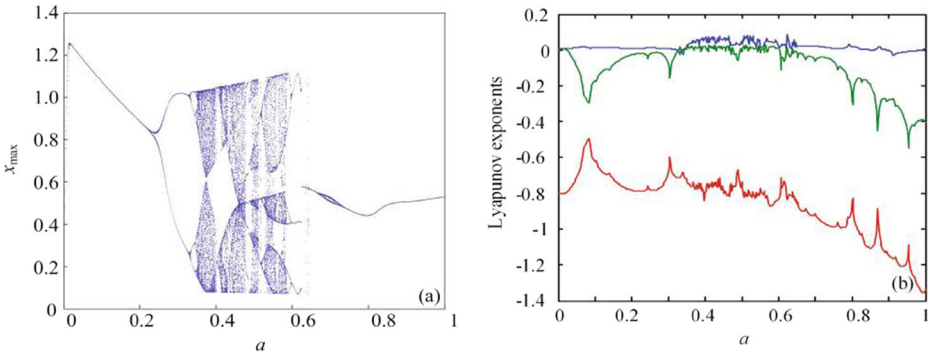

Fig. 6 LEs and bifurcation diagram of reference [42]

(SE) and C_0 complexity algorithm, the complexity of the fractional-order no-equilibrium chaotic system when the order q and the parameter α change simultaneously are calculated as shown in Fig. 7a and b. Different colors indicate different complexity, the lighter the color, the smaller the complexity values in the interval, the worse the randomness of the sequences. The greater the complexity of the chaotic sequence and the greater its randomness, the more difficult it is for the sequence to be recovered. It can be seen from Fig. 7 that when $q = 1$, the system is in the form of integer-order, the color in this range is the lightest and the complexity is the lowest. When $0.45 < q < 0.8$, the darker the color, the greater the complexity. Compared with the integer-order system, fractional-order no-equilibrium chaotic system is more suitable for image encryption systems.

Setting $\alpha = 0.5$, $q = 0.67$, other parameter values remain unchanged, and the SE complexity and C_0 complexity of the system when the parameters β and γ change at the same time are illustrated in Fig. 8a and b. It can be seen from the figure that when $0.63 < \alpha < 0.7$, $0.45 < q < 0.53$, $0.09 < \beta < 0.2$, $1.2 < \gamma < 1.35$, the color is the darkest, the complexity and randomness of the system are the best. Therefore, when the system is applied to image encryption, the chaotic sequences in this area should be selected.

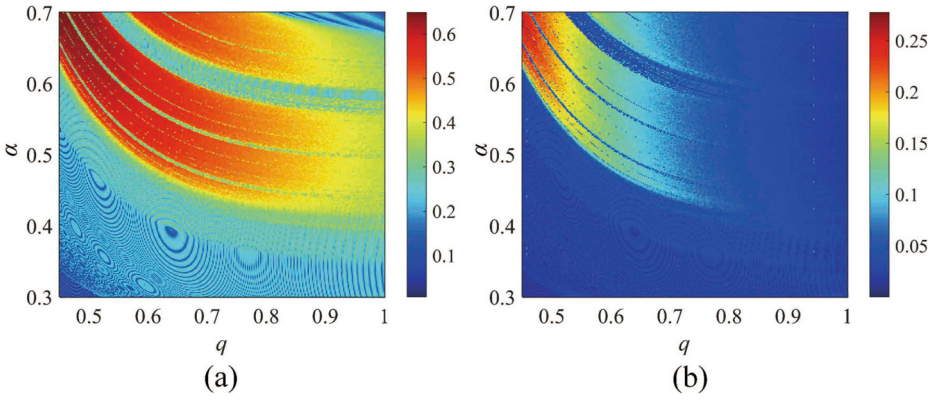

Fig. 7 The complexity of $\alpha \in [0.3, 0.7]$, $q \in [0.45, 1]$: (a) SE complexity (b) C_0 complexity

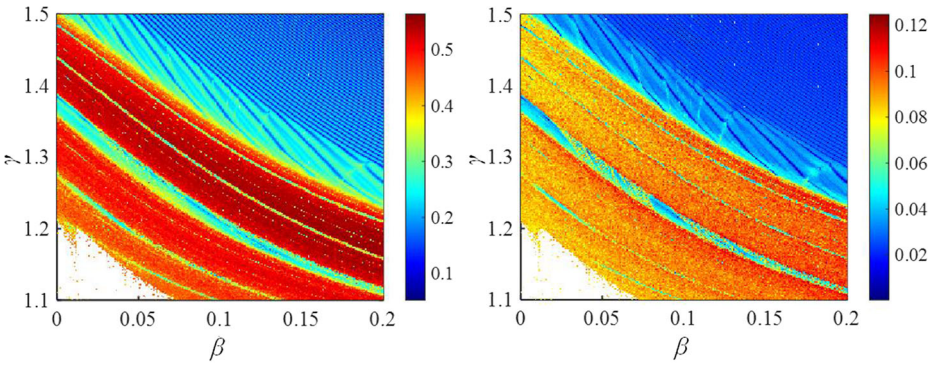

Fig. 8 The complexity of $\beta \in [0, 0.2]$, $\gamma \in [1.1, 1.5]$: (a) SE complexity (b) C_0 complexity

2.6 Attractor basin

The dynamic map reflects the state information of the chaotic attractor, which can provide an effective parameter selection basis for the application of the chaotic system in engineering. Setting iteration time step $h = 0.01$ initial values $x_0 = [0, 0.1, 0]$. The attractor basin of the q-α plane when $\beta = 0.1$, $\gamma = 1.3$ is shown in Fig. 9a, and the attractor basin of the β-γ plane when $\alpha = 0.65$, $q = 0.47$ is plotted in Fig. 9b. It can be clearly seen from Fig. 9a that there are yellow and red parts, which represent the limit cycle and chaotic state, respectively. In Fig. 9b, there are yellow, orange and blue, which are limit cycles, chaotic states and divergence state, respectively. When applying the chaotic system to secure communication, the red and orange area should be selected. In addition, the attractor state may jump at the boundary point, so the boundary point of each area should be carefully selected.

2.7 DSP implementation of fractional-order no-equilibrium chaotic system

DSP digital signal processor has the advantages of good stability, high precision, strong programmability, and easy implementation. Therefore, the DSP platform implements digital

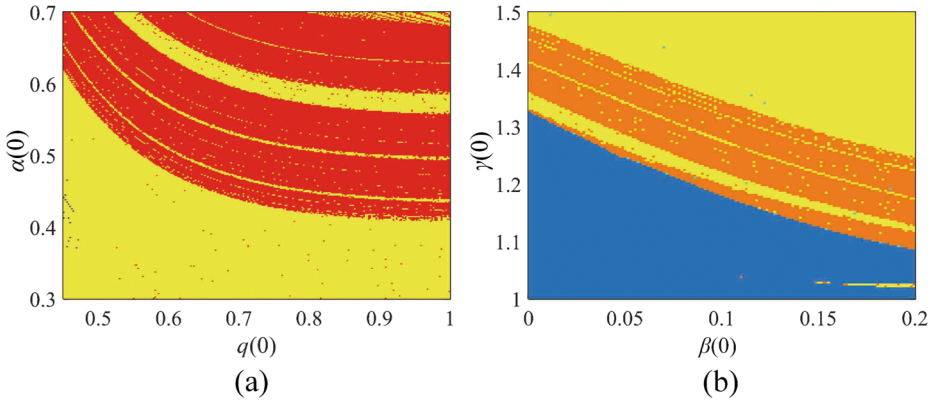

Fig. 9 Attractor basin (a) $\alpha \in [0.3, 0.7]$, $q \in [0.45, 1]$ (b) $\beta \in [0, 0.2]$, $\gamma \in [1, 1.5]$

hardware implementation of the fractional-order no-equilibrium chaotic system. The hardware realization platform is illustrated in Fig. 10. Here the DSP chip is TMS320F28335, and the time series generated by DSP is converted by 16-bit dual-channel D/A converter DAC8552 [11, 29, 31]. Letting $\alpha = 0.5$, $\beta = 0.1$, $\gamma = 1.3$, $q = 0.67$, and $h = 0.01$, the initial values $x_0 = [0, 0.1, 0]$, Fig. 11a–c show the phase diagram of the fractional-order no-equilibrium chaotic map captured by the oscilloscope, which are the same as the computer simulation results.

3 Application of fractional-order no-equilibrium chaotic system in image encryption

3.1 Encryption algorithm

A color image encryption algorithm based on the fractional-order no-equilibrium chaotic system is introduced in this section. The algorithm divides the color image into R, G, B three channels, which are performed: DCT sparse transformation, scrambling algorithm, and diffusion algorithm based on GF (257) domain. The encryption scheme for an image of size $N*N$ ($N = 256$) is shown in Fig. 12, and the specific steps are as follows:

Step 1: Input the original color image I with a size of $N \times N$ and decompose it into R (red), G (green), B (blue) three-channel images.

Step 2: The sparse coefficient matrices R_1, G_1 and B_1 are got by using the discrete cosine transform (DCT) to sparse the R, G, B three-channel pixel matrices.

Step 3: The fractional-order no-equilibrium chaotic system is iterated L ($L = m+s$) times to obtain three chaotic sequences, the sequence x is quantized by (16), which is discarded first s items to get a pseudo-random sequence X of length m. Moreover, the elements of X are sorted in descending order to obtain the index sequence S.

$$x(i) = mod(floor((x(i) + abs(x(i))) * 10^{16}), 256) + 1 \tag{16}$$

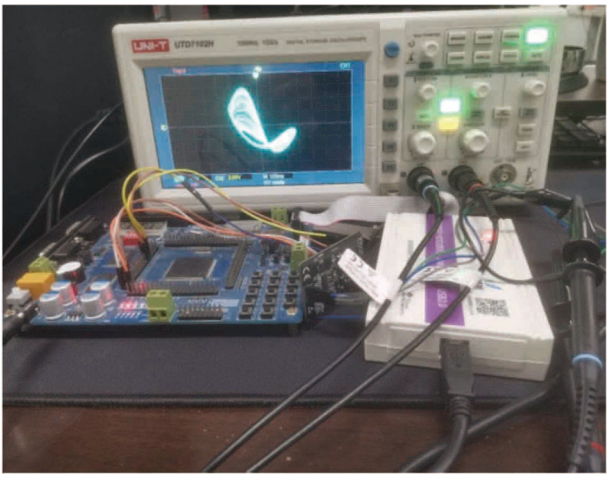

Fig. 10 DSP implementation platform

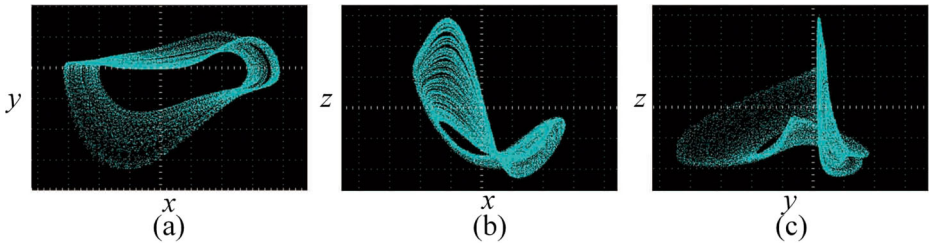

Fig. 11 Phase diagram realized by DSP platform (a) $x - y$ plane (b) $x - z$ plane (c) $y - z$ plane

Step 4: According to sequence S and the Hadamard matrix of $N \times N$, determine the measurement matrix ϕ of $m \times N$. The Hadamard matrix is generated by

$$\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \tag{17}$$

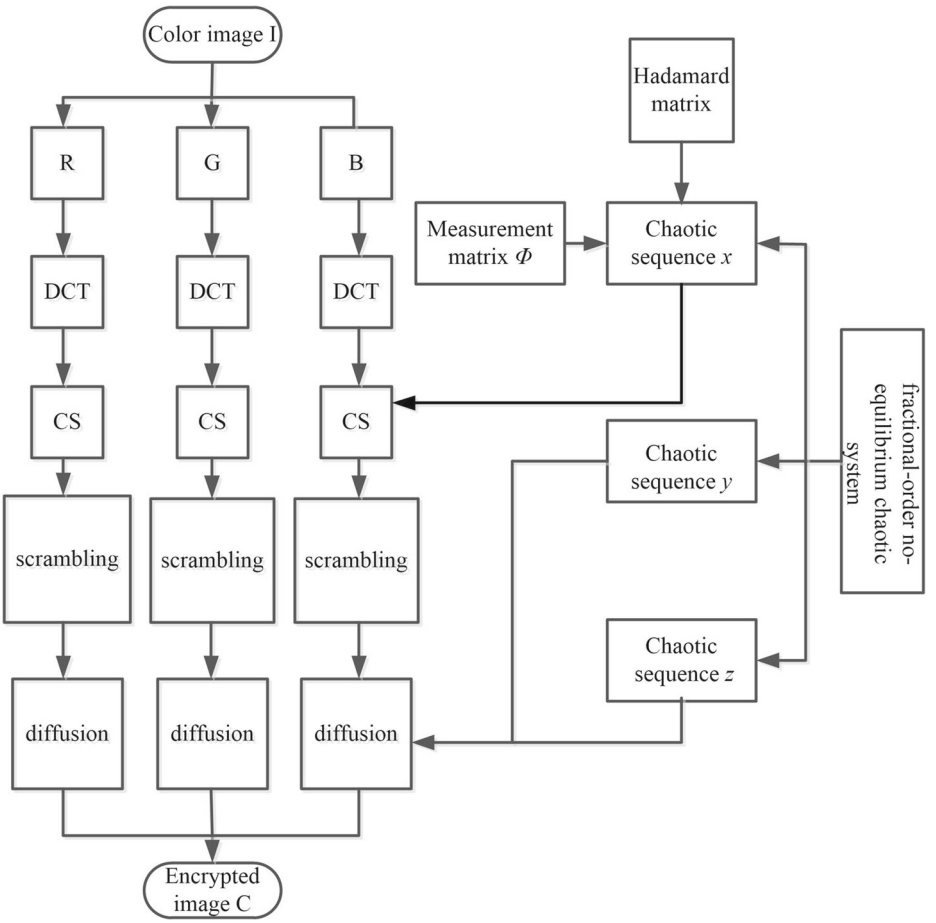

Fig. 12 Encryption flow chart

Step 5: According to (18), the three-channel sparse coefficient matrices of R_1, G_1 and B_1 are compressed and sampled to obtain the compressed image pixel matrices R_2, G_2 and B_2 of $m \times m$.

$$\begin{cases} R_2 = \Phi(\Phi R_1)' \\ G_2 = \Phi(\Phi G_1)' \\ B_2 = \Phi(\Phi B_1)' \end{cases} \tag{18}$$

Step 6: The element values of matrices R_2, G_2 and B_2 are quantized to an integer in the range of 0-255 by (19).

$$\begin{cases} R_3 = round(255 * (C11 - Min(R_2))/(Max(R_2) - Min(R_2))) \\ G_3 = round(255 * (C11 - Min(G_2))/(Max(G_2) - Min(G_2))) \\ B_3 = round(255 * (C11 - Min(B_2))/(Max(B_2) - Min(B_2))) \end{cases} \tag{19}$$

Step 7: Scrambling of the pixel matrix. Flip the odd-numbered column elements of the matrices R_3, G_3, B_3 and then generate a non-repetitive random integer sequence M with a length of m and values between 1 and m, which scrambles the rows of the three-channel pixel matrices.

Step 8: Set the parameters and initial values of the chaotic system (2), and then the system iterates $t+2\times m\times m$ times, where t is generated by the three-channel pixel matrices R, G, B. According to (20) and (21), pseudo-random sequences X, Y are generated from chaotic sequences y and z. The pseudo-random sequences $S1$ and $S2$ of forward diffusion and reverse diffusion are obtained by X and Y, respectively.

$$\begin{cases} X = mod(floor(abs(y) * 10^{16}), 256) \\ Y = mod(floor(abs(z) * 10^{16}), 256) \end{cases} \tag{20}$$

$$\begin{aligned} S1 &= X(1 : m \times m) \\ S2 &= Y(1 : m \times m) \end{aligned} \tag{21}$$

Step 9: The multiplication table of GF (257) domain can be generated by the computer. Then, with the help of (22) and (23), the scrambled R, G, B three-channel pixel matrices are diffused.

$$\begin{cases} C_{i,H} = C_{i-1,H} \times S_{i,H} \times I_{i,H}, C_{i,L} = C_{i-1,L} \times S_{i,L} \times I_{i,L} \\ C = (C_{i,H} \times 16 + C_{i,L}) \end{cases} \tag{22}$$

$$\begin{cases} C_{i,H} = C_{i+1,H} \times S_{i,H} \times I_{i,H}, C_{i,L} = C_{i+1,L} \times S_{i,L} \times I_{i,L} \\ C = (C_{i,H} \times 16 + C_{i,L}) \end{cases} \tag{23}$$

in which, (22) and (23) are the forward diffusion process and the reverse diffusion process, respectively. I represents one-dimensional vector of the pixel matrix. C and S are cryptographic vectors, initial values C_0 comes from the secret key (i = 1, 2, 3, ..., $m \times m$), H is the upper 4 bits of the data, and L represents the lower 4 bits of the data.

Step 10: Integrate the three-channels of R, G, and B the encrypted image C is obtained.

3.2 Decryption algorithm

As shown in Fig. 13, the decryption process of the color image can be realized by the reverse operation encryption process. It is worth mentioning that the OMP algorithm realizes the reconstruction of the image. The specific decryption steps are as follows:

Step 1: Dividing the encrypted image C into three-channels of R, G, and B. The pseudo-random sequence $S1$, $S2$ generated by step 8 of the encryption algorithm performs

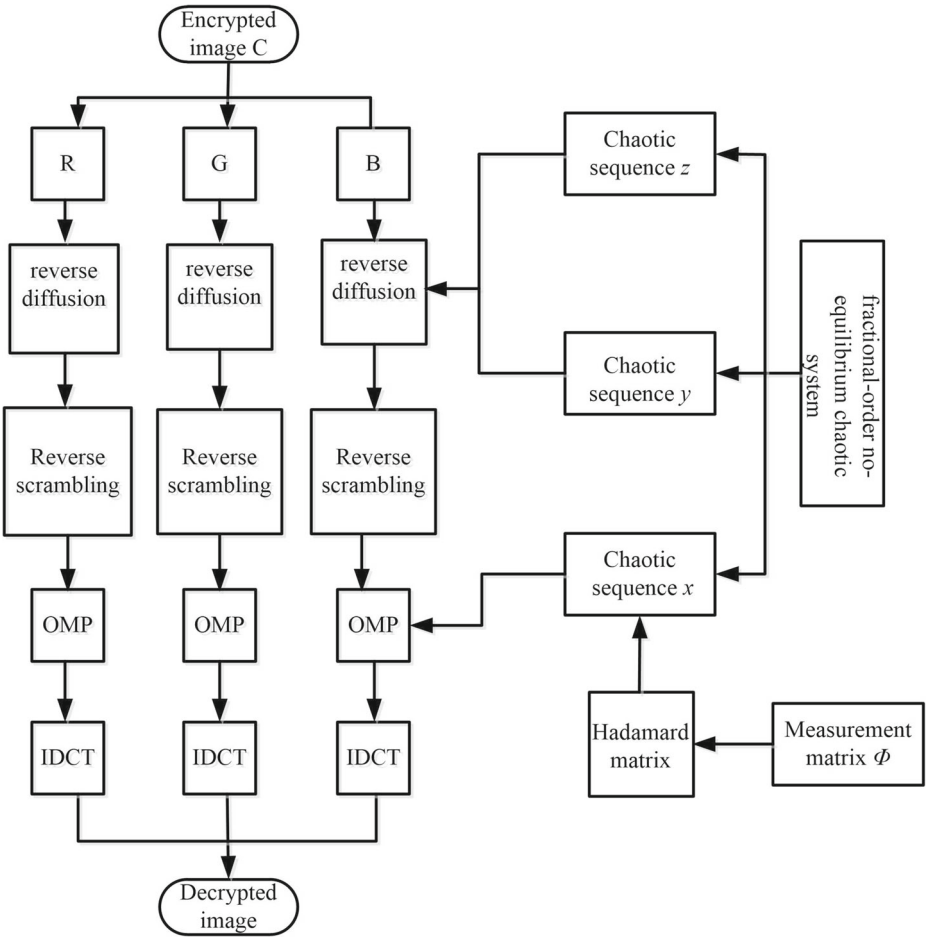

Fig. 13 The architecture of decryption algorithm

inverse diffusion processing in the GF (257) domain on pixel matrices of each channel. The diffusion processes are

$$\begin{cases} I_{i,H} = C_{i,H} \div C_{i+1,H} \div S_{i,H}, I_{i,L} = C_{i,L} \div C_{i+1,L} \div S_{i,L} \\ I_i = (I_{i,H} \times 16 + I_{i,L}) \end{cases} \tag{24}$$

$$\begin{cases} I_{i,H} = C_{i,H} \div C_{i-1,H} \div S_{i,H}, I_{i,L} = C_{i,L} \div C_{i-1,L} \div S_{i,L} \\ I_i = (I_{i,H} \times 16 + I_{i,L}) \end{cases} \tag{25}$$

Step 2: The M sequence generated by step 7 of the encryption algorithm inversely scrambles the rows of the three-channel pixel matrices, and then flips the odd-numbered column elements of the pixel matrices.

Step 3: Use the OMP algorithm and the measurement matrix generated in step 4 of the encryption algorithm to reconstruct the three-channel planar sparse pixel matrices with a size of $N \times N$.

Step 4: The three-channel pixel matrices of the decrypted image are got by inverse discrete cosine transform (IDCT), which are combined to get the decrypted image.

4 Encryption simulation results and performances analysis

4.1 Experimental results

To verify the reliability and security of the algorithm, we encrypt the four different 512×512 color images and four different 256×256 color images. The chaotic system parameters are $\alpha = 0.65$, $\beta = 0.1$, $\gamma = 1.3$, $q = 0.47$, $h = 0.01$, initial values $[x_0, y_0, z_0] = [0, 0.1, 0]$, $CR = 0.75$, the encryption and decryption algorithms have the same key. The compression ratio CR is calculated by

$$CR = \frac{C_{\text{heigt}} \times C_{\text{width}}}{I_{\text{heigt}} \times I_{\text{width}}} \tag{26}$$

here I is plain image, C is encrypted image. The original 512×512 color images "4.1.03", "4.1.04", "House" and "Airplane" are shown in Fig. 14a, the encrypted images are illustrated in Fig. 13b, the corresponding decrypted images are in Fig. 14c. Figure 15a plotted the original 256×256 color images "Lena", "Pepper", "Barbara" and "Fruits", the encrypted images are in Fig. 15b, and the corresponding decrypted images are shown in Fig. 15c. From Figs. 14b and 15b, the compressed and encrypted images are obviously smaller than the corresponding original image, and the cipher images completely change the characteristics of the plaintext images. The encryption scheme can reduce the network transmission pressure and carry out safe transmission. In addition, the decrypted images shown in Figs. 14c and 15c are basically the same as their corresponding original images. The algorithm has good

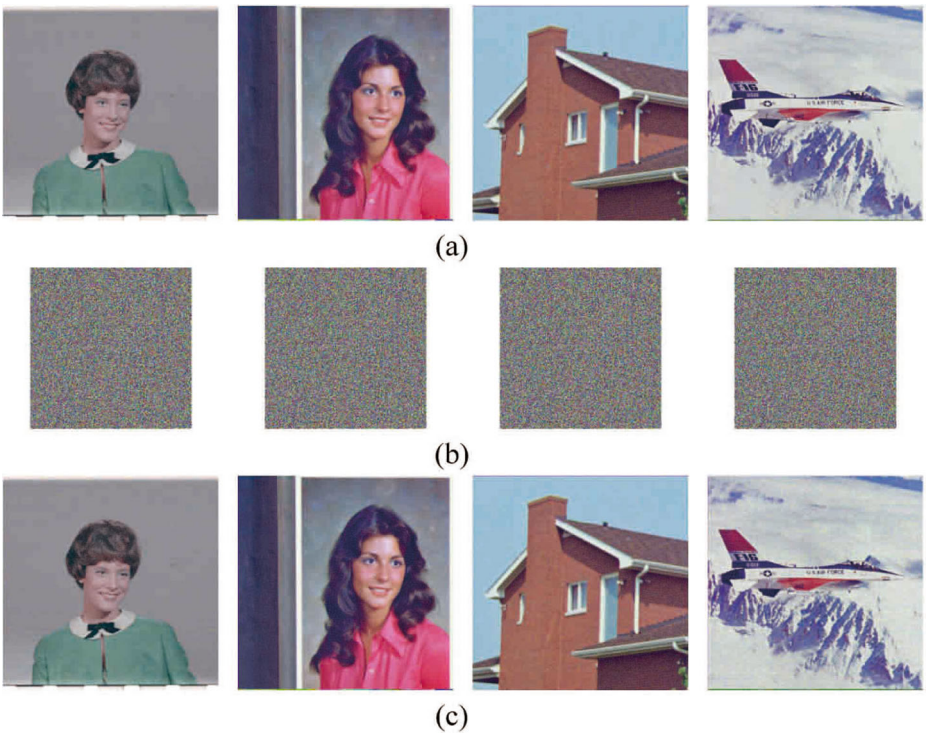

Fig. 14 Simulation results of 512×512 color images"4.1.0", "4.1.04", "House" and "Airplane" (a) original color images (b) encrypted images (c) decrypted images

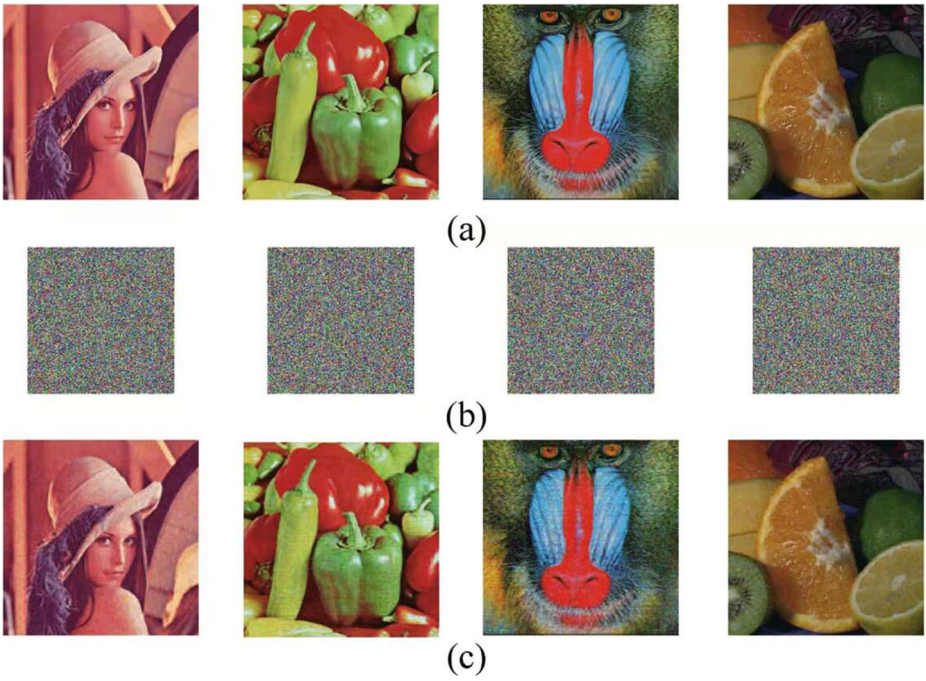

Fig. 15 Simulation results of 256×256 color images"Lenna", "Pepper", "Barbara" and "Fruits" (**a**) original color images (**b**) encrypted images (**c**) decrypted images

encryption and decryption effects. Selecting the color image Lena with a size of 256×256, and divide it into three channels of R, G, B, the encryption and decryption process flow chart as shown in Fig. 16.

4.2 The compression ratio analysis

In this subsection, the mean structural similarity (MSSIM) and peak signal to noise ratio (PSNR) are adopted to evaluate image compression performance with different compression rates.

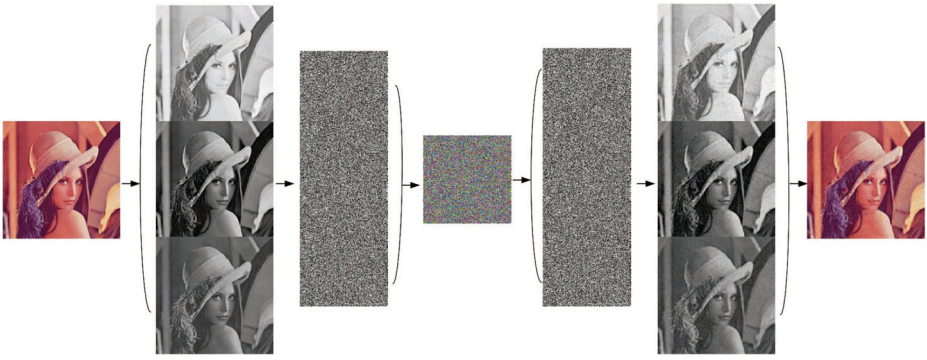

Fig. 16 Lena image is divided into R, G, B three-channel encryption and decryption process

4.2.1 Mean structural similarity (MSSIM)

The mean structural similarity (MSSIM) is an index to evaluate the similarity of two images, which is defined as

$$L(x, y) = \frac{2u_x u_y + (K_1 \times L)^2}{u_x^2 + u_y^2 + (K_1 \times L)^2} \tag{27}$$

$$C(x, y) = \frac{2\sigma_x \sigma_y + (K_2 \times L)^2}{\sigma_x^2 + \sigma_y^2 + (K_2 \times L)^2} \tag{28}$$

$$S(x, y) = \frac{\sigma_{xy} + (K_2 \times L)^2/2}{\sigma_x \sigma_y + (K_2 \times L)^2 2} \tag{29}$$

$$\mathrm{SSIM}(x, y) = L(x, y) \times C(x, y) \times S(x, y) \tag{30}$$

$$\mathrm{MSSIM}(x, y) = \frac{1}{M} \sum_{k=1}^{M} \mathrm{SSIM}(x_k, y_k) \tag{31}$$

where x is the original color image and y is the decrypted image. u_x , u_y, σ_x, σ_y are the mean, variance values of x and y, respectively. and σ_{xy} represents the covariance of x and y. The parameters are as follows: $K_1 = 0.01$, $K_2 = 0.03$, $L = 255$ and $M = 64$.

Table 1 lists the MSSIM values of each channel of 256×256 color images at different compression ratios. From Table 1, the MSSIM values of different images are similar at the same compression ratios, so the proposed algorithm is stable. When the compression ratio changes, the values of MSSIM will change accordingly, so images can be effectively compressed and encrypted according to different actual needs.

Table 1 MSSIM values of different images at different CRs

Images	Channel	0.25	0.5	0.75
Lena	R	0.6235	0.8014	0.7169
	G	0.5741	0.7642	0.6689
	B	0.6540	0.7996	0.6989
Pepper	R	0.6490	0.7109	0.7233
	G	0.5898	0.7320	0.6582
	B	0.6542	0.7226	0.7500
Barbara	R	0.5224	0.8159	0.6300
	G	0.5517	0.7593	0.6483
	B	0.5402	0.8248	0.6496
Fruits	R	0.6732	0.8193	0.7495
	G	0.6096	0.7785	0.6915
	B	0.5012	0.6745	0.6477

4.2.2 Peak signal to noise ratio (PSNR)

Peak signal to noise ratio is an important indicator to judge the ability of image reconstruction, which calculation is as follows:

$$\mathrm{PSNR} = 10 \times \log_{10}\left(\frac{255^2}{(1/H \times W)\sum_{i=1}^{H}\sum_{j=1}^{W}(L(i,j) - l(i,j))^2}\right) \tag{32}$$

here $L(i, j)$ is the decrypted image and $l(i, j)$ is the original image. H and W represent the length and width of the image. Table 2 shows the PSNR values of each channel of 256×256 color images at different compression ratios. It can be seen that even if there is very little information sampled at $CR = 0.25$, the values of PSNR are close to 30, so the image reconstruction effect is better and is beneficial to transmission.

4.3 Key space

The sum of the keys in the image encryption process is the key space, which is a necessary condition for measuring the encryption scheme. In order to resist brute force attack, the key space should be greater than 2^{100}. In the proposed method, if the calculation accuracy is 10^{-15}, the key space is $(10^{15})^9 = 10^{135} \approx 2^{448}$. Moreover, considering the key t related to the plaintext, the key of the algorithm is$>2^{448}$, which is large enough to resist brute force attacks. Under the same encryption algorithm and calculation precision, the key space of the integer-order no-equilibrium chaotic system is 2^{398} [40], which is smaller than that of the fractional-order chaotic system. In contrast, fractional-order no-equilibrium chaotic systems is more suitable for image encryption system.

4.4 Key sensitivity

Key sensitivity analyzes the difference between two cipher images got when the same plain image is encrypted with a slight change in the key. If the two cipher images are significantly different, the key sensitivity of cryptographic system is extreme. If the difference between

Table 2 PSNR values of different images at different CRs

Images	Channel	0.25	0.5	0.75
Lena	R	30.9433	33.9007	32.8822
	G	30.3003	32.6915	31.6604
	B	31.7238	34.3102	33.0332
Pepper	R	31.2489	34.5650	33.1666
	G	29.8887	32.5430	31.4032
	B	30.5915	34.1997	33.3982
Barbara	R	29.7470	31.0011	30.3063
	G	29.9549	31.4833	30.6977
	B	29.7540	31.2852	30.6075
Fruits	R	32.6814	35.7249	34.4416
	G	31.5458	34.1925	32.8927
	B	29.8284	31.5178	30.4616

the two cipher images is small, the key sensitivity of the cryptographic system is weak. An excellent cryptographic system should be sufficiently sensitive to all secret keys. In this test, the"Peppe" image is used as the test image, and the original image and the encrypted image C with the correct key are displayed in Fig. 17a and b, The secret key is changed to $\alpha+10^{-15}$, $\beta+10^{-15}$, $\gamma+10^{-15}$, $h+10^{-15}$, $q+10^{-15}$, $m+10^{-15}$, x_0+10^{-15}, y_0+10^{-15}, z_0+10^{-15}, the new encrypted images are C1, C2, C3, C4, C5, C6, C7, C8, C9, which are shown in Fig. 17c–k, The differences between the original cipher image and the new cipher images are represented in Fig. 17l–t. The test results show that when the key is slightly changed, the two cipher images got by encrypting the same plain image are significantly different. So the key of the proposed algorithm is sufficiently sensitive.

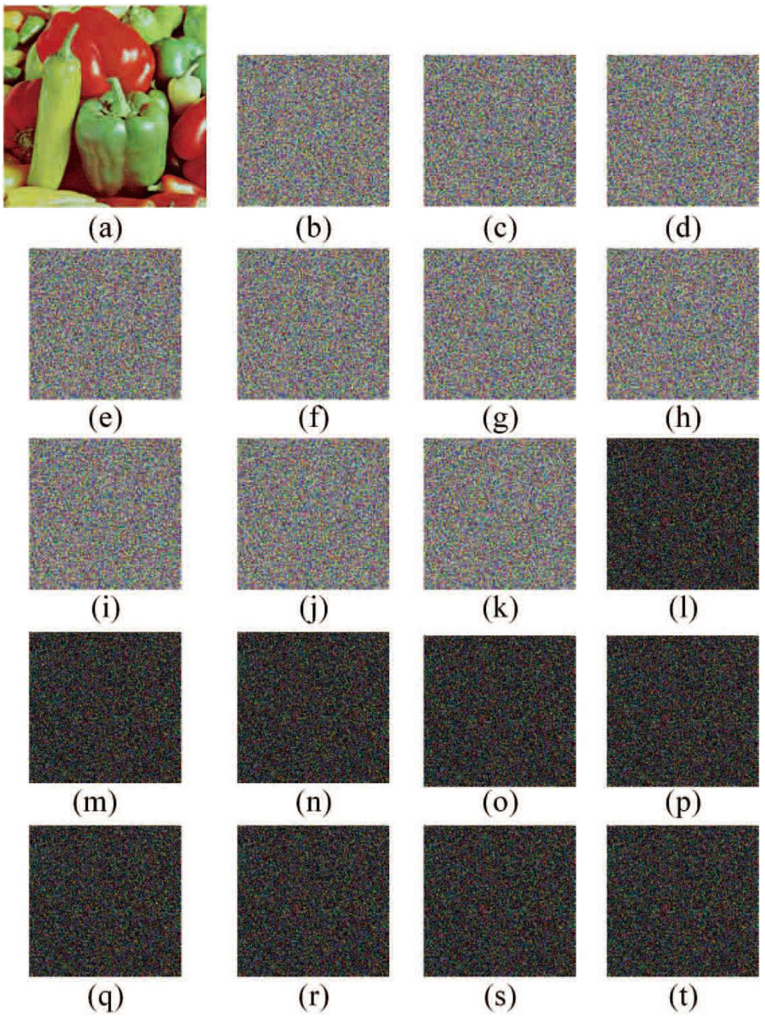

Fig. 17 Key sensitivity analysis results (a) Original "Pepper" image (b) Cipher image C (c) Cipher image C1 (d) Cipher image C2 (e) Cipher image C3 (f) Cipher image C4 (g) Cipher image C5 (h) Cipher image C6 (i) Cipher image C7 (j) Cipher image C8 (k) Cipher image C9 (l) |C-C1| (m) |C-C2| (n) |C-C3| (o) |C-41| (p) |C-C5| (q) |C-C6| (r) |C-C7| (s) |C-C8| (t) |C-C9|

4.5 Statistical analysis

4.5.1 Histogram analysis

The histogram is a statistical table reflecting the pixel distribution of an image. The cipher image should disrupt the statistical characteristics of the plain image to prevent an attacker from obtaining effective statistical information. Figure 18 draws the histogram of the plain image and the cipher image of "Lena". In this test, the pixel value distribution of the histogram of the encrypted image is uniform. Compared with the histogram of the original image, the encrypted image completely changes the statistical characteristics of the original image. On the other hand, χ^2-values statistics are usually used to show the uniformity of the image histogram, Table 3 lists the χ^2-values of different images. From the χ^2-values in Table 3, we can see that the cipher images are uniformly distributed.

4.5.2 Correlation analysis

The adjacent pixel correlation coefficient is a performance index for evaluating the cryptographic system, and it reflects the correlation between adjacent pixels. The closer the correlation coefficient is to 0, the better the cryptographic system. The correlation of adjacent pixels can be reduced by an effective encryption algorithm. The correlation coefficient is calculated by

$$\begin{cases} \rho_{uv} = \frac{\mathrm{cov}(u,v)}{\sqrt{D(u)}\sqrt{D(v)}} \\ \mathrm{cov}(u,v) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(u))(y_i - E(v)) \\ D(u) = \frac{1}{N}\sum_{i=1}^{N}(u_i - E(u))^2 \\ E(u) = \frac{1}{N}\sum_{i=1}^{N}u_i \end{cases} \tag{33}$$

where u, v, are the gray values of two adjacent pixels

Randomly select 2000 pixel pairs and measure the correlation coefficients in the horizontal, vertical, and diagonal directions. Figure 19 depicts the correlation of adjacent pixels of different images in various directions, and Table 4 lists the correlation coefficients of adjacent pixels of different images. For original images, the correlation coefficients of adjacent pixels are close to 1, which has a powerful correlation. After encryption, the correlation coefficients of adjacent pixels in all directions are close to 0, it indicates that adjacent pixels have almost no correlation. In addition, it can be seen from Fig. 19 that the encryption algorithm breaks the correlation between adjacent pixels in all directions. Table 5 compares the correlation coefficients between the proposed scheme and other schemes. From the results, the encrypted image in this paper has less correlation than other schemes in all directions.

4.6 Information entropy

We analyze the randomness of color images through information entropy. For an image with 256 gray values, the closer the entropy value is to 8, the stronger the randomness of the image information, the amount of understood image information is less. We calculated the information entropy of different images and their corresponding encrypted images, and listed calculation results in Table 6. Moreover, Table 6 shows the information entropy of each channel. The information entropy values of the cipher images are closer to 8 than

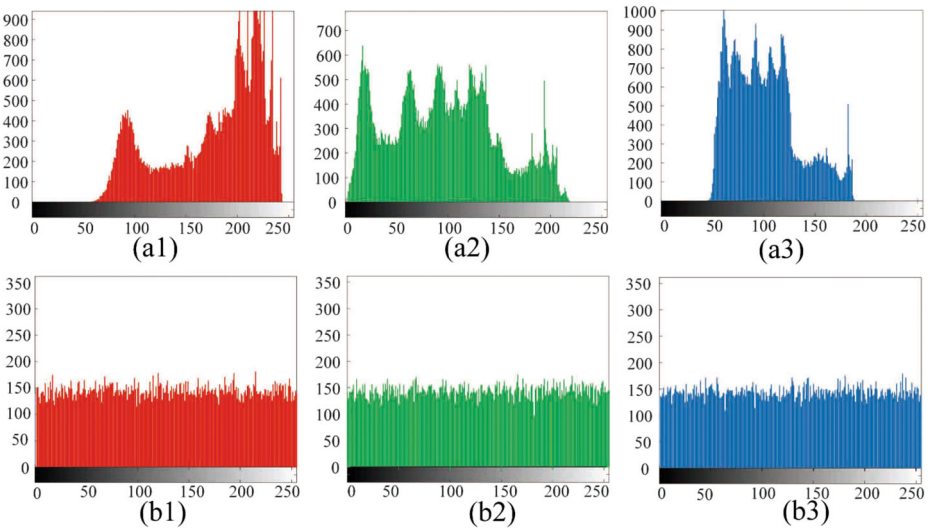

Fig. 18 Histogram of original image and encrypted image (a1) R channel of the original image (a2) G channel of the original image (a3) B channel of the original image (b1) R channel of the encrypted image (b2) G channel of the encrypted image (b3) B channel of the encrypted image

that of the plain images, so the information leakage of the encrypted image may be very small, which means that the proposed algorithm can resist statistical attacks. The information entropy values of the Lena image under different algorithms are listed in Table 7. It can be seen that compared to other algorithms, the information entropy in this paper is closer to the theoretical value.

4.7 Differential attacks

Generally, NPCR (pixel change rate) and UACI (uniform average change intensity) are used to analyze whether the cryptosystem can resist differential attacks. For two cipher images

Table 3 the χ^2-values of different images

Images	χ^2-values(Plaintext)	χ^2-values(Cipher)	Critical Value		
			$\chi^2_{0.1}(255) =$ 284.33591	$\chi^2_{0.5}(255) =$ 293.24783	$\chi^2_{0.01}(255) =$ 310.45739
Lena	67946.0052	248.2824	pass	pass	pass
Pepper	76396.8255	267.2685	pass	pass	pass
Barbara	63425.6589	210.7222	pass	pass	pass
Fruits	99403.7943	245.1713	pass	pass	pass
4.1.03	5813051.4499	259.7292	pass	pass	pass
4.1.04	407859.7858	259.1840	pass	pass	pass
House	1331300.7513	227.2298	pass	pass	pass
Airplane	2309831.3346	240.8299	pass	pass	pass

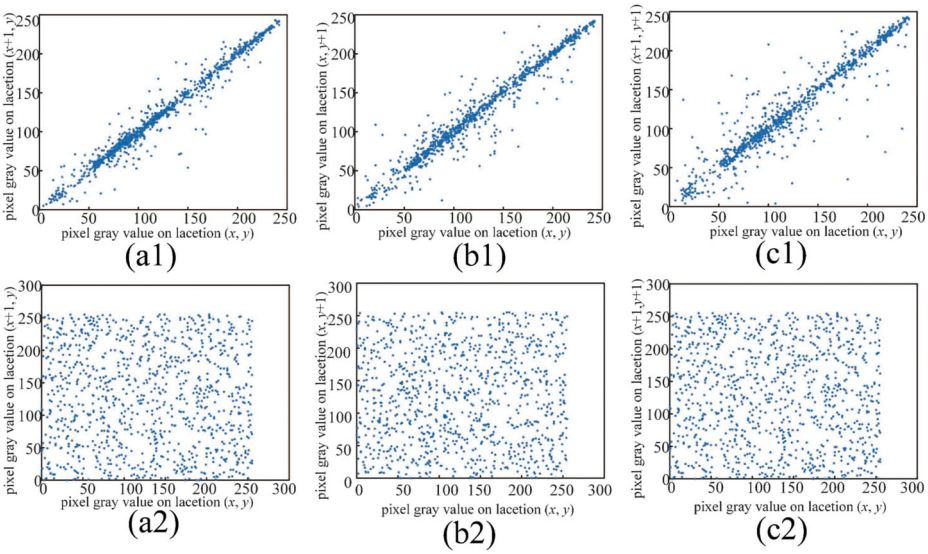

Fig. 19 Correlation analysis (first line is original "Lena" image, second line is encrypted "Lena" image) (a1) and (a2) Horizontal direction (b1) and (b2) Vertical (c1) and (c2) Diagonal

Table 4 Correlation coefficients of different images

	Images	Horizontal	Vertical	Diagonal
Lena	Original image	0.9828	0.9625	0.9476
	Encrypted image	–0.0021	–0.0026	0.0012
pepper	Original image	0.9717	0.9651	0.9392
	Encrypted image	–0.0015	0.0019	0.0008
Barbara	Original image	0.9574	0.9222	0.8894
	Encrypted image	0.0003	–0.0001	–0.0015
Fruits	Original image	0.9690	0.9693	0.9466
	Encrypted image	0.0017	–0.0001	0.0007

Table 5 Compare correlation coefficients with other algorithms

Component(Lena)	Direction	Lena	Ours	[48]	[33]	[7]	[43]
Red	Horizontal	0.9779	0.0054	–0.0131	0.0071	0.0001	–0.0080
	Vertical	0.9559	0.0004	0.0142	0.0009	0.0091	0.000029
	Diagonal	0.9324	0.0001	–0.0044	–0.0043	–0.0023	–0.0086
Green	Horizontal	0.9707	0.0059	–0.0007	–0.0005	–0.0074	0.0039
	Vertical	0.9448	–0.0031	–0.0167	–0.0034	–0.0059	–0.0034
	Diagonal	0.9196	–0.00006	–0.0145	0.0026	0.0015	–0.0044
Blue	Horizontal	0.9573	–0.0038	0.0036	–0.0029	–0.0015	0.0013
	Vertical	0.9271	–0.0014	0.0083	0.0045	–0.0010	0.00053
	Diagonal	0.9012	–0.0002	–0.0214	0.0008	–0.0083	0.0027

Table 6 Information entropy values of different images

Images	Plain			Cipher		
	R	G	B	R	G	B
Lena	7.7147	7.1655	7.5578	7.9950	7.9948	7.9947
Pepper	7.3006	7.5576	7.0996	7.9956	7.9959	7.9953
Barbara	7.6638	7.4477	7.5255	7.9954	7.9952	7.9951
Fruits	7.5071	7.3231	6.7437	7.9950	7.9946	7.9950
4.1.03	5.7010	5.3482	5.6841	7.9987	7.9986	7.9987
4.1.04	7.4335	7.4478	6.9544	7.9981	7.9990	7.9987
House	6.3958	6.5437	6.2161	7.9989	7.9990	7.9988
Airplane	67178	6.7990	6.2138	7.9988	7.9987	7.9989

C1 and C2, whose plain images differ by 1 bit of pixel value, the NPCR and UACI of them are defined by

$$\begin{aligned} \mathrm{NPCR} &= \frac{1}{M\times N}\sum_{i=1}^{M}\sum_{j=1}^{M} E(i,j)\times 100\% \\ \mathrm{UACI} &= \frac{1}{M\times N}\sum_{i=1}^{M}\sum_{j=1}^{M} \frac{|C_1(i,j)-C_2(i,j)|}{255}\times 100\% \end{aligned} \tag{34}$$

where M and N are the size of cipher images, if $C1(i,j) = C2(i,j)$, then $D(i,j) = 0$. Otherwise, $E(i,j) = 1$. The theoretical expectations of NPCR and UACI are 99.6094% and 33.4635%, respectively. A new standards for NPCR and UACI are established by Wu et al. [50]. If the calculated NPCR value is greater than the critical value under the significance level α, the NPCR test passed. The NPCR at significant level α is calculated as

$$\mathrm{NPCR}^{*}_{\alpha} = \frac{H - \Phi^{-1}(\alpha)\sqrt{H/(M\times N)}}{H+1} \tag{35}$$

here H represents the maximum allowable value of image pixel value. For UACI, if the calculated value of UACI is in the interval ($\mathrm{UACI}^{*-}_{\alpha}$,$\mathrm{UACI}^{*+}_{\alpha}$), This represents passing the UACI test.

$$\begin{aligned} \mathrm{UACI}^{*-}_{\alpha} &= \frac{H+2}{3H+3} - \Phi^{-1}\left(\frac{\alpha}{2}\right)\sqrt{\frac{(H+2)(H^2+2H+3)}{18(H+1)^2M\times N\times H}} \\ \mathrm{UACI}^{*+}_{\alpha} &= \frac{H+2}{3H+3} + \Phi^{-1}\left(\frac{\alpha}{2}\right)\sqrt{\frac{(H+2)(H^2+2H+3)}{18(H+1)^2M\times N\times H}} \end{aligned} \tag{36}$$

In this test, randomly select a pixel value of the plain image and modified it. The average test results of UACI and NPCR are listed in Tables 8 and 9, respectively. As we can see, NPCR test values are greater than the critical values, UACI test values are within the theoretical allowable ranges. This shows that the algorithm has passed NPCR and UACI tests and has the ability to resist differential attacks [13]. Table 10 lists the comparison results with

Table 7 Information entropy of image under different algorithms

Schemes	Ours	[14]	[2]	[35]	[36]	[13]
Lena	7.9984	7.9941	7.9985	7.9972	7.9943	7.9951

Table 8 NPCR test values of different images

Images(256×256)	NPCR(%)	Critical value		
		$NPCR^{*}_{0.05} = 99.5693\%$	$NPCR^{*}_{0.01} = 99.5527\%$	$NPCR^{*}_{0.015} = 99.5341\%$
Lena	99.6063	pass	pass	pass
Pepper	99.6130	pass	pass	pass
Barbara	99.6093	pass	pass	pass
Fruits	99.6084	pass	pass	pass
4.1.03	99.6080	pass	pass	pass
4.1.04	99.5981	pass	pass	pass
House	99.6162	pass	pass	pass
Airplane	99.6150	pass	pass	pass

other schemes. From Table 10, our results are closer to the ideal value than other schemes.

4.8 Cropping and noise attack analysis

Generally, color image unavoidably presents with noise interference and data loss in actual encryption and transmission processing. Therefore, the image encryption system is required to have good robustness to resist noise attacks and data loss. In order to evaluate the robust performance of the algorithm, the following tests are performed. The encrypted image is added with salt and pepper noises of 0.001, 0.01, 0.1 and 0.2, and the experimental results are displayed in Fig. 20. Even if there is noise interference, the main information of the original image can be identified by the decryption algorithm, when the noise increases to 0.1 and 0.2, the decrypted images become faintness, but the basic contour of the plain image can still be decrypted. Besides, the encrypted image data is lost 1/16, 1/8, 1/4 and 1/2, and the decrypted images are plotted in Fig. 21. Obviously, the decrypted images can identify most of the main information of the original images. In summary, the proposed algorithm is robust against noise interference and data loss, and is suitable for practical applications.

Table 9 UACI test values of different images

Images(256×256)	UACI(%)	Critical value		
		$UAC^{*-}_{0.05} = 33.2824\%$ $UACI^{*+}_{0.05} = 33.6447\%$	$UACI^{*-}_{0.01} = 33.225\%$ $UACI^{*+}_{0.01} = 33.7016\%$	$UACI^{*-}_{0.001} = 33.1594\%$ $UACI^{*+}_{0.001} = 33.7677\%$
Lena	33.4657	pass	pass	pass
Pepper	33.4643	pass	pass	pass
Barbara	33.4721	pass	pass	pass
Fruits	33.4603	pass	pass	pass
4.1.03	33.4592	pass	pass	pass
4.1.04	33.4801	pass	pass	pass
House	33.4544	pass	pass	pass
Airplane	33.4823	pass	pass	pass

Table 10 The NPCR and UACI values of the images under different algorithms

Images	Index	Ours	[16]	[14]	[46]	[33]
Lena	NPCR(%)	99.6063	99.6089	99.6236	99.5977	99.6300
	UACI(%)	33.4657	33.5071	33.3619	33.4062	33.6352
Pepper	NPCR(%)	99.6130	99.6106	99.6164	99.6082	99.6493
	UACI(%)	33.4643	33.4368	33.3688	33.4346	33.4693

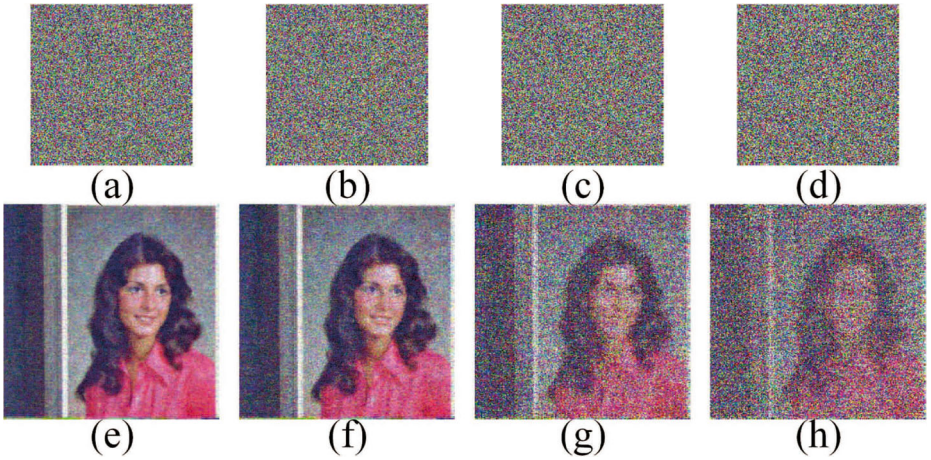

Fig. 20 Noise Attack: 4.1.04 (256× ×256) has salt and pepper noise of (a) 0.001, (b) 0.01, (c) 0.1and (d) 0.2; the decrypted image of (e) Figs. 15a, f Fig. 15b, g Fig. 15c and h Fig. 15d

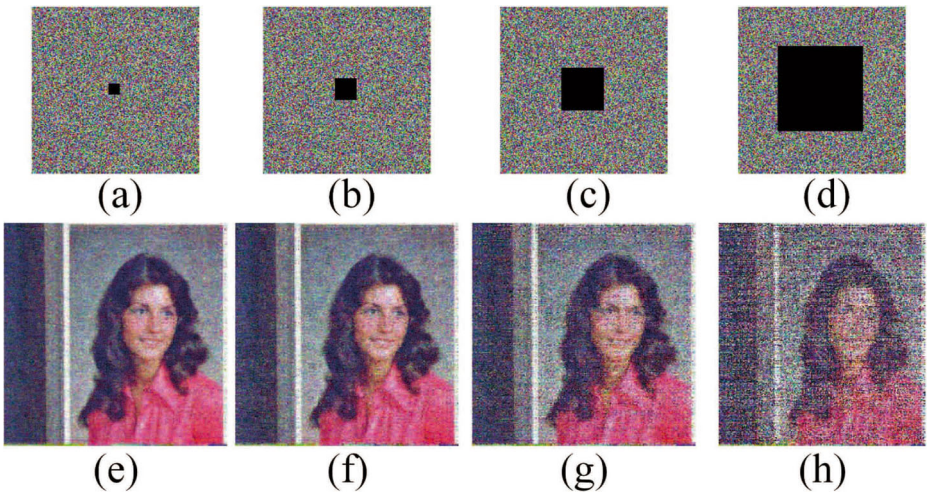

Fig. 21 Cropping Attack: 4.1.04 (256×256) has data loss of (a) 1/16, (b) 1/8, (c) 1/4 and (d) 1/2; the decrypted image of (e) Fig. 16a, f Fig. 16b, g Fig. 16c and h Fig. 16d

5 Conclusion

A fractional-order non-equilibrium chaotic system with hidden attractors is proposed, and its dynamical characteristics are analyzed. The complexity and attractor basin are used to analyze and determine the optimal parameter range of the system in the secure communication system. Moreover, we design an image encryption scheme in which compression and encryption are performed simultaneously. The scheme uses random row and column scrambling and GF (257) domain diffusion algorithm to encrypt images. The key is related to the plaintext, which can improve the resistance to known or selected plaintext attacks. The experimental results indicate that the encrypted image is obviously smaller than the original image, and the information of the original image is successfully destroyed. The algorithm has good compression performance. Even the $CR = 0.25$, the obtained PSNR values and MSSIM values are large enough to still identify the main information of the original image. In addition, the proposed algorithm can resist various attacks such as differential attacks, shearing attacks, and noise attacks. Statistical analysis, secret key space and secret key sensitivity analysis prove the security and effectiveness of the algorithm and the algorithm has good practical application value.

Acknowledgments This work was supported by the National Natural Science Foundation of China (Grant Nos. 62061014); The Natural Science Foundation of Liaoning province(2020-MS-274); The Basic Scientific Research Projects of Colleges and Universities of Liaoning Province (Grant Nos. LJKZ0545).

Author Contributions Haiying Hu designed and carried out experiments, data analyzed and manuscript wrote. Yinghong Cao and Jun Mou made the theoretical guidance for this paper. Jin Hao carried out experiment on the DSP platform. Xuejun Li improved the algorithm. All authors reviewed the manuscript.

Declarations

Conflict of Interests No conflicts of interests about the publication by all authors.

References

1. Chai X, Bi J, Gan Z, Liu X, Zhang Y, Chen Y (2020) Color image compression and encryption scheme based on compressive sensing and double random encryption strategy. Signal Process 176:107684
2. Chai X, Fu X, Gan Z, Lu Y, Chen Y (2019) A color image cryptosystem based on dynamic dna encryption and chaos. Signal Process 155:44–62
3. Chai X, Gan Z, Chen Y, Zhang Y (2016) A visually secure image encryption scheme based on compressive sensing. Signal Process 134:35–51
4. Chai X, Gan Z, Zhang M (2016) A fast chaos-based image encryption scheme with a novel plain image-related swapping block permutation and block diffusion. Multimed Tools Appl 76(14):15561–15585
5. Chai X, Wu H, Gan Z, Zhang Y, Chen Y (2020) Hiding cipher-images generated by 2-d compressive sensing with a multi-embedding strategy. Signal Process 171:107525
6. Chen C, Min F, Zhang Y, Bao B (2021) Memristive electromagnetic induction effects on hopfield neural network. Nonlin Dynam 106(3):2559–2576
7. Chen L, Yin H, Yuan L, Lopes AM, Machado JAT, Wu R (2020) A novel color image encryption algorithm based on a fractional-order discrete chaotic neural network and dna sequence operations. Front Inform Technol Electr Eng 21(6):866–879
8. Gao X, Mou J, Xiong L, Sha Y, Yan H, Cao Y (2022) A fast and efficient multiple images encryption based on single-channel encryption and chaotic system. Nonlin Dyn 108(1):613–636
9. Gao X, Mou J, Banerjee S, Cao Y, Xiong L, Chen X (2022) An effective multiple-image encryption algorithm based on 3d cube and hyperchaotic map. Journal of King Saud University - Computer and Information Sciences 34(4):1535–1551

10. Gu W, Yu Y, Hu W (2017) Artificial bee colony algorithm-based parameter estimation of fractional-order chaotic system with time delay. IEEE/CAA J Autom Sinica 4(1):107–113
11. Han X, Mou J, Jahanshahi H, Cao Y, Bu F (2022) A new set of hyperchaotic maps based on modulation and coupling. Eur Phys J Plus 137:4
12. Hasanzadeh E, Yaghoobi M (2019) A novel color image encryption algorithm based on substitution box and hyper-chaotic system with fractal keys. Multimed Tools Appl 79(11-12):7279–7297
13. Hu H, Cao Y, Xu J, Ma C, Yan H (2021) An image compression and encryption algorithm based on the fractional-order simplest chaotic circuit. IEEE Access 9:22141–22155
14. Hu X, Wei L, Chen W, Chen Q, Guo Y (2020) Color image encryption algorithm based on dynamic chaos and matrix convolution. IEEE Access 8:12452–12466
15. Huang R, Rhee KH, Uchida S (2012) A parallel image encryption method based on compressive sensing. Multimed Tools Appl 72(1):71–93
16. Huang R, Liao X, Dong A, Sun S (2020) Cryptanalysis and security enhancement for a chaos-based color image encryption algorithm. Multimed Tools Appl 79(37–38):27483–27509
17. Iqbal N, Hanif M, Abbas S, Khan MA, Almotiri SH, Al Ghamdi MA (2020) Dna strands level scrambling based color image encryption scheme. IEEE Access 8:178167–178182
18. Jafari S, Sprott JC, Hashemi Golpayegani SMR (2013) Elementary quadratic chaotic flows with no equilibria. Phys Lett A 377(9):699–702
19. Jia HY, Chen ZQ, Qi GY (2017) Chaotic characteristics analysis and circuit implementation for a fractional-order system. IEEE Trans Circ Syst I Regular Papers 61(3):845–853
20. Kuznetsov, N. V, Leonov, G. A, Seledzhi, S. M (2011) Hidden oscillations in nonlinear control systems. IFAC Proceed Vol 44(1):2506–2510
21. Lan R, He J, Wang S, Gu T, Luo X (2018) Integrated chaotic systems for image encryption. Signal Process 147:133–145
22. Leonov GA, Kuznetsov NV (2011) Algorithms for searching for hidden oscillations in the Aizerman and Kalman problems. Dokl Math 84(1):475
23. Leonov GA, Kuznetsov NV (2011) Analytical-numerical methods for investigation of hidden oscillations in nonlinear control systems. Ifac Proc Vol 44(1):2494–2505
24. Leonov GA, Kuznetsov NV, Kiseleva MA, Solovyeva EP, Zaretskiy AM (2014) Hidden oscillations in mathematical model of drilling system actuated by induction motor with a wound rotor. Nonlin Dyn 77(1-2):277–288
25. Leonov GA, Kuznetsov NV, Vagaitsev VI (2011) Localization of hidden chuas attractors. Phys Lett A 375(23):2230–2233
26. Li X, Mou J, Cao Y, Banerjee S (2022) An optical image encryption algorithm based on a fractional-order laser hyperchaotic system. Int J Bifur Chaos 32:03
27. Li X, Mou J, Banerjee S, Wang Z, Cao Y (2022) Design and dsp implementation of a fractional-order detuned laser hyperchaotic circuit with applications in image encryption. Chaos, Solitons and Fractals 159:112133
28. Liu H, Kadir A, Liu J (2019) Color pathological image encryption algorithm using arithmetic over galois field and coupled hyper chaotic system. Opt Lasers Eng 122:123–133
29. Liu T, Banerjee S, Yan H, Mou J (2021) Dynamical analysis of the improper fractional-order 2d-sclmm and its dsp implementation. Eur Phys J Plus 136(5):1–17
30. Liu W, Sun K, Zhu C (2016) A fast image encryption algorithm based on chaotic map. Opt Lasers Eng 84:26–36
31. Ma C, Mou J, Li P, Liu T (2021) Dynamic analysis of a new two-dimensional map in three forms: integer-order, fractional-order and improper fractional-order. Eur Phys J Special Topics 230(7):1945–1957
32. Ma C, Mou J, Xiong L, Banerjee S, Han X (2021) Dynamical analysis of a new chaotic system: asymmetric multistability, offset boosting control and circuit realization. Nonlin Dyn 103(6):1–14
33. Malik MGA, Bashir Z, Iqbal N, Imtiaz MA (2020) Color image encryption algorithm based on hyper-chaos and dna computing. IEEE Access 8:88093–88107
34. Min F, Cheng Y, Lu L, Li X (2021) Extreme multistability and antimonotonicity in a shinriki oscillator with two flux-controlled memristors. International Journal of Bifurcation and Chaos
35. Mou J, Yang F, Chu R, Cao Y (2019) Image compression and encryption algorithm based on hyper-chaotic map. Mobile Networks and Applications
36. Musanna F, Kumar S (2018) A novel fractional order chaos-based image encryption using fisher yates algorithm and 3-d cat map. Multimed Tools Appl 78(11):14867–14895
37. Ojoniyi OS, Njah AN (2016) A 5d hyperchaotic sprott b system with coexisting hidden attractors. Chaos, Solitons and Fractals 87:172–181

38. Pham VT, Vaidyanathan S, Volos CK, Jafari S (2015) Hidden attractors in a chaotic system with an exponential nonlinear term. Eur Phys J Spec Topics 224(8):1507–1517
39. Pham VT, Volos C, Gambuzza LV (2014) A memristive hyperchaotic system without equilibrium. Scientific World Journal 2014:368986
40. Pham V-T, Vaidyanathan S, Volos CK, Azar AT, Hoang TM, Van Yem V (2017) A three-dimensional no-equilibrium chaotic system: analysis, synchronization and its fractional order form 688:449–470
41. Pham V-T, Vaidyanathan S, Volos CK, Hoang TM, Van Yem V (2016) Dynamics, synchronization and spice implementation of a memristive system with hidden hyperchaotic attractor 337:35–52
42. Ruan J, Sun K, Mou J, He S, Zhang L (2018) Fractional-order simplest memristor-based chaotic circuit with new derivative. The European Physical Journal Plus, 133
43. Shakir HR (2019) An image encryption method based on selective aes coding of wavelet transform and chaotic pixel shuffling. Multimed Tools Appl 78(18):26073–26087
44. Sharma PR, Shrimali MD, Prasad A, Kuznetsov NV, Leonov GA (2015) Control of multistability in hidden attractors. Eur Phys J Spec Topics 224(8):1485–1491
45. Vaidyanathan S (2016) Analysis, control and synchronization of a novel 4-d highly hyperchaotic system with hidden attractors 337:529–552
46. Wang H, Xiao D, Chen X, Huang H (2018) Cryptanalysis and enhancements of image encryption using combination of the 1d chaotic map. Signal Process 144:444–452. https://doi.org/10.1016/j.sigpro.2017.11.005
47. Wang S, Wang C, Xu C (2020) An image encryption algorithm based on a hidden attractor chaos system and the Knuth-Durstenfeld algorithm. Opt Lasers Eng 128:105995
48. Wang X-Y, Li Z-M (2019) A color image encryption algorithm based on hopfield chaotic neural network. Opt Lasers Eng 115:107–118
49. Wang X, Chen G (2012) Constructing a chaotic system with any number of equilibria. Nonlin Dyn 71(3):429–436
50. Wu Y, Noonan JP (2011) Npcr and uaci randomness tests for image encryption. Cyber Journals: Multidisciplinary Journals in Science and Technology, Journal of Selected Areas in Telecommunications 2:31–38
51. Xu C, Sun J, Wang C (2020) An image encryption algorithm based on random walk and hyperchaotic systems. Int J Bifur Chaos 30(04):2050060
52. Xu Q, Sun K, Cao C, Zhu C (2019) A fast image encryption algorithm based on compressive sensing and hyperchaotic map. Opt Lasers Eng 121:203–214
53. Xu Y, Sun K, He S, Zhang L (2016) Dynamics of a fractional-order simplified unified system based on the adomian decomposition method. Europ Phys J Plus 131(6):1–12
54. Yang F, Mou J, Luo C, Cao Y (2019) An improved color image encryption scheme and cryptanalysis based on a hyperchaotic sequence. Phys Scr 94(8):085206
55. Yang F, Mou J, Sun K, Cao Y, Jin J (2019) Color image compression-encryption algorithm based on fractional-order memristor chaotic circuit. IEEE Access 7:58751–58763
56. Yang F, Mou J, Yan H, Hu J (2019) Dynamical analysis of a novel complex chaotic system and application in image diffusion. IEEE Access 7:118188–118202
57. Zhang L-M, Sun K-H, Liu W-H, He S-B (2017) A novel color image encryption scheme using fractional-order hyperchaotic system and dna sequence operations. Chin Phys B 26(10):100504
58. Zhu K, Cheng J (2020) Color image encryption via compressive sensing and chaotic systems. MATEC Web Conf 309:03017