

A color image encryption scheme based on a 2D coupled chaotic system and diagonal scrambling algorithm

Jingming Su(苏静明), Shihui Fang(方士辉), Yan Hong(洪炎), and Yan Wen(温言)

Citation: Chin. Phys. B, 2024, 33 (**7**): 070502. DOI: 10.1088/1674-1056/ad3efa
Journal homepage: http://cpb.iphy.ac.cn; http://iopscience.iop.org/cpb

What follows is a list of articles you may be interested in

Novel self-embedding holographic watermarking image encryption protection scheme

Linian Wang(王励年), Nanrun Zhou(周楠润), Bo Sun(孙博), Yinghong Cao(曹颖鸿), and Jun Mou(牟俊)
Chin. Phys. B, 2024, 33 (**5**): 050501. DOI: 10.1088/1674-1056/ad1c5b

A color image encryption algorithm based on hyperchaotic map and DNA mutation

Xinyu Gao(高昕瑜), Bo Sun(孙博), Yinghong Cao(曹颖鸿), Santo Banerjee, and Jun Mou(牟俊)
Chin. Phys. B, 2023, 32 (**3**): 030501. DOI: 10.1088/1674-1056/ac8cdf

Image encryption technique based on new two-dimensional fractional-order discrete chaotic map and Menezes-Vanstone elliptic curve cryptosystem

Zeyu Liu(刘泽宇), Tiecheng Xia(夏铁成), Jinbo Wang(王金波)
Chin. Phys. B, 2018, 27 (**3**): 030502. DOI: 10.1088/1674-1056/27/3/030502

A novel color image encryption scheme using fractional-order hyperchaotic system and DNA sequence operations

Li-Min Zhang(张立民), Ke-Hui Sun(孙克辉), Wen-Hao Liu(刘文浩), Shao-Bo He(贺少波)
Chin. Phys. B, 2017, 26 (**10**): 100504. DOI: 10.1088/1674-1056/26/10/100504

A novel color image encryption algorithm based on genetic recombination and the four-dimensional memristive hyperchaotic system

Xiu-Li Chai(柴秀丽), Zhi-Hua Gan(甘志华), Yang Lu(路杨), Miao-Hui Zhang(张苗辉), Yi-Ran Chen(陈怡然)
Chin. Phys. B, 2016, 25 (**10**): 100503. DOI: 10.1088/1674-1056/25/10/100503

A color image encryption scheme based on a 2D coupled chaotic system and diagonal scrambling algorithm

Jingming Su(苏静明)[1], Shihui Fang(方士辉)[1,†], Yan Hong(洪炎)[1], and Yan Wen(温言)[2,‡]

[1] *Anhui Mining Machinery and Electrical Equipment Coordination Innovation Center, Anhui University of Science and Technology, Huainan* 232001, *China*
[2] *School of Computer Science and Information Engineering, Hefei University of Technology, Hefei* 230009, *China*

(Received 15 March 2024; revised manuscript received 7 April 2024; accepted manuscript online 16 April 2024)

A novel color image encryption scheme is developed to enhance the security of encryption without increasing the complexity. Firstly, the plain color image is decomposed into three grayscale plain images, which are converted into the frequency domain coefficient matrices (FDCM) with discrete cosine transform (DCT) operation. After that, a two-dimensional (2D) coupled chaotic system is developed and used to generate one group of embedded matrices and another group of encryption matrices, respectively. The embedded matrices are integrated with the FDCM to fulfill the frequency domain encryption, and then the inverse DCT processing is implemented to recover the spatial domain signal. Eventually, under the function of the encryption matrices and the proposed diagonal scrambling algorithm, the final color ciphertext is obtained. The experimental results show that the proposed method can not only ensure efficient encryption but also satisfy various sizes of image encryption. Besides, it has better performance than other similar techniques in statistical feature analysis, such as key space, key sensitivity, anti-differential attack, information entropy, noise attack, etc.

Keywords: color image encryption, discrete cosine transform, two-dimensional (2D) coupled chaotic system, diagonal scrambling

PACS: 05.45.Gg, 94.05.–a, 07.05.Pj **DOI:** 10.1088/1674-1056/ad3efa

1. Introduction

With the rapid progress of network technology, multimedia communication becomes more and more popular. However, image transmission security faces a variety of challenges, such as differential attack, chosen plaintext attack, resistance to brute-force attacks, etc.[1–3] Therefore, many scholars have paid much attention to the encryption techniques for image transmission in recent years.[4,5]

Compared with the text encryption mode, due to the large amount of image data and the high correlation between pixels,[4,6] traditional encryption modes such as RSA, AES and IDEA[7–9] are not suitable for image encryption. In addition, due to the integrity requirement and inseparability of the image, the block encryption modes such as ECB[10] and CFB[11] are incompetent to fulfill the encryption of different sizes of images. Since Matthews and Robert suggested a logistic map-based chaotic sequence cipher method in the 1990s, the chaotic mapping image encryption technique has been widely employed in the field of image encryption.[12–14] Chaotic systems have been proven to be pseudo-random, unpredictable, and sensitive to initial values and parameters, so researchers have constructed a variety of image encryption algorithms. Lai and Liu[15] introduced a novel two-dimensional (2D) chaotic mapping model that excels in generating random sequences with robust randomness, achieved through sinusoidal mapping and mathematical formulations. This model enables the creation of secure, sensitive keys via adjustable parameters, avoiding data redundancy. They also innovatively implemented a peripheral pixel expansion to bolster cryptographic resilience against attacks and enhanced color image encryption's efficiency and security using a cross-channel encryption technique. Zhao *et al*.[16] proposed image encryption by using a double chaotic system. Compared with the classical chaotic system, the proposed quadratic map has a larger Lyapunov exponent, which means it has better chaotic characteristics and unpredictability. In addition, low-dimensional chaotic map systems have a restricted range of chaotic sequences and the generated key stream becomes predictable, but high-dimensional chaotic map systems have more parameters and a larger chaotic sequence space.[13,17–19] Wang *et al*.[20] used a six-dimensional hyperchaotic image encryption algorithm based on DNA operation and bit-level alignment, and the horizontal displacement makes the algorithm better security. However, these encryption models also have high implementation costs and low security in practical applications to some extent.[21]

To solve those problems, many image encryption schemes in spatial and frequency domains have been proposed. Various transform methods, such as the fast Fourier transform (FFT),[20] discrete wavelet transform (DWT),[22] or discrete cosine transform (DCT)[23] are used to encrypt images from the spatial domain to the frequency domain in order to obtain the coefficient matrix. After that, the final ci-

†Corresponding author. E-mail: fsh@aust.edu.cn
‡Corresponding author. E-mail: wenyan@hainanu.edu.cn

© 2024 Chinese Physical Society and IOP Publishing Ltd

pher image is generated by scrambling these coefficients and performing the inverse transform on the scrambled coefficient matrix. Cheng *et al.*[24] proposed an image-hiding algorithm based on DCT, however, the algorithm encrypts and embeds single images, which cannot meet the encryption requirements of a large number of images. Wang *et al.*[25] proposed an image encryption and hiding algorithm based on compressive sensing (CS) and DCT transform. Firstly, DWT is used to sparse the gray plain image to obtain the sparse matrix. Then the sparse matrix is scrambled by the position index and 3D-zigzag scrambling. The 2D chaotic system generates a measurement matrix to observe the scrambled sparse matrix. Finally, the cipher image is embedded into the carrier image to obtain the final cipher image. These algorithms have relatively satisfactory encryption performance. However, they still have shortcomings in compression, security, and efficiency. To summarize the above, this paper introduces a novel chaos-based image encryption scheme with diagonal scrambling and DCT transform. The main goal of this solution is to improve the security of image encryption and optimize compression efficiency, thereby solving the problems of insufficient security and low compression performance in the existing technology. Through carefully designed chaotic mapping and diagonal replacement strategies, the solution in this article not only ensures data security, but also improves image compression performance, bringing new research directions and application prospects to the field of image encryption. This work makes the following three major contributions:

(1) A newly devised two-dimensional chaotic mapping is introduced, characterized by its robust dynamic properties.

(2) A novel diagonal scrambling structure is proposed. Compared with the traditional algorithm, such as Arnold scrambling, circular scrambling, and zigzag scrambling,[26] the pixel position transformation is more random and unrecoverable.

(3) Compared with other similar algorithms, this algorithm has better encryption performance without increasing implementation costs.

The article is separated into the following sections. Section 2 provides an overview of the pertinent knowledge regarding the 2D coupled chaotic system. Section 3 explains details of the encryption algorithm utilized. Section 4 presents the experimental results along with a security analysis. The article concludes with a summary in Section 5.

2. Relevant knowledge

2.1. Logistic mapping

The logistic is a one-dimensional chaotic system whose dynamic behavior is complex despite its simple mathematical form. It is commonly utilized in the study of chaos[27] and described by

$$x_{i+1} = ux_i(1-x_i), \tag{1}$$

where u is the parameter of the logistic system, x_i is the chaotic sequence of the system. The bifurcation diagram and the Lyapunov exponent (LE) are shown in Fig. 1. Observably, a minor portion of the LE index exceeds the threshold of 0, indicating that the chaotic attributes are not prominently exhibited.

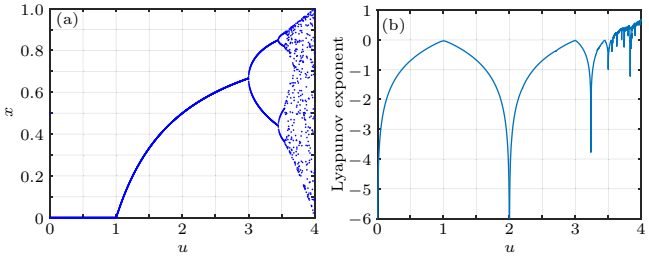


Fig. 1. (a) Bifurcation diagram; (b) Lyapunov exponent diagram.

2.2. Henon mapping

Henon is two-dimensional chaotic mapping. It possesses the qualities of simplicity, consistent power spectrum density, and high relevance.[29] The corresponding mathematical formula is

$$\begin{cases} x_{n+1} = y_n - ax_n^2 + 1, \\ y_{n+1} = bx_n, \end{cases} \tag{2}$$

where a and b are the parameters of the system. The bifurcation diagram and the Lyapunov exponent distribution of the Henon mapping are shown in Fig. 2. The diagram shows the

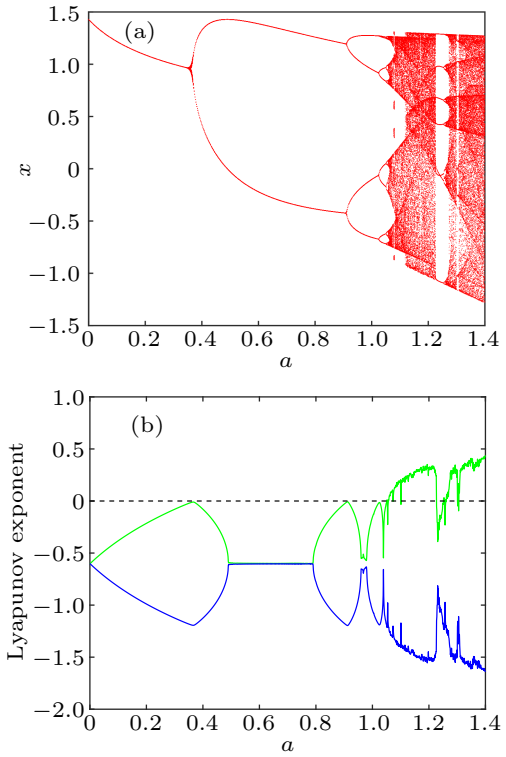


Fig. 2. Henon mapping: (a) bifurcation diagram, (b) Lyapunov exponent diagram.

system is chaotic when $a \in (1.07,1.4)$, $b = 0.3$. It is evident that chaos occurs in a relatively small section of the parameter space within this range.

2.3. The 2D coupled chaotic system

Logistic and Henon have the following problems. For example, the sequences created are usually highly correlated, with limited key space and weak security. To be able to overcome these flaws, according to Eqs. (1) and (2), we expand the mapping parameters of the logistic chaotic system, extend the iteration parameter from $\{x_n\}$ to $\{x_n$ and $y_n\}$ and use triangular wave and cosine wave functions to generate high-dimensional chaotic attractors to enhance the randomness and controllability of the chaotic system. Thus, a novel 2D chaotic mapping system with state variables $\{a,b\}$ is proposed as

$$f(x_{n+1},y_{n+1}) = \begin{cases} \sin\left(\dfrac{y_n}{x_n} - ax_n^2 + a\right), \\ \dfrac{\pi}{2}\arcsin(\cos(bx_n)). \end{cases} \tag{3}$$

Figure 3 demonstrates the Lyapunov exponent of the improved chaotic system based on logistic and Henon mapping. Figures 3(a) and 3(b) show the Lyapunov exponents of chaotic system parameters a and b. In order to make the system have better chaotic characteristics, we set the parameters $a \in (0.3,3.1)$ and $b \in (5,7)$. Obviously, the parameter range of the upgraded chaotic system has been greatly expanded.

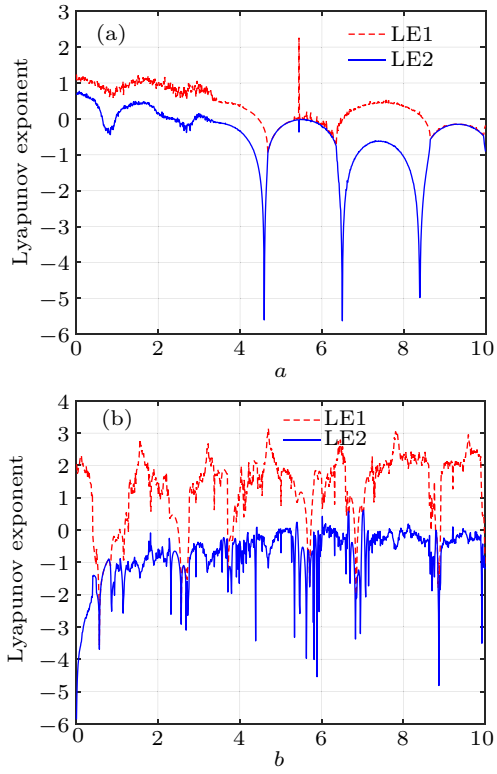


Fig. 3. Lyapunov exponent diagram: (a) Lyapunov exponent diagram of parameter a, (b) Lyapunov exponent diagram of parameter b.

We use the bifurcation diagram and the Poincaré section diagram to further intuitively study the proposed chaotic system. The initial values of the chaotic mapping are set as $x_0 = 0.4$, $y_0 = 0.3$, $a \in [0,10]$, $b \in [0,15]$, the bifurcation diagrams of the system are shown in Fig. 4, which shows that the bifurcation diagram of the new chaotic system is more random and has better chaotic characteristics than those of logistic and Henon systems.

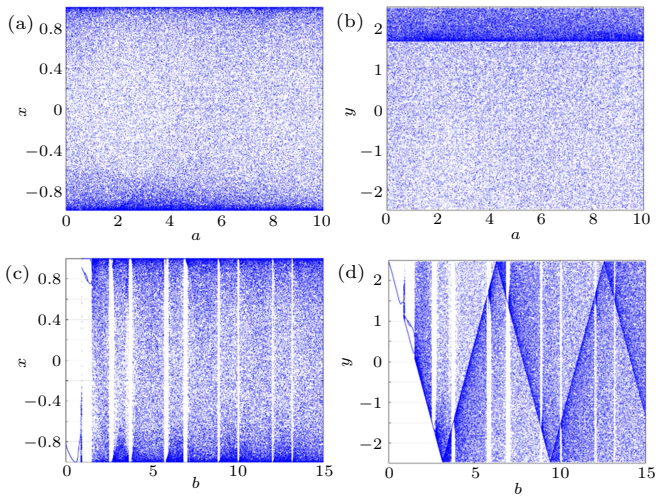


Fig. 4. Bifurcation figure. (a), (c) The bifurcation of the sequence x when $a \in [0,10]$ and $b \in [0,15]$, respectively. (b), (d) The bifurcation of the sequence y when $a \in [0,10]$ and $b \in [0,15]$, respectively.

The initial parameters of the chaotic system have been precisely set as $a = 2.5$ and $b = 6.8$. Figure 5 comprehensively exhibits the Poincaré section diagrams of the chaotic system, providing a thorough visual basis for the in-depth study of its dynamics. By observing the Poincaré cross-section depicted in Fig. 5, we can clearly identify distinct thick patches, which exhibit a pronounced hierarchical structure within the novel chaotic system. The existence of this hierarchical structure not only reveals the intricate chaotic behavior within the system but also underscores the high complexity of its dynamic characteristics. Given its unique dynamic properties, this chaotic system serves as an ideal candidate for use as a key generator in encryption systems, offering a relatively secure guarantee for image encryption.

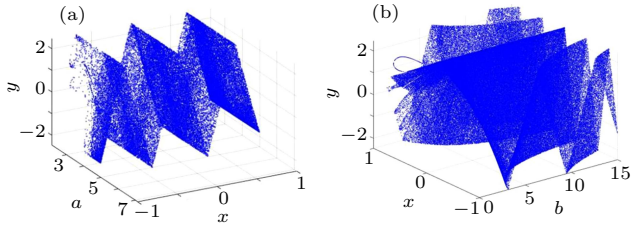


Fig. 5. Poincaré section diagram. (a) The Poincare section diagram when $a = 2.5$. (b) The Poincare section diagram when $b = 6.8$.

What is more, a good chaotic system should have the characteristics of initial value sensitivity and parameter sensitivity. Figure 6 shows the iterative trajectory diagram of small changes in the initial value of the system. Initial value,

$x_0 = 0.256$, $y_0 = 0.3218$, $a = 2.5$, $b = 6.8$, Figs. 6(a) and 6(b) respectively show the mapping trajectories where $x_0 = 0.256 + 10^{-14}$ and $y_0 = 0.3218 + 10^{-14}$. It shows that after a few iterations, the sequence changes a lot, indicating that the system has a strong initial value sensitivity.

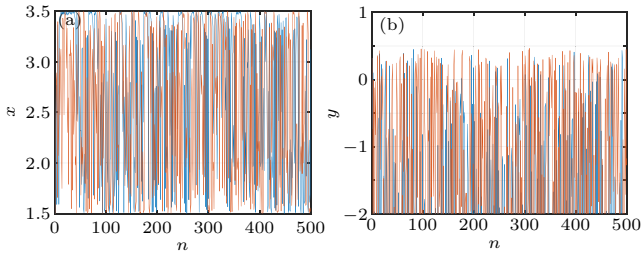


Fig. 6. Iterative trajectory diagram: (a) trajectory of $x_0 = 0.256$ and $x_0 = 0.256 + 10^{-14}$, (b) trajectory of $y_0 = 0.3218$ and $y_0 = 0.3218 + 10^{-14}$.

In the field of information theory, Kolmogorov entropy, also known as Kolmogorov–Sinai entropy, is used to measure the level of uncertainty associated with a random variable.[28] The higher the Kolmogorov entropy, the more complex and unpredictable the dynamic system is.

As shown in Fig. 7, it can be seen that the proposed algorithm exhibits higher Kolmogorov entropy compared to the reference outlined in Ref. [15], which means superior chaotic performance and enhanced unpredictability, and this is a desirable feature in encryption and security applications. This advancement emphasizes the robustness of the algorithm and its potential effectiveness in contributing to the field of cryptosystems.

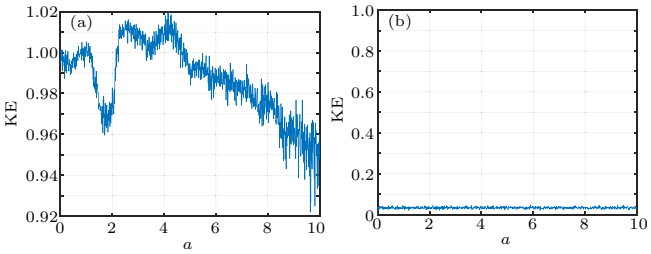


Fig. 7. Kolmogorov entropy.

3. Algorithm description

3.1. SHA-512 function

In order to improve the security of the algorithm and the correlation between key and plaintext images, the algorithm uses the hash function to generate system parameters and encryption. Divide the 512-bit key K into 16-bit blocks, which can be expressed as $K = k_1, k_2, \ldots, k_{32}$. The parameters are generated according to the following equations:

$$\begin{cases} x_0 = \dfrac{\bmod\left(\text{floor}\left(k_1 \oplus k_2 \cdots \oplus k_8\right) \times 2^{10}, 256\right)}{256}, \\ y_0 = \dfrac{\bmod\left(\text{floor}\left(k_9 \oplus k_{10} \cdots \oplus k_{16}\right) \times 2^{10}, 256\right)}{256}, \end{cases} \tag{4}$$

$$\begin{cases} a = \dfrac{\bmod\left(\text{fix}\left(k_{17} \oplus k_{18} \cdots \oplus k_{24}\right) \times 2^{10}, 256\right)}{256}, \\ b = \dfrac{\bmod\left(\text{fix}\left(k_{25} \oplus k_{26} \cdots \oplus k_{32}\right) \times 2^{10}, 256\right)}{256}, \end{cases} \tag{5}$$

where x_0, y_0, a, and b are the initial values and parameters of the system, and where mod is the modulus operation, floor(x) means the largest integer not greater than x, fix(x) means rounding to the nearest integer.

3.2. Diagonal scrambling

In this paper, a new scrambling algorithm has been proposed. The image pixels are scrambled diagonally. First, the pixels in the upper triangular position are scrambled from top to bottom along the main diagonal direction, and then the pixels in the lower triangular position are scrambled from bottom to top along the diagonal direction. The confusion diagram is shown in Fig. 8.

After the diagonal is scrambled, the position of the pixel can be effectively disturbed. Figure 9 shows the scrambled and recovery effect with the proposed diagonal algorithm. On the left, there are plain images. In the middle, they are cipher images while part of the information is lost. On the right, there are the recovery images, which can still effectively restore the plain information after the image is destroyed. This process proves the robustness of diagonal scrambling.

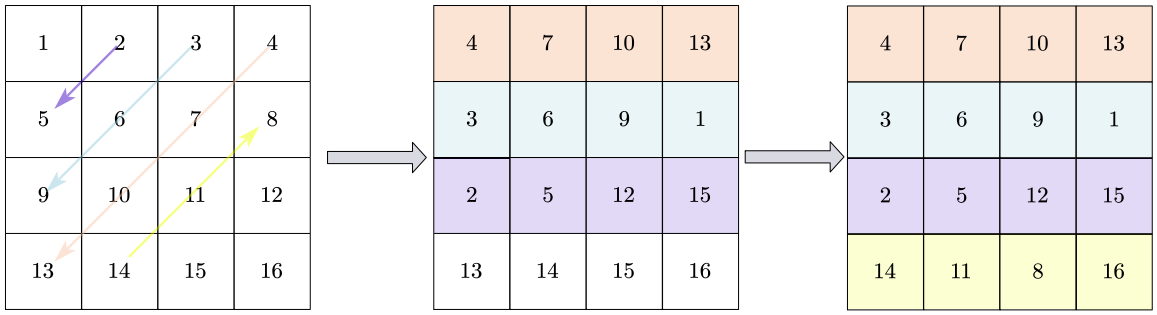


Fig. 8. The scrambling method.

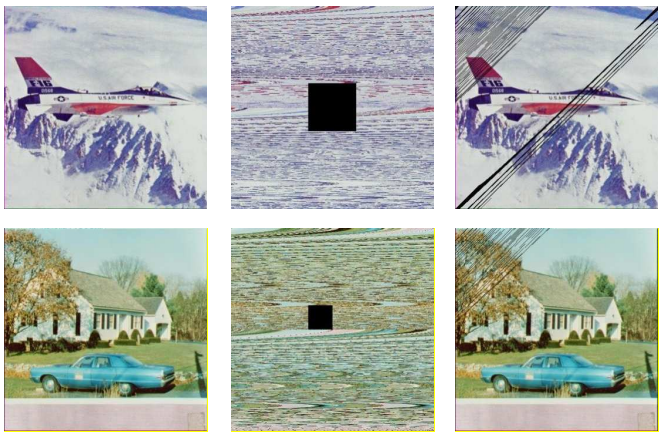


Fig. 9. Scrambling performance of diagonal scrambling.

3.3. The 3D DCT

The discrete cosine transform (DCT) effectively converts signals from the spatial domain to the frequency domain using sine functions, renowned for its excellent decorrelation capabilities. This transformation is predominantly utilized for the compression of data and images, enhancing efficiency and quality in storage and transmission.

In this algorithm, 3D DCT transform is used to embed the matrix in R, G and B of the plain color image. Firstly, two methods are used to apply the 3D DCT to a three-dimensional matrix. One of the methods is to directly perform the 3D DCT on the three-dimensional matrix. Another method is the pseudo-3D DCT; that is, the three-dimensional color image is regarded as a three-dimensional matrix stacked from three grayscale images. Then, the 2D DCT is performed on each image, and then 1D DCT is performed. 3D DCT transform and inverse transform are shown below:

$$\begin{aligned} F(e,u,v) &= C(e)C(u)C(v)\sum_{x=0}^{n_x-1}\sum_{y=0}^{n_y-1}\sum_{z=0}^{n_z-1} \\ &\quad \times f(x,y,z)\cdot g(x,y,z), \end{aligned} \tag{6}$$

$$\begin{aligned} f(x,y,z) &= \sum_{x=0}^{n_x-1}\sum_{y=0}^{n_y-1}\sum_{z=0}^{n_z-1} C(e)C(u)C(v) \\ &\quad \times F(e,u,v)\cdot g(x,y,z), \end{aligned} \tag{7}$$

$$\begin{aligned} C(e) &= \begin{cases} \sqrt{1/n_x}, & e=0, \\ \sqrt{2/n_x}, & e\neq 0, \end{cases} \\ C(u) &= \begin{cases} \sqrt{1/n_y}, & u=0, \\ \sqrt{2/n_y}, & u\neq 0, \end{cases} \\ C(v) &= \begin{cases} \sqrt{1/n_z}, & v=0, \\ \sqrt{2/n_z}, & v\neq 0, \end{cases} \\ g(x,y,z) &= \frac{(2x+1)e\pi}{2n_x}\frac{(2y+1)u\pi}{2n_y}\frac{(2z+1)v\pi}{2n_z}, \end{aligned} \tag{8}$$

where the size of the three-dimensional matrix is n_x, n_y, n_z. At (x, y, z), $f(x, y, z)$ represents a three-dimensional matrix's function value. $F(x, y, z)$ represents the coefficients after applying the 3D DCT.

3.4. The encryption algorithm

To improve the security of the encryption technique and suppress the correlation among images, this paper mainly divides the encryption operation into two parts: embedding and encryption. Figure 10 demonstrates the flow chart of the encryption algorithm. In the embedding process, the specific operations are as follows.

Step 1 The R, G and B channels of plain images $I(m\times n\times 3)$ are obtained and separated into 8×8 data blocks. When the plain image cannot be divided by 8, the 0 could be filled in. Then, the 3D-DCT is used and generates the frequency coefficient matrices f_{r}, f_{g} and f_{b}.

Step 2 Iteration $m\times n+1000$ times for chaotic sequence x_n, y_n. To avoid the instantaneous effect, discard the first 1000 values and do the following for the sequence to get embedding matrices E_1', E_2', E_3' and encryption matrices P_1', P_2', P_3':

$$\begin{cases} E_n' = \mathrm{mod}(\mathrm{floor}(\mathrm{abs}(x_i+y_i) \\ \qquad +\mathrm{floor}(x_i+y_i)\times 10^{14}),2^{10}), \quad n=1,2,3, \\ P_n' = \mathrm{mod}(\mathrm{floor}(\mathrm{abs}(y_i-x_i) \\ \qquad -\mathrm{floor}(y_i-x_i)\times 10^{14}),2^{8}), \quad n=1,2,3. \end{cases} \tag{9}$$

Step 3 The E_1', E_2', E_3' are correspondingly embedded into f_{r}, f_{g} and f_{b} to get ciphertext image of R, G and B channels, which are expressed as I_{R}, I_{G} and I_{B},

$$\begin{cases} I_{\mathrm{R}} = f_{\mathrm{r}}+\alpha\times E_1', \\ I_{\mathrm{G}} = f_{\mathrm{g}}+\alpha\times E_2', \\ I_{\mathrm{B}} = f_{\mathrm{b}}+\alpha\times E_3', \end{cases} \tag{10}$$

where α is the gain factor, which can adjust the embedding intensity, it can be adjusted according to the embedding effect.

Step 4 The 3D inverse discrete cosine transform (IDCT3) is applied to the three-dimensional matrix I_{RGB} to get the cipher image in the frequency domain $S'(m\times n\times 3)$, it is expressed as

$$S' = \mathrm{floor}(\mathrm{IDCT}(I_{\mathrm{RGB}})). \tag{11}$$

After the frequency domain operation, the frequency domain cipher is scrambled and encrypted, the specific steps are as follows.

Step 1 The three channels of S' are separated into S_{R}', S_{G}' and S_{B}'. The scrambling matrix $\mathrm{S_R}$, S_{G} and S_{B} are obtained by diagonal scrambling operation and the size is $m\times n$.

Step 2 The encryption matrices P_1', P_2', P_3' are using encryption $\mathrm{S_R}$, S_{G}, S_{B} respectively and the operation is as follows:

$$\begin{cases} M_{\mathrm{R}} = \mathrm{bitxor}(S_{\mathrm{R}},P_1'), \\ M_{\mathrm{G}} = \mathrm{bitxor}(S_{\mathrm{G}},P_2'), \\ M_{\mathrm{B}} = \mathrm{bitxor}(S_{\mathrm{B}},P_3'). \end{cases} \tag{12}$$

Step 3 The image M_{RGB} obtained in Step 2 is subjected to a bit shifting operation, so as to obtain the final encrypted image M.

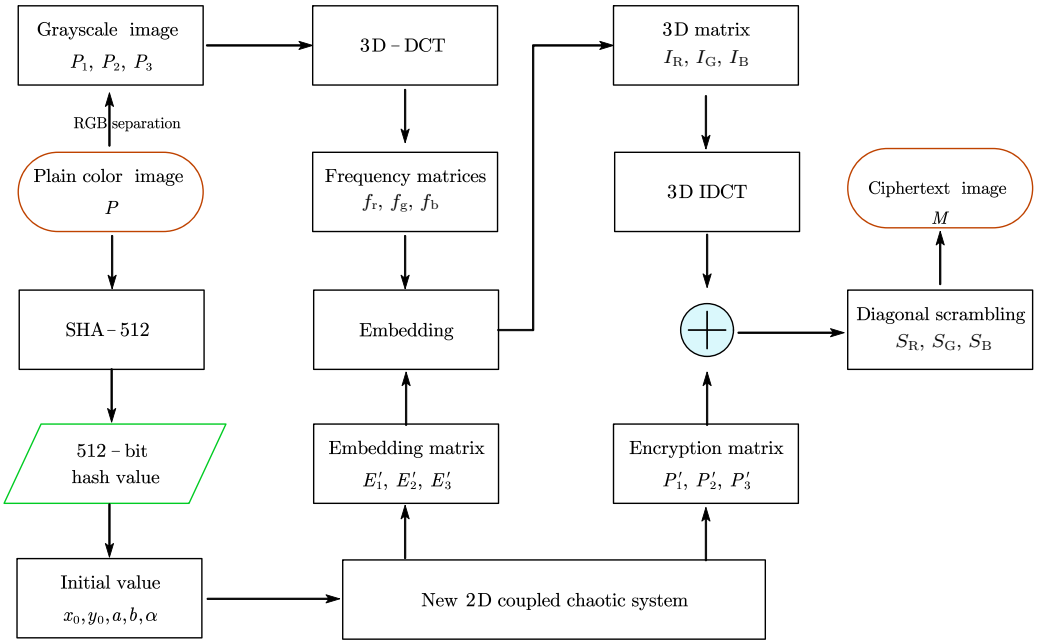


Fig. 10. Flowchart of proposed encryption algorithm.

3.5. The decryption algorithm

The decryption algorithm is the inverse process of the encryption algorithm. It mainly consists of four processes.

Step 1 The cipher image M is decomposed and the red, green and blue color components of the M are denoted M_R, M_G, M_B.

Step 2 The encryption matrices P'_1, P'_2, P'_3 are introduced to perform XOR operation and inverse diagonal scrambling is performed on M_R, M_G, M_B to obtain S_R, S_G, S_B. Then, the DCT is applied to get I_R, I_G, I_B.

Step 3 The frequency coefficient f_r, f_g, f_b.matrices are extracted from I_R, I_G, I_B. The formulas are described as follows:

$$\begin{cases} f_r = \alpha \times E'_1 - I_R, \\ f_g = \alpha \times E'_1 - I_G, \\ f_b = \alpha \times E'_1 - I_B. \end{cases} \tag{13}$$

Step 4 The inverse 3D DCT is performed to get the three final decrypted gray plain images and the three parts are combined to get the final decrypted image I. At this point, the decryption process is complete.

4. Experimental results and safety analysis

The experimental simulation test is based on MATLAB R2020, the computer is configured with 1.6 GHz CPU and 16 GB memory, and the operation system is Microsoft Windows 10. During the encryption process, the initial values $x_0 = 0.256$, $y_0 = 0.3218$, the parameters $a = 2.5$, $b = 6.82$, and the gain factor $\alpha = 0.15$. Figure 11 is the encryption results of four different color images using this encryption algorithm, namely, Lena (512×512), Car (256×256), White (512×512), and Black (512×512).

Figures 11(a), 11(e), 11(i), 11(k) are plaintext images, Figs. 11(b) and 11(f) are images after diagonal scrambling, Figs. 11(c), 11(g), 11(j), and 11(l) are the encrypted images, Figs. 11(d) and 11(h) are decrypted images of ciphertext images. It can be seen from Fig. 11 that after scrambling operation, the image information is effectively scrambled at the visual level, and the encryption algorithm has a good encryption effect on various sizes of images. After inputting the correct key, the decrypted image can be obtained.

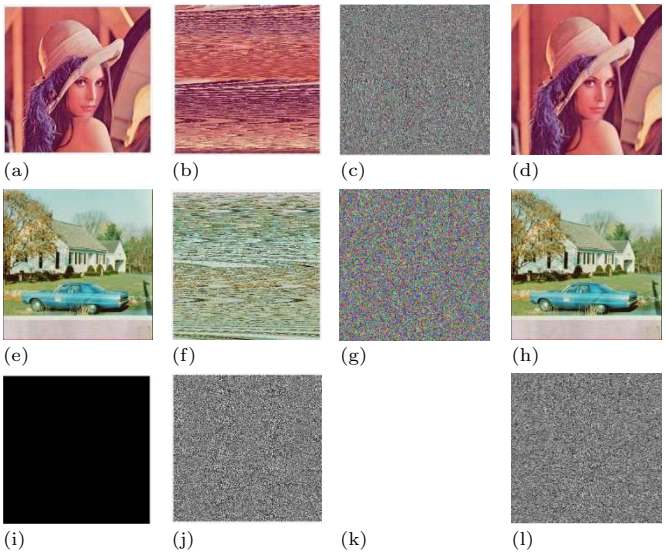


Fig. 11. (a), (e), (i), (k) Plain images; (b), (f) scrambling images; (c), (g), (j), (l) encryption images; (d), (h) decryption images.

4.1. Key analysis

4.1.1. Key space analysis

The key space size has an impact on the performance of the cryptographic algorithm, and a great image encryption algorithm must have a large key space to resist violent attacks.

In this paper, the initial values x_0 and y_0 are also the key to the encryption, in addition to the control parameters a and b, and the gain function α. The key space of each key is set to 10^{14} and the calculation of the key space is as follows:

$$\begin{aligned}\text{Key space} &= 10^{14}\times 10^{14}\times 10^{14}\times 10^{14}\times 10^{14}\\ &= 10^{70}\approx 2^{232}\gg 2^{128}.\end{aligned}$$

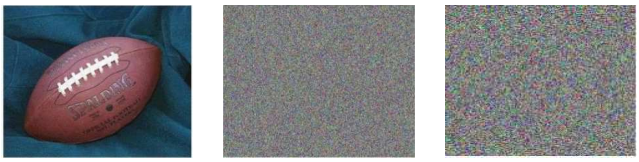
The result shows the description of the security of the algorithm is good and could resist the violent attack.

4.1.2. Key sensitivity analysis

A good encryption algorithm is sensitive to the key; throughout the encryption and decryption process, the key should be very sensitive. We change the encryption key to test the algorithm's key sensitivity. Assume that one parameter is altered while the others remain the same. The key of the proposed algorithm is K and the slightly changed keys are K_2 and K_3, and the amount of change is 10^{-14}. The results are shown in Fig. 12.

$K =$ 'f8c9d7c28409b90b31eadd1e3c4359ed0e0a8857087b6598f01a33e2a94ad55f',
$a =$ 'f8c9d7c28409b90b31eadd1e3c4359ed0e0a8857087b6598f01a33e2a94ad55a',
$b =$ 'f8c9d7c28409b90b31eadd1e3c4359ed0e0a8857087b6598f01a33e2a94ad55e'.

The results show that if the key is slightly altered, the cipher image created by encrypting the identical plain image changes dramatically, and it will not be able to accurately decipher the original cipher image if the key is modified slightly, demonstrating that our proposed algorithm is highly sensitive to the key in both the encryption and decryption processes.



(a) (b) (c)

Fig. 12. Key sensitivity results in decryption process.

4.2. Differential attack analysis

Differential attack is a way to attack the encryption algorithm that is performed by the comparison and analysis of specific differences in plaintext in terms of change propagated through the encryption. Therefore, in order to resist the differential attack, it is necessary to reduce the correlation between the plaintext image and the ciphertext image, if the plaintext image changes very little, it can lead to great changes in the encrypted image. We use the pixel change rate (NPCR) and average consistent change intensity (UACI) pairs to measure the ability of the encryption algorithm to resist differential attacks. For color images, NPCR and UACI are calculated by

$$\text{NPCR} = \frac{1}{M\times N}\sum_{i=0}^{M-1}\sum_{j=0}^{N-1} D(i,j)\times 100\%, \tag{14}$$

$$\text{UACI} = \frac{1}{M\times N}\left[\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}\frac{|C_1(i,j)-C_2(i,j)|}{255}\right], \tag{15}$$

where M represents the length of the image and N represents the width of the image. C_1 represents the encrypted image corresponding to the plaintext image, and C_2 represents the encrypted image after changing a randomly selected pixel value of the plain images. The D is expressed as

$$D(i,j) = \begin{cases} 0, & C_1(i,j) = C_2(i,j),\\ 1, & C_1(i,j) \neq C_2(i,j).\end{cases} \tag{16}$$

There are two random images. For any position, the probability that the pixel values of the two images are the same at this position is $p = 1/256$, and the probability that they are different is $p' = 1-p = 255/256$. Therefore, the ideal expected value of NPCR is 99.6094%.

Even if the pixels in all positions of the two images are not equal, that is, NPCR = 100 %, the difference between the two images is still small if the pixel values of their corresponding positions are very small. So, using NPCR alone cannot accurately describe the difference. Therefore, UACI is used to describe the change intensity of pixel values.

It can be seen from Table 2 that the proposed encryption algorithm is very sensitive to tiny changes in the plain image, even if there is only a one-bit difference between two plain images, the encrypted images will be completely different, and the result shows that this scheme is superior to the other references. The proposed scheme can resist the attack difference and meet certain security requirements.

Table 1. Values of NPCR and UACI.

Image	NPCR			Average	UACI			Average
	R	G	B		R	G	B	
Lena	99.6162	99.6128	99.5949	99.6080	32.9411	32.6818	31.6677	32.4302
Car	99.6006	99.5987	99.6086	99.6026	31.0881	31.1944	31.0769	31.1198
White	99.6284	99.6284	99.6284	99.6284	33.7540	33.7540	33.7540	33.7540
Black	99.6195	99.6195	99.6195	99.6195	33.8147	33.8147	33.8147	33.8147

Table 2. Compare with other algorithms.

	Ours	Ref. [30]	Ref. [31]	Ref. [32]	Ref. [33]	Ref. [34]
NPCR	99.6143	99.6217	99.6158	99.6133	99.6102	99.6135
UACI	33.4880	33.4983	33.4494	30.3600	30.4737	33.4646

4.3. Histogram analysis

A histogram is the statistical feature of image pixel value and a form of image pixel distribution. It can display the distribution number of pixel points under each pixel value in the image. For a good image encryption algorithm, the image histogram corresponding to the ciphertext should be regional uniform, and the average degree of the histogram also shows the quality of the encryption algorithm. Figures 13(b), 13(e), and 13(h) show the histogram of the plaintext image, and Figs. 13(c), 13(f), and 13(i) show the histogram of their corresponding ciphertext. According to the histogram in Fig. 13, it can be clearly shown that compared with the plaintext image, the histogram of the ciphertext image encrypted by the encryption algorithm tends to be more average, indicating that the encryption algorithm has a good encryption effect.

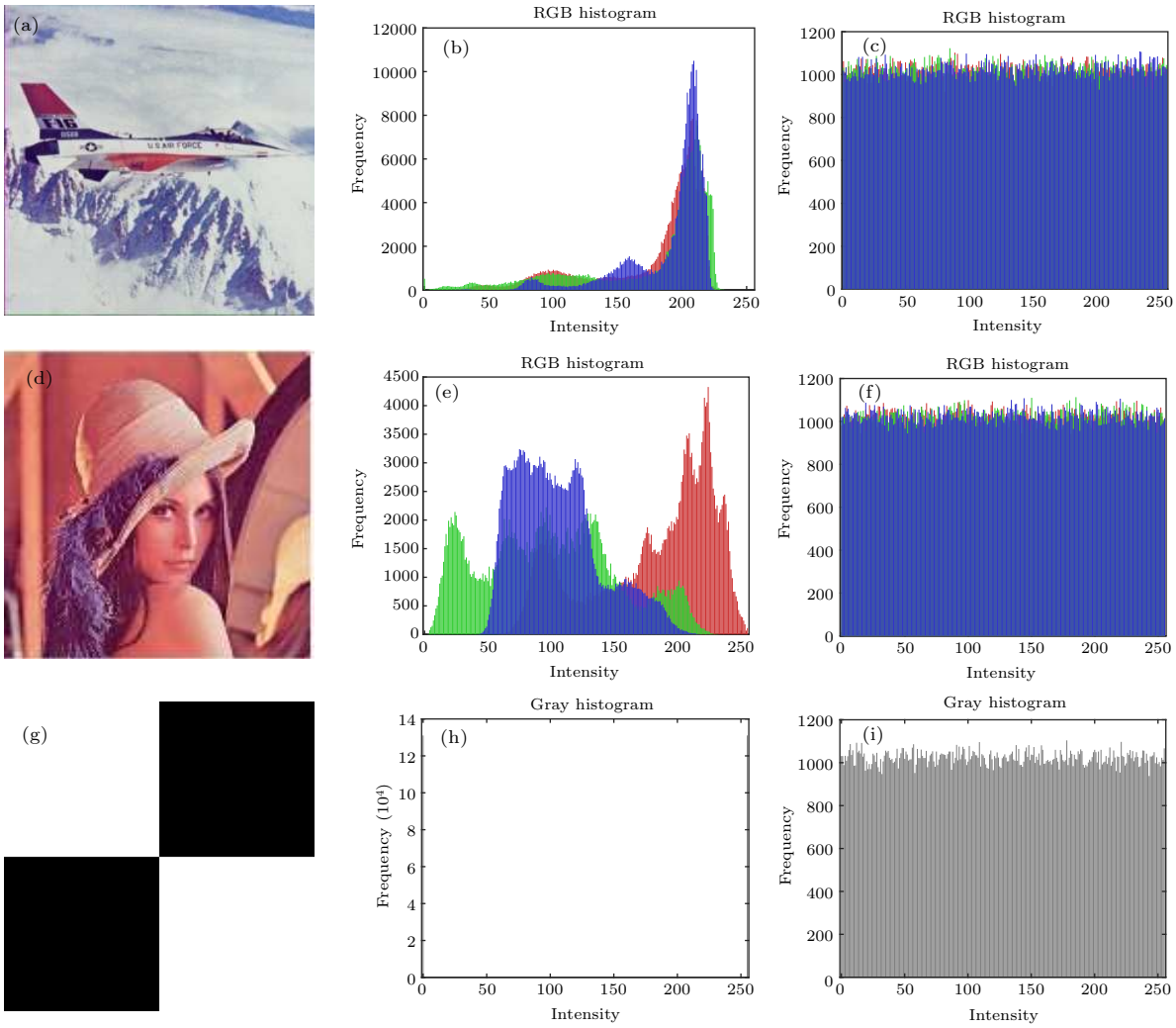


Fig. 13. (a), (d), (h) Plain images; (b), (e), (i) the histogram of plain images; (c), (f), (g), the histogram of cipher images.

4.4. Correlation analysis

In the plaintext images, the adjacent pixels in the horizontal, vertical and diagonal directions have a high correlation. The attacker can recover the image, according to the analysis of the correlation of the plaintext image. Therefore, as an effective encryption algorithm, the correlation of the plaintext image should be eliminated, and the ciphertext image with low correlation should be generated after encryption. The calculation methods of correlation coefficients $r(x, y)$ are

$$r_{xy}(x,y) = \frac{E((x-E(x))(y-E(y)))}{\sqrt{D(x)}\sqrt{D(y)}},$$

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

$$D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2, \tag{17}$$

where x and y are the gray values of adjacent pixels in the image, $E(x)$, $E(y)$ and $D(x)$, $D(y)$ represent the expectation and variance of variables x and y, and N represents the number of adjacent pixels selected when calculating the correlation.

In the analysis, 2500 pairs of adjacent pixels are selected from the plaintext image and the corresponding ciphertext image from the horizontal, vertical and diagonal directions respectively. The correlation coefficients and distribution of adjacent pixels of the plaintext image and the corresponding cipher image are shown in Fig. 14. Upon examination, it becomes evident that the RGB channels of the plaintext image exhibit a pronounced clustering in three distinct directions, indicative of a high level of correlation among them. Conversely, the ciphertext image displays a uniform distribution, devoid of any correlation characteristics. This observation underscores the resilience of the encryption algorithm against ciphertext attacks.

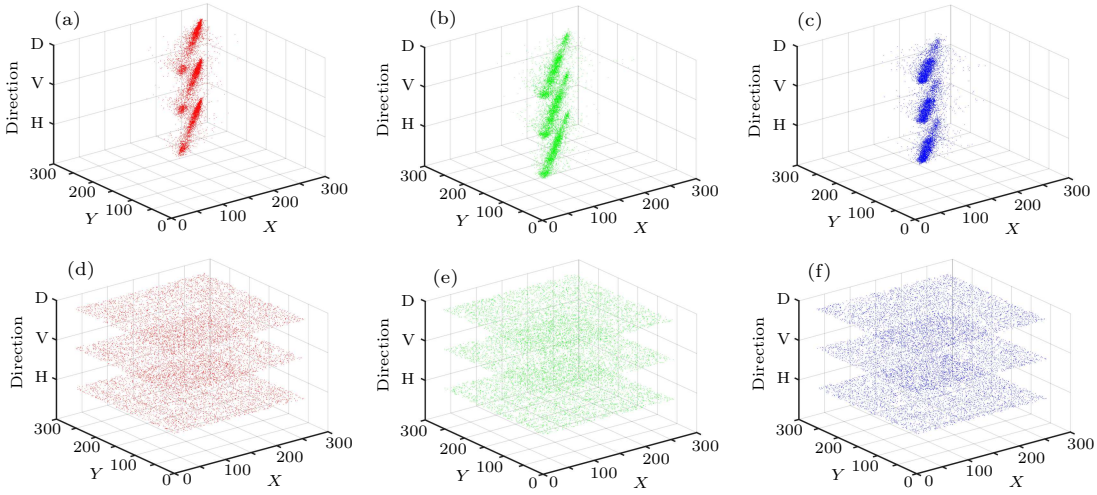


Fig. 14. Correlation between adjacent pixels of three directions. (a) Red component of the plain Jet plane. (b) Green component of the plain Jet plane. (c) Blue component of the plain Jet plane. (d) Red component of the cipher Jet plane. (e) Green component of the cipher Jet plane. (f) Blue component of the cipher Jet plane.

4.5. Information entropy analysis

Information entropy is often used to measure the randomness of the system. For information source m, the calculation formula of information entropy $H(m)$ is

$$H(m) = \sum_{i=0}^{2^n-1} p(m_i)\log\frac{1}{p(m_i)}, \tag{18}$$

where $p(m_i)$ represents the probability of occurrence of gray value m_i. For the real random signal 2^n, its information entropy is n. It is predictable to some extent if the cipher $H(m)$ information entropy is smaller than n.

The information entropy of the plain and cipher images is shown in Table 3, and the comparison of different algorithms is illustrated in Table 4.

Table 3. Entropy of the cipher images.

Cipher image	Channels			Average
	R	G	B	
Lena	7.9992	7.9993	7.9993	7.9993
Baboon	7.9995	7.9991	7.9992	7.9993
Black	7.9993	7.9993	7.9993	7.9993
White	7.9988	7.9988	7.9988	7.9988

The results in Table 3 attest that the information entropy of the encrypted image is very close to the theoretical value, which shows that the encrypted image has good random distribution characteristics. In addition, Table 4 shows the comparison of the information entropy with other encryption technologies. The proposed algorithm is superior to those in Refs. [30,32,35–37], so the proposed encryption scheme has good security performance and can resist entropy analysis attacks.

Table 4. Entropy for different algorithms.

Algorithm	Information entropy
Lena	7.2718
Proposed algorithm	7.9993
Ref. [30]	7.9974
Ref. [35]	7.9975
Ref. [36]	7.9880
Ref. [32]	7.9997
Ref. [37]	7.9973

4.6. Noise attack

In the process of image transmission, encrypted images may be subject to various attacks. Therefore, a reliable encryption scheme can effectively improve the image's anti-attack capability. Figure 15 shows the result of decrypting the cipher images with salt and pepper noise (SPN). Figures 15(a), 15(b), 15(c) show the baboon image encrypted by adding 1%, 2% and 5% SPN, respectively, and Figs. 15(d), 15(e), 15(f)

show the corresponding decrypted image. According to the decrypted images, as the number of state variables increases, the plain image becomes noisier. The plain image can still be distinguished when the variable is 0.001, suggesting that the encryption technique can withstand noise assaults.

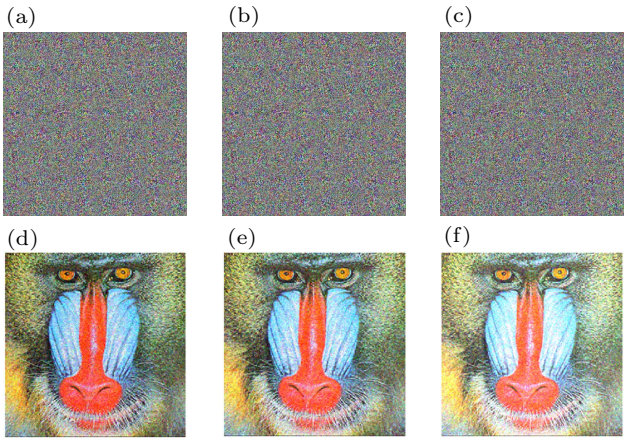


Fig. 15. Cipher and decryption images with SPN. (a) Cipher image with 1% SPN, (b) cipher image with 2% SPN, (c) cipher image with 5% SPN, (d) decrypted image with 1% SPN, (e) decrypted image with 2% SPN, (f) decrypted image with 5% SPN.

4.7. Efficiency analysis

Under the similar working environment, the encryption time cost of the proposed algorithm is compared with that of the existing color image encryption algorithm, which is presented in Table 5. The comparison of the results shows that even when processing large-scale data, the run time of the proposed model is short. Therefore, the proposed algorithm is more efficient. Due to the times being heavily dependent on computer and hardware used, so Table 5 is not meant for comparison, but rather a rough account of computation time.

Table 5. Encryption time comparison.

Algorithms	Size (Kb)	Time (s)
Proposed algorithm	256	0.889
Ref. [38]	–	1.750
Ref. [39]	263	3.780
Ref. [40]	–	1.222
Ref. [41]	358	0.221

5. Conclusion

This paper presents a color image encryption algorithm based on 3D DCT and a coupled chaotic system. Two sequences are generated using a novel two-dimensional chaotic mapping: one for generating the embedding matrix and the other for obtaining the encryption matrix. The Lyapunov exponents and numerical change rates demonstrate that the chaotic system exhibits excellent chaotic characteristics and pseudo-randomness. By incorporating a new scrambling algorithm, the security of the ciphertext image is significantly enhanced. Simulation results indicate that the algorithm effectively reduces the statistical characteristics of the image through frequency domain encryption. Correlation analysis of adjacent pixels reveals that this algorithm can significantly decrease the correlation between adjacent pixels, suggesting that the algorithm is resistant to chosen-plaintext attacks.

Finally, the transmission of images is often compressed and converted. Other encryption techniques can be combined with frequency-domain encryption so that the encryption algorithm has anti-compression properties. At the same time, it can reduce the noise interference in the process of image transmission, and achieve a more effective and safe encryption process.

Acknowledgements

Project supported by the National Natural Science Foundation of China (Grant Nos. 62105004 and 52174141), the College Student Innovation and Entrepreneurship Fund Project (Grant No. 202210361053), Anhui Mining Machinery and Electrical Equipment Coordination Innovation Center, Anhui University of Science & Technology (Grant No. KSJD202304), and the Anhui Province Digital Agricultural Engineering Technology Research Center Open Project (Grant No. AHSZNYGC-ZXKF021).

References

[1] Farajallah M, Assad S E and Deforges O 2018 *Multimedia Tools Appl.* **77** 28225
[2] Wen H, Yu S and Lü J 2019 *Entropy* **21** 246
[3] Zhu C and Sun K 2018 *IEEE Access* **6** 18759
[4] Sneha P S, Sankar S and Kumar A S 2020 *J. Ambient Intell. Humanized Comput.* **11** 1289
[5] Xiong Z, Wu Y , Ye C H, Zhang X M and Xu F 2019 *Multimedia Tools Appl.* **22** 31035
[6] Xian Y, Wang X, Yan X, Li Q and Wang X 2020 *Optics and Lasers in Engineering* **134** 106202
[7] Wu H S, Zhu H Y and Ye G D 2021 *Phys. Scr.* **96** 105202
[8] Sun F Y and Lv Z W 2021 *Multimedia Tools Appl.* **81** 3959
[9] Du S and Ye G 2023 *Alexandria Engineering Journal* **66** 979
[10] Faragallah O S, El-sayed H S, Afifi A and El-Zoghdy S F 2021 *Wireless Personal Communications* **118** 1559
[11] Elashry I F, El-Shafai W, Hasan E S, El-Rabaie S, Abbas A M, Abd El-Samie F E and Faragallah O S 2020 *Multimedia Tools Appl.* **79** 20665
[12] Gong L H, Luo H X, Wu R Q and Zhou N R 2022 *Physica A* **591** 126793
[13] Gong L H and Luo H X 2023 *Opt. Laser Technol.* **167** 109665
[14] Lai Q and Chen Z J 2023 *Chaos, Solitons & Fractals* **170** 113341
[15] Lai Q and Liu Y 2023 *Expert Syst. Appl.* **223** 119923
[16] Zhao Y and Liu L 2021 *Entropy* **23** 1127
[17] Zhou N R, Tong L J and Zou W P 2023 *Signal Processing* **211** 109107
[18] Zhou M J and Wang C H 2020 *Signal Processing* **171** 107484
[19] Zhou N R, Hu L L, Huang Z W, Wang M M and Luo G S 2024 *Expert Syst. Appl.* **238** 122052
[20] Wang T and Wang M H 2020 *Optics & Laser Technology* **132** 106355
[21] Ghadirli H M, Nodehi A and Enayatifar R 2019 *Signal Processing* **164** 163
[22] Joshi A B, Kumar D, Mishra D C, *et al.* 2020 *Journal of Modern Optics* **67** 933
[23] Ma Y, Li N, Zhang W, *et al.* 2021 *Optics Express* **29** 28338

[24] Cheng J, Xie C, Bian W, *et al.* 2012 *Pattern Recognition Letters* **33** 476
[25] Wang X, Liu C and Jiang D 2021 *Information Sciences* **574** 505
[26] Guleria V and Mishra D C 2021 *Fractals* **29** 2150151
[27] Suman R R, Mondal B and Mandal T 2022 *Multimedia Tools Appl.* **81** 27089
[28] Faure P and Korn H 1998 *Phys. D* **122** 265
[29] Chen L, Yin H, Yuan L, Machado JAT, Wu R and Alam Z 2021 *Signal Processing: Image Communication* **97** 116363
[30] Zhou J, Zhou N R and Gong L H 2020 *Optics and Laser Technology* **131** 106437
[31] Li Z, Peng C G, Tan W and Li L 2020 *Symmetry* **12** 1497
[32] Wen W Y, Wei K K, Zhang Y S, *et al.* 2020 *Nonlinear Dynam.* **99** 1587
[33] Hong Y, Fang S, Su J, Xu W, Wei Y, Wu J and Yang Z 2023 *Comput. Mater. Contin.* **77** 139
[34] Teng L, Wang X, Yang F, *et al.* 2021 *Nonlinear Dynam.* **105** 1859
[35] Wang T and Wang M H 2020 *Optics and Laser Technology* **132** 106355
[36] ElKamchouchi D H, Mohamed H G and Moussa K H 2020 *Entropy* **22** 2
[37] Luo H B and Ge B 2019 *Multimedia Tools Appl.* **78** 34323
[38] Jin X, Zhu S Y, Xiao C E, Sun H B, Li X, Zhao G and Ge S M 2017 *Sci. China Inf. Sci.* **60** 122107
[39] Xu J, Zhao C and Mou J 2020 *IEEE Access* **8** 145995
[40] Sun J 2021 *Modern Physics Letters B* **35** 2150465
[41] Gao S, Wu R, Wang X, Wang J, Li Q, Wang C and Tang X 2023 *Signal Processing* **202** 108745