A color image encryption algorithm with a novel coupled chaotic system and 3D-DCT

Yan Wen (wenyan@hainanu.edu.cn)
Anhui University of Science and Technology https://orcid.org/0000-0001-8606-9639
jingming Su
Anhui University of Science and Technology
Yan Hong
Anhui University of Science and Technology
Pingshun Gong
Anhui University of Science and Technology

Research Article

Keywords: color image encryption, 3D-DCT, chaos, coupled system

Posted Date: March 11th, 2022

DOI: https://doi.org/10.21203/rs.3.rs-1426094/v1

A color image encryption algorithm with a novel coupled chaotic system and 3D-DCT

Abstract

In order to improve the security of image transmission and reduce the complexity of encryption algorithm, an efficient color image encryption algorithm is developed based on 3D-DCT and coupled chaotic system. Firstly, the plain color image is decomposed into three grayscale plain images, which are transformed by DCT to obtain the corresponding frequency coefficient matrices. Then, the novel 2-D chaotic system is designed and used to generate the embedded matrices, which is implanted to the frequency coefficient matrices and forms the embedded frequency coefficient matrices. And then, the embedded matrices were scrambled and encrypted by Diagonal scrambling method and the encryption matrix generated by the 2-D chaotic system respectively, which resulted in the production of the ultimate color cipher image. In order to meet the requirement of the era of big data, the hash function SHA-256 is introduced to generate the key of encryption algorithm. This scheme is thoroughly validated on different sized plain-images with modern statistical analyses to prove the security and sensitivity. Eventually, compared with other schemes further demonstrates its competence and superiority in robustness and anti-interference.

Key words: color image encryption · 3D-DCT · chaos · coupled system

Authors information:

First author: Wen Yan[1], email:wenyan@hainanu.edu.cn

corresponding author: SU Jingming*[1], email:su_jingming@163.com

second author: Hong Yan[1], email: hong5212724@163.com

Third author: Gong Pingshun[1], email:2506021415@qq.com

Acknowledgment:

This work was supported by Anhui Natural Science Fund Project (No.1808085MF169,No. 2108085ME158) .

[1] Anhui university of science and technology, Huainan 232001, China

1. Introduction

With the development of network technology, multimedia information transmission is becoming more and more common, and image transmission security is also facing various forms of threats, such as differential attack, chosen plaintext attack[1-3], violent resolution, etc. Therefore, ensuring the security of image transmission is the research direction of many scholars in recent years[4, 5].

Different from text information, traditional information encryption techniques such as RSA, AES, IDEA[6-8] are not suitable for image transmission due to the large amount of image data and the strong correlation between adjacent pixels[4, 9]. In 1990s，Matthews and Robert proposed a chaotic sequence cipher scheme based on Logistic map. Since then, the image encryption algorithm based on chaotic mapping has been widely used in the field of image encryption[10-12]. Because the chaotic system has the characteristics of pseudo-random, unpredictable, initial value and parameter sensitivity, so researchers construct a variety of image encryption algorithms. Yao et al. [13] introduce an algorithm using 4-pixel structure based on chaotic systems. In the confusion stage, a new structure is used to scramble the pixel position, and the chaotic sequence generated by the linear chaotic system is used to encrypt the pixel value to obtain the final ciphertext image. Zhao et al. [14] proposed an image encryption by using double chaotic system. Compared with the classical chaotic map, the proposed quadratic map has a larger Lyapunov exponent, which means it has better chaotic characteristics and unpredictability. Nevertheless, low-dimensional chaotic map systems have shortcoming of a limited range of chaotic sequences and poor safety, while high-dimensional chaotic systems have more parameters, large chaotic sequence space[11, 15-17]. Wang et al. [18] used a six-dimensional hyperchaotic image encryption algorithm based on DNA operation and bit level alignment, and the horizontal displacement makes the algorithm has better security.

In addition, many image encryption schemes in spatial and frequency domains have been proposed. First, use various transforms, such as the fast Fourier transform(FFT)[18], discrete wavelet transform(DWT)[19], Discrete Cosine Transform (DCT)[20] to map the plain image to a frequency coefficient matrix,

then these coefficients are scrambled, the corresponding inverse transform is performed on the scrambled coefficient matrix to generate the final cipher image. Cheng et al. [21] proposed an image hiding algorithm based on DCT, however, the algorithm encrypts and embeds single images, which cannot meet the requirement of the era of big data. Wang et al. [22] proposed an image encryption and hiding algorithm based compressive sensing(CS) and DCT transform. First, the grayscale plain images are represented by the DWT, then the sparse matrices are scrambled by the index sort scrambling and zigzag scrambling. The measurement matrix generated by the 2D chaotic system. Finally, the compressed matrices are embedded into a color carrier image using 3D DCT to get a cipher image.

To summarize the above, in order to improve the security and reduce the complexity of chaotic system, an image encryption algorithm based on 3D DCT and coupled chaotic system is proposed. The new 2D chaotic system based on combination of Logistic mapping and Henon mapping, which is analyzed with Lyapunov exponent, numerical change rate, bifurcation diagram. The results showed improved chaotic mapping exhibits better chaotic characteristics and random. Based on the new 2D chaotic mapping, we generated embedding matrices and encryption matrices. In addition, a new scrambling algorithm is proposed. Compared with the traditional algorithm, as Arnold scrambling[23], circular scrambling and zigzag scrambling[24], the pixel position transformation is more random and unrecoverable. After the image is destroyed, most of the effective information can be retained, and it is visually imperceptible. In the encryption process, the preprocessed scrambled image is transformed into the frequency domain through 3D DCT, and the embedding matrix generated by the 2D chaotic system is embedded into the frequency domain image. By embedding the encryption matrix in the frequency domain, better encryption quality and visual security can be provided, and better robustness can also be obtained. Then the final ciphertext image is obtained by combining IDCT operation and encryption matrix. The simulation results show that compared with other algorithms, this algorithm has better encryption characteristics, larger key space and security.

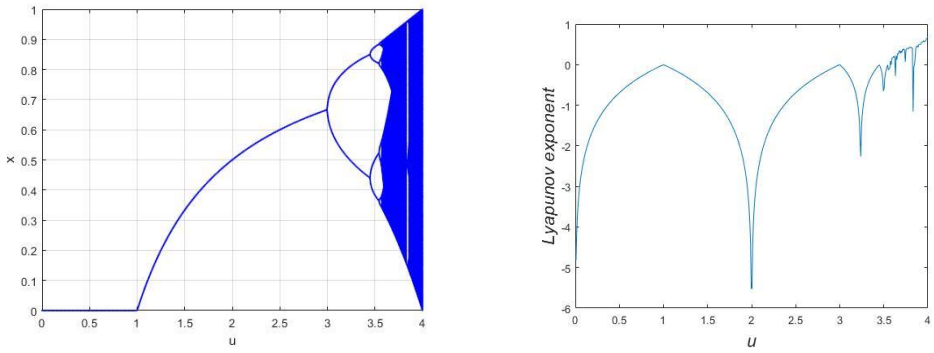
2. Relevant knowledge

2.1 Logistic mapping

Logistic is one-dimensional chaotic system, although the mathematical form of the Logistic is sample, its dynamic behavior is complex, so it is widely used in the field of chaos[25]. It is described as Eq.(1):

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

where, u is the parameter of Logistic system, $x_i$is the chaotic sequence of the system. Where $u \in (3.56,4)$,the system is chaotic sate. The bifurcation diagram and the Lyapunov exponent are shown in Fig.1.



a b

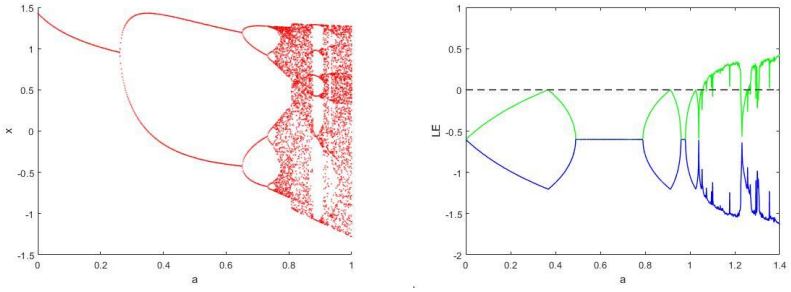
Figure 1.**(a)** Bifurcation diagram; **(b)** Lyapunov exponent diagram

2.2 Henon mapping

Henon is two-dimensional chaotic mapping, it has the characteristic of the simplicity, power spectrum density uniformity, and good relevance[26], etc. The corresponding mathematical is defined in Eq.(2):

$$\begin{cases} x_{n+1} = y_n - a \times x_n^2 + 1 \\ y_{n+1} = b \times x_n \end{cases} \tag{2}$$

where， a and b are the parameters of system. The bifurcation diagram and the Lyapunov exponent distribution of the Henon mapping are shown in Fig.2. The diagram shows that when a∈(1.07,1.4), b=0.3, the system is chaotic.



a b

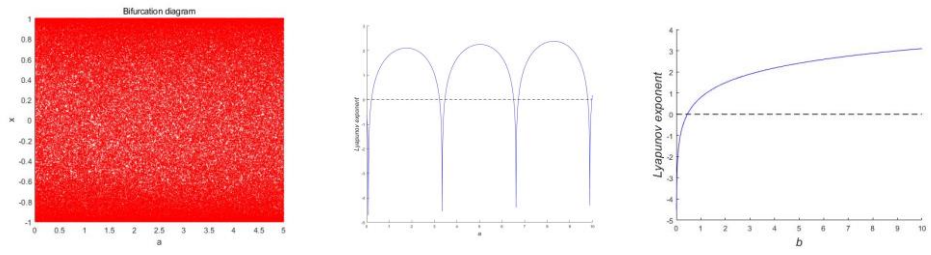
Figure 2. **(a)** Bifurcation diagram; **(b)** Lyapunov exponent diagram

2.3 Improved chaotic system based on Logistic and Henon mapping

Logistic and Henon have the following problems. For example, the sequences they generate have a strong correlation generally, the key space is small and the security is poor. In order to overcome these shortcomings, we propose a new 2D chaotic mapping system, which has better ergodicity and randomness, and improves the key space and security, as shown in Eq.(3).

$$f(x_{n+1},\ y_{n+1}) = \begin{cases} sin(\frac{y_n}{x_n} - a \times x_n^2 + a) \\ \frac{\pi}{2} \times arcsin(cos(b \times x_n)) \end{cases} \tag{3}$$

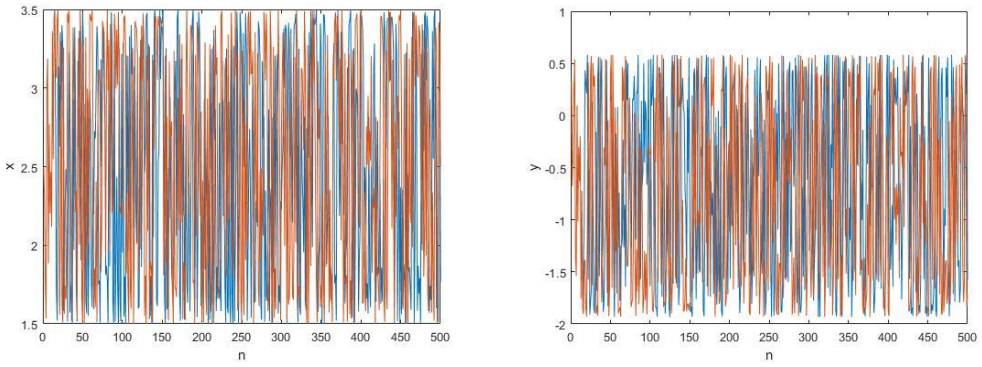
Fig.3 demonstrates the bifurcation diagram and Lyapunov exponent of the improved chaotic system based on Logistic and Henon mapping. Fig.3a shows the bifurcation diagram of the new chaotic system, which is more random and better chaotic characteristics than that of Logistic and Henon systems. Fig.3b and Fig.3c 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∈(0.3,3.1)， b∈(5,7). It is obvious that the parameter range of improved chaotic system has been significantly improved.



a b c

Figure 3. **(a)** Bifurcation diagram; **(b)** Lyapunov exponent diagram of parameter a; **(c)** Lyapunov exponent diagram of parameter b

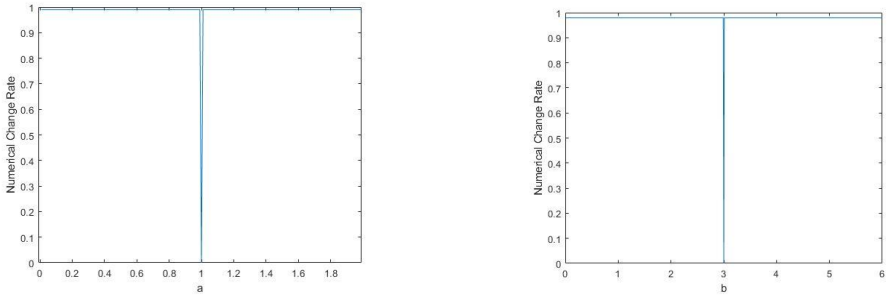
A good chaotic system should have the characteristics of initial value sensitivity and parameter sensitivity. Fig. 4 shows the iterative trajectory diagram of small changes in the initial value of the system. We set parameters and initial values x_0=0.256, y_0=0.3218, a=2.5,b=6.8, Fig.4a and Fig.4b respectively show the mapping trajectories when x_0=0.256+10^{-14} and y_0=0.3218+10^{-14}, which show the figure that after a few iterations, the sequence is very different, indicating that the system has a strong initial value sensitivity.



a b

Figure 4. **(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}

When the initial parameters a = 1 and b = 3 of the chaotic system are set, Fig. 5a and Fig. 5b show the data change rate of the chaotic sequence when the system parameters a and b are slightly changed. It can be seen that the new chaotic sequence has good randomness and unpredictability compared with Logistic and Henon mapping.



a b

Figure 5.Numerical change rate of parameter a and b

3. Algorithm description

3.1 SHA-256 function

In order to improve the security of the algorithm and the correlation between key and plaintext image, the algorithm uses hash function to generate system parameters and encryption. Divide the 265-bit key K into 8-bit blocks, which can be express as K=k_1, k_2,…, k_{32}, the parameters are generated according to the following Eq.(4) and Eq.(5):

$$\begin{cases} x_0 = \frac{mod(floor(k_1 \oplus k_2 \ldots \oplus k_8) \times 2^{10}, 256)}{256} \\ y_0 = \frac{mod(floor(k_9 \oplus k_{10} \ldots \oplus k_{16}) \times 2^{10}, 256)}{256} \end{cases} \tag{4}$$

$$\begin{cases} a = \frac{mod(fix(k_{17} \oplus k_{18} \ldots \oplus k_{24}) \times 2^{10}, 256)}{256} + x_0 \\ b = \frac{mod(fix(k_{25} \oplus k_{26} \ldots \oplus k_{32}) \times 2^{10}, 256)}{256} + y_0 \end{cases} \tag{5}$$

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

3.2 Diagonal scrambling

In this paper, we propose a new scrambling algorithm. The image pixels are scrambled in turn along the diagonal direction. 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. 6.

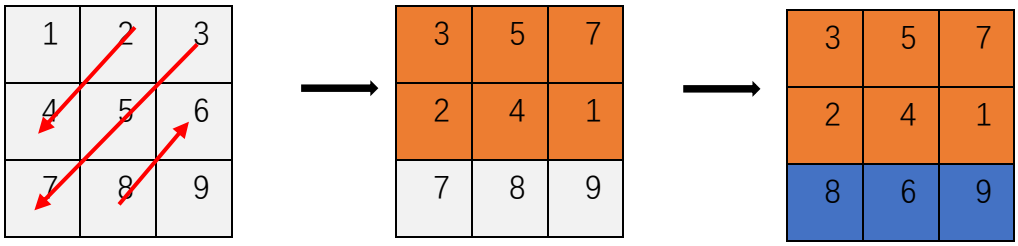


Figure 6. Scrambling method

After the diagonal is scrambled, the position of the pixel can be effectively changed. Fig.7 shows the recovery effect when the ciphertext image information is lost, which can still effectively restore the plaintext information after the image is destroyed.

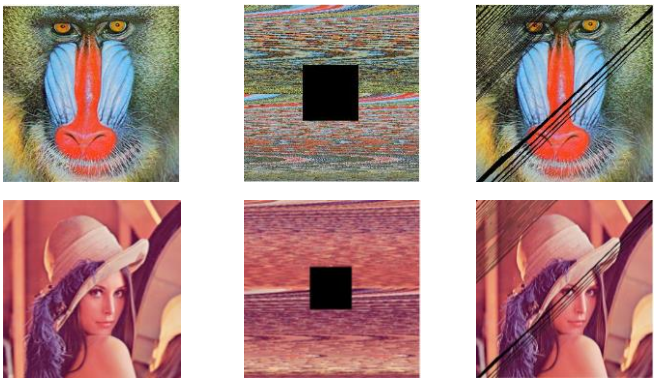


Figure 7. Scrambling performance of diagonal scrambling

3.3 3D DCT

DCT is Discrete Cosine Transform, signals in spatial domain are converted to frequency domain by sine function, which has good decorrelation performance and is mainly used to compress data or images. In this paper, 3D DCT transform is used to embed matrix in each channel of image. Firstly, 2D DCT transform is performed on the image, and then 1D DCT transform is performed again on this basis. 3D DCT transform and inverse transform are shown in Eq.(6)(7)(8), the size of three-dimensional matrix is n_x, n_y, n_z, f(x,y,z) represents the function value of a three-dimensional matrix at(x,y,z), F(x,y,z) represents the coefficients after applying the 3D DCT.

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

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

Where,

$$C(e) = \begin{cases} \sqrt{1/n_x}, & e = 0 \\ \sqrt{2/n_x}, & e \neq 0 \end{cases}$$

$$C(u) = \begin{cases} \sqrt{1/n_y}, & u = 0 \\ \sqrt{2/n_y}, & u \neq 0 \end{cases} \quad (8)$$

$$C(v) = \begin{cases} \sqrt{1/n_z}, & v = 0 \\ \sqrt{2/n_z}, & v \neq 0 \end{cases}$$

$$\mathrm{g(x,y,z)} = \frac{(2x+1)e\pi}{2n_x}\frac{(2y+1)u\pi}{2n_y}\frac{(2z+1)v\pi}{2n_z}$$

3.4 The encryption algorithm

In order to reduce the correlation between images and enhance the security of encryption algorithm, this paper mainly divides the encryption operation into two parts : frequency domain embedding and encryption. The flow chart of the encryption algorithm is shown in Fig.8. In the frequency domain embedding part, the specific operation is as follows :

Step 1. The R, G and B channels of plain image I(m× n × 3) are separated, and 8×8 data block is separated. When the plaintext image cannot be divided by 8, the image is filled with 0. DCT transform the image according to 8×8 data block to get f_r, f_g, f_b.

Step 2. Iteration m× 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'.

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

Step 3. The E_1',E_2',E_3' is correspondingly embedded into f_r, f_g, f_b to get ciphertext image of R,G and B channels, which are expressed as I_R,I_G and I_B. where, α is the gain factor, which can adjust the embedding intensity, it can be

adjusted according to the embedding effect.

$$\begin{cases} \mathrm{I_R} = \mathrm{f_r} + \alpha \times \mathrm{E}_1' \\ \mathrm{I_G} = \mathrm{f_g} + \alpha \times \mathrm{E}_2' \\ \mathrm{I_B} = \mathrm{f_b} + \alpha \times \mathrm{E}_3' \end{cases} \qquad (10)$$

Step 4. The 3D inverse discrete cosine transform(IDCT3) is applied to the three-dimensional matrix I_{RGB} to get cipher image in frequency domain S'(m× $n \times 3$),it is expressed as Eq.(11):

$$S' = floor(IDCT(I_{RGB})) \qquad (11)$$

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× n.

Step 2. The encryption matrices P_1', P_2', P_3' are using encrypt $\mathrm{S_R}$, S_G, S_B respectively, the operation as follow Eq.(12):

$$\begin{cases} M_R = bitxor(S_R, P_1') \\ M_G = bitxor(S_G, P_2') \\ M_B = bitxor(S_B, P_3') \end{cases} \qquad (12)$$

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.

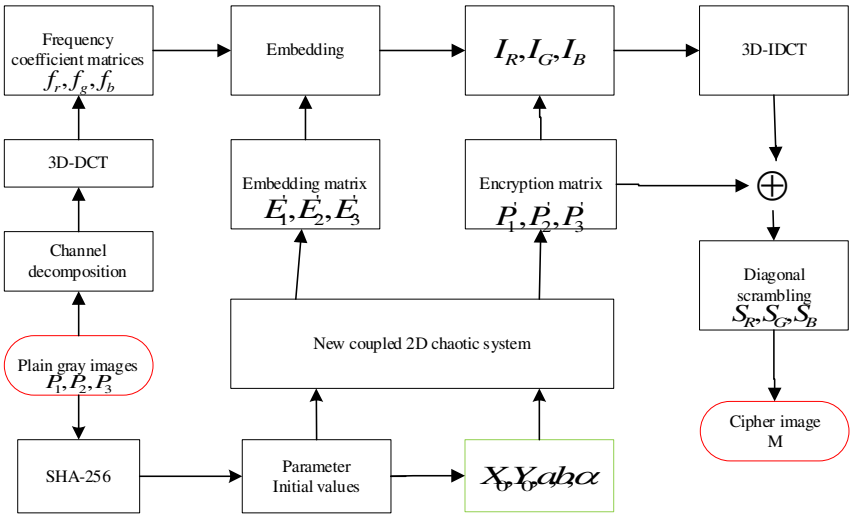


Figure 8. Flowchart of proposed encryption algorithm

4. Experimental results and safety analysis

The experimental simulation test is based on MATLAB R2020,the computer is configured with 1.6GHz CPU and 16GB 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 α=0.15. Fig 9 is the encryption results of four different color images using this encryption algorithm, namely Lena (512 × 512), Car (320 × 256), White (512 × 512), Black (512 × 512).

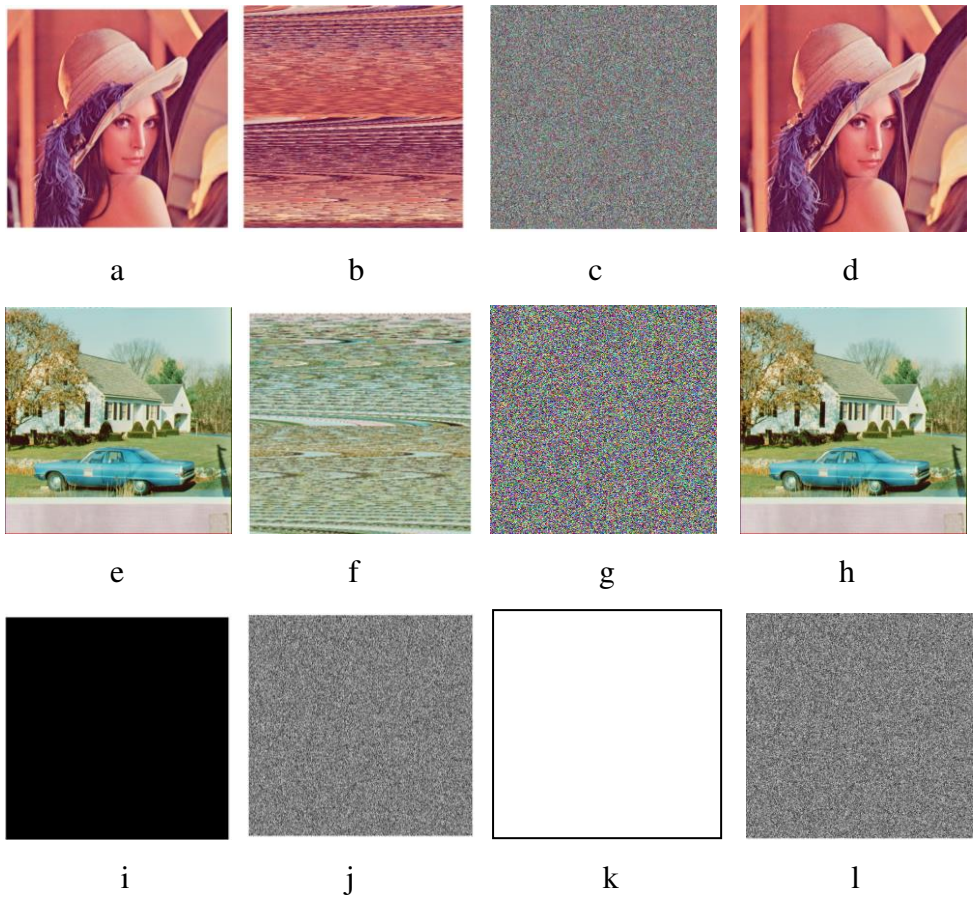


Figure 9. **(a)**,**(e)**,**(i)**,**(k)** are plain images; **(b)**,**(f)** are scrambling images;**(c)**,**(g)**,**(j)**,**(l)** are encryption images; **(d)**,**(h)** are decryption images

In Fig.9a, e, i, k are plaintext images, b and f are images after diagonal scrambling, c, g, j and l are the encrypted images, d and h are decrypted images of ciphertext images. It can be seen from Fig.9 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.

4.1 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 resisting 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:

$$\text{Key space} = 10^{14} \times 10^{14} \times 10^{14} \times 10^{14} \times 10^{14} = 10^{70} \approx 2^{232} \gg 2^{128}$$

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

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 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 as Eq.(13) and Eq.(14):

$$NPCR = \frac{1}{M \times N} \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} D(i,j) \times 100\% \qquad (13)$$

$$UACI = \frac{1}{M \times N} \left[\sum_{i=0}^{M-1} \sum_{j=0}^{N-1} \frac{|c_1(i,j) - c_2(i,j)|}{255} \right] \qquad (14)$$

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. For matrix D is expressed as Eq.(15).

$$D\ (i,\ j)\ = \begin{cases} 0, & C_1\ (i,\ j)\ = C_2\ (i,\ j) \\ 1, & C_1\ (i,\ j)\ \neq C_2\ (i,\ j) \end{cases} \qquad (15)$$

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.

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.[27]	Ref.[28]	Ref.[29]	Ref.[30]	Ref.[31]
Average NPCR	99.61433	99.6217	99.6158	99.6133	99.60	99.6135
Average UACI	33.488	33.4983	33.4494	30.36	33.37	33.4646

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.

4.3 Histogram analysis

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. In Fig.10b, e, i and l show the histogram of plaintext image, and in

Fig.10c, f, j and m show the histogram of their corresponding ciphertext. According to the histogram in Fig. 10, 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.

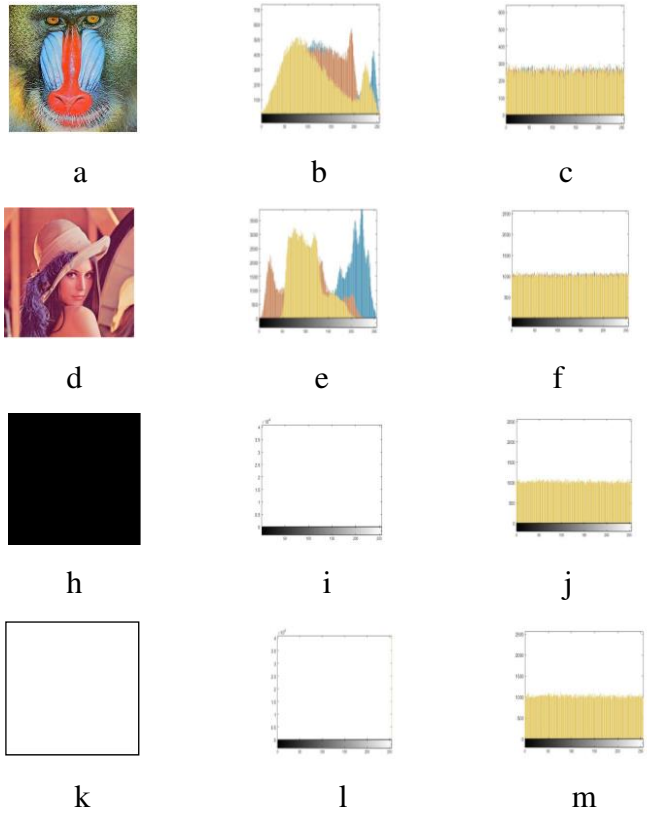


Figure 10. Result of encryption

4.4 Correlation analysis

In the plaintext images, the adjacent pixels in the horizontal, vertical and diagonal directions have 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 as Eq.(16):

$$r_{x,y} = \frac{E((x-E(x))(y-E(y)))}{\sqrt{D(x)\mathrm{D}(y)}}$$
$$E(x) = \frac{1}{\mathrm{N}}\sum_{i=1}^{N} x_i \qquad (16)$$
$$D(x) = \frac{1}{\mathrm{N}}\sum_{i=1}^{N}(x_i - E(x))^2$$

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 as Fig.11:

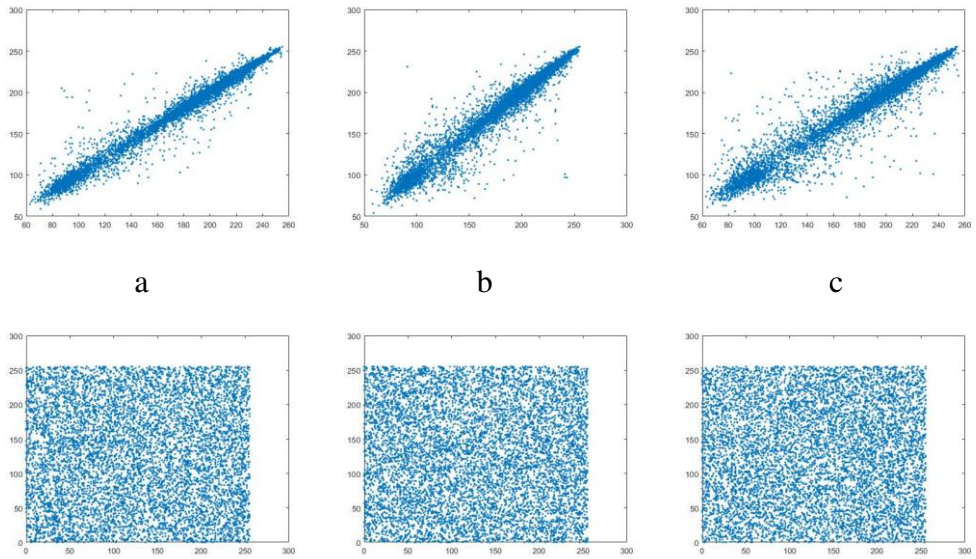


Figure 11. Correlation between adjacent pixels. (a) Horizontal correlation for plain Lena.(b) Vertical correlation for plain Lena. (c) Diagonal correlation for plain Lena. (d)Horizontal correlation for cipher Lena.(e) Vertical correlation for cipher Lena. (f) Diagonal correlation for cipher Lena.

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 as Eq(17):

$$H(m) = \sum_{i=0}^{2^n-1} p(m_i) \log \frac{1}{p(m_i)} \qquad (17)$$

here 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. Therefore, for the gray random image with gray value of 255, its bit plane depth is 8, so its theoretical information entropy is 8. If its ciphertext H (m) information entropy is less than N, it is predictable to a certain extent.

The entropy of the plain and cipher images is shown in Fig.12, and the comparison of other algorithms is illustrated in Table 3.

From the results, it can be seen that the value of information entropy of ciphertext images using the encryption algorithm is very close to the theoretical value, so the encryption algorithm has a good random distribution function for ciphertext images. In addition, the following table shows the comparison of the information entropy of the encryption algorithm with other encryption algorithms. It can be seen that the encryption algorithm is obviously stronger than other literature.

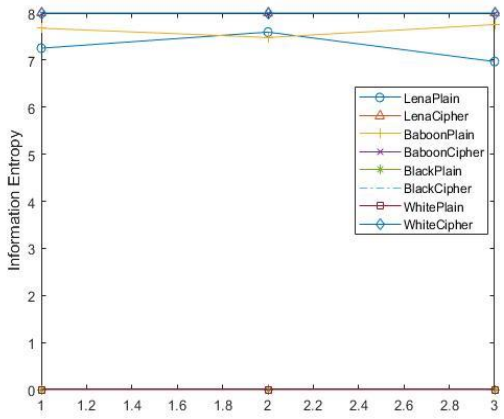


Figure 12. Entropy of the plain and cipher images

Table 3 Entropy for different algorithms

Algorithm	Information Entropy
Lena	7.2718
Proposed Algorithm	7.9993
Ref.[27]	7.9974
Ref.[32]	7.9975
Ref.[33]	7.9880
Ref.[29]	7.9997
Ref.[34]	7.9973

5. Conclusion

This paper proposed a color image encryption algorithm based on 3D DCT and coupled chaotic system. Two sequences are generated using a new 2D chaotic mapping: one to generate the embedding matrix, the other is to get encryption matrix. Lyapunov exponents and numerical change rate illustrate that the chaotic system has good chaotic characteristics and pseudo-random. Combined with the new scrambling algorithm, the security of ciphertext image is greatly improved. The simulation results show that the algorithm significantly reduces the statistical characteristics of the image by frequency domain encryption. Correlation analysis of adjacent pixels shows that this algorithm can well reduce the correlation of adjacent pixels, indicating that the algorithm can well resist the chosen plaintext attack.

Finally, the transmission of images is often compressed and converted. Other encryption technique can be combined with frequency-domain encryption, so that the encryption algorithm anti-compression property. 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.

References:

[1] M. Farajallah, S. El Assad, and O. Deforges, "Cryptanalyzing an image encryption scheme using reverse 2-dimensional chaotic map and dependent diffusion," Multimedia Tools and Applications, vol. 77, no. 21, pp. 28225-28248, Nov, 2018.

[2] H. Wen, S. Yu, and J. Lue, "Breaking an Image Encryption Algorithm Based on DNA Encoding and Spatiotemporal Chaos," *Entropy,* vol. 21, no. 3, Mar 5, 2019.

[3] C. Zhu, and K. Sun, "Cryptanalyzing and Improving a Novel Color Image Encryption Algorithm Using RT-Enhanced Chaotic Tent Maps," *Ieee Access,* vol. 6, pp. 18759-18770, 2018, 2018.

[4] P. S. Sneha, S. Sankar, and A. S. Kumar, "A chaotic colour image encryption scheme combining Walsh-Hadamard transform and Arnold-Tent maps," *Journal of Ambient Intelligence and Humanized Computing,* vol. 11, no. 3, pp. 1289-1308, Mar, 2020.

[5] Z. Xiong, Y. Wu, C. Ye *et al.*, "Color image chaos encryption algorithm combining CRC and nine palace map," *Multimedia Tools and Applications,* vol. 78, no. 22, pp. 31035-31055, Nov, 2019.

[6] H. Wu, H. Zhu, and G. Ye, "Public key image encryption algorithm based on pixel information and random number insertion," *Physica Scripta,* vol. 96, no. 10, Oct, 2021.

[7] F. Sun, and Z. Lv, "A secure image encryption based on spatial surface chaotic system and AES algorithm," *Multimedia Tools and Applications*, 2021.

[8] M. Khan, F. Masood, A. Alghafis *et al.*, "A novel image encryption technique using hybrid method of discrete dynamical chaotic maps and Brownian motion," *Plos One,* vol. 14, no. 12, Dec 19, 2019.

[9] Y. Xian, X. Wang, X. Yan *et al.*, "Image Encryption Based on Chaotic Sub-Block Scrambling and Chaotic Digit Selection Diffusion," *Optics and Lasers in Engineering,* vol. 134, Nov, 2020.

[10] X. Kang, and Z. Guo, "A new color image encryption scheme based on DNA encoding and spatiotemporal chaotic system," *Signal Processing-Image Communication,* vol. 80, Feb, 2020.

[11] N. Tsafack, J. Kengne, B. Abd-El-Atty *et al.*, "Design and implementation of a simple dynamical 4-D chaotic circuit with applications in image encryption," *Information Sciences,* vol. 515, pp. 191-217, Apr, 2020.

[12] S. Wang, C. Wang, and C. Xu, "An image encryption algorithm based on a hidden attractor chaos system and the Knuth-Durstenfeld algorithm," *Optics and Lasers in Engineering,* vol. 128, May, 2020.

[13] W. Yao, X. Zhang, Z. Zheng *et al.*, "A colour image encryption algorithm using 4-pixel Feistel structure and multiple chaotic systems," *Nonlinear Dynamics,* vol. 81, no. 1-2, pp. 151-168, Jul, 2015.

[14] Y. Zhao, and L. Liu, "A Bit Shift Image Encryption Algorithm Based on Double Chaotic Systems," *Entropy,* vol. 23, no. 9, Sep, 2021.

[15] M. Kaur, D. Singh, K. H. Sun *et al.*, "Color image encryption using non-dominated sorting genetic algorithm with local chaotic search based 5D chaotic map," *Future Generation Computer Systems-the International Journal of Escience,* vol. 107, pp. 333-350, Jun, 2020.

[16] M. J. Zhou, and C. H. Wang, "A novel image encryption scheme based on conservative hyperchaotic system and closed-loop diffusion between blocks," *Signal Processing,* vol. 171, Jun, 2020.

[17] S. Q. Zhu, and C. X. Zhu, "Secure Image Encryption Algorithm Based on Hyperchaos and Dynamic DNA Coding," *Entropy,* vol. 22, no. 7, Jul, 2020.

[18] C. Sun, E. Wang, and B. Zhao, "Image Encryption Scheme with Compressed Sensing Based on a New Six-Dimensional Non-Degenerate Discrete Hyperchaotic System and Plaintext-Related Scrambling," *Entropy,* vol. 23, no. 3, Mar, 2021.

[19] A. B. Joshi, D. Kumar, D. C. Mishra *et al.*, "Colour-image encryption based on 2D discrete wavelet transform and 3D logistic chaotic map," *Journal of Modern Optics,* vol. 67, no. 10, pp. 933-949, Jun, 2020.

[20] Y. Ma, N. Li, W. Zhang *et al.*, "Image encryption scheme based on alternate quantum walks and discrete cosine transform," *Optics Express,* vol. 29, no. 18, pp. 28338-28351, Aug 30, 2021.

[21] J. Cheng, C. Xie, W. Bian *et al.*, "Feature fusion for 3D hand gesture recognition by learning a shared hidden space," *Pattern Recognition Letters,* vol. 33, no. 4, pp. 476-484, Mar, 2012.

[22] X. Wang, C. Liu, and D. Jiang, "A novel triple-image encryption and hiding algorithm based on chaos, compressive sensing and 3D DCT," *Information Sciences,* vol. 574, pp. 505-527, Oct, 2021.

[23] V. Guleria, and D. C. Mishra, "MULTIPLE RGB IMAGE ENCRYPTION ALGORITHM WITH MULTILAYERS BY AFFINE HILL CIPHER WITH FRDCT AND ARNOLD TRANSFORM," *Fractals-Complex Geometry Patterns and Scaling in Nature and Society,* vol. 29, no. 06, Sep, 2021.

[24] X. Y. Wang, and N. N. Guan, "A novel chaotic image encryption algorithm based on extended Zigzag confusion and RNA," *Optics and Laser Technology,* vol. 131, Nov, 2020.

[25] R. R. Suman, B. Mondal, and T. Mandal, “A secure encryption scheme using a Composite Logistic Sine Map (CLSM) and SHA-256,” *Multimedia Tools and Applications*, 2022.

[26] L. Chen, H. Yin, L. Yuan *et al.*, “Double color image encryption based on fractional order discrete improved Henon map and Rubik's cube transform,” *Signal Processing-Image Communication,* vol. 97, Sep, 2021.

[27] J. Zhou, N. R. Zhou, and L. H. Gong, “Fast color image encryption scheme based on 3D orthogonal Latin squares and matching matrix,” *Optics and Laser Technology,* vol. 131, Nov, 2020.

[28] Z. Li, C. G. Peng, W. J. Tan *et al.*, “A Novel Chaos-Based Color Image Encryption Scheme Using Bit-Level Permutation,” *Symmetry-Basel,* vol. 12, no. 9, Sep, 2020.

[29] W. Y. Wen, K. K. Wei, Y. S. Zhang *et al.*, “Colour light field image encryption based on DNA sequences and chaotic systems,” *Nonlinear Dynamics,* vol. 99, no. 2, pp. 1587-1600, Jan, 2020.

[30] X. Zhang, L. Wang, G. Cui *et al.*, “Entropy-Based Block Scrambling Image Encryption Using DES Structure and Chaotic Systems,” *International Journal of Optics,* vol. 2019, Aug 15, 2019.

[31] L. Teng, X. Wang, F. Yang *et al.*, “Color image encryption based on cross 2D hyperchaotic map using combined cycle shift scrambling and selecting diffusion,” *Nonlinear Dynamics,* vol. 105, no. 2, pp. 1859-1876, Jul, 2021.

[32] T. Wang, and M. H. Wang, “Hyperchaotic image encryption algorithm based on bit-level permutation and DNA encoding,” *Optics and Laser Technology,* vol. 132, Dec, 2020.

[33] D. H. ElKamchouchi, H. G. Mohamed, and K. H. Moussa, “A Bijective Image Encryption System Based on Hybrid Chaotic Map Diffusion and DNA Confusion,” *Entropy,* vol. 22, no. 2, Feb, 2020.

[34] H. B. Luo, and B. Ge, “Image encryption based on Henon chaotic system with nonlinear term,” *Multimedia Tools and Applications,* vol. 78, no. 24, pp. 34323-34352, Dec, 2019.

Statement and Declarations

Funding

This work was supported by Anhui Natural Science Fund Project (No.1808085MF169,No. 2108085ME158) .

Competing Interests

The authors have no financial or proprietary interests in any material discussed in this article.

Author Contributions

All authors contributed to the study conception and design. Material preparation, data collection and analysis were performed by Wen yan. The first draft of the manuscript was written by Su Jingming and all authors commented on previous versions of the manuscript. All authors read and approved the final manuscript.

Data Availability

The datasets generated during and/or analyzsed during the current study are available from the corresponding author on reasonable request.