Journal of King Saud University – Computer and Information Sciences 35 (2023) 101660

HOSTED BY

Contents lists available at ScienceDirect

Journal of King Saud University – Computer and Information Sciences

journal homepage: www.sciencedirect.com

High-quality color image compression-encryption using chaos and block permutation

Heping Wen [a,b,*], Yiming Huang [a], Yiting Lin [a,b]

[a] University of Electronic Science and Technology of China, Zhongshan Institute, Zhongshan 528402, China
[b] School of Information and Communication Engineering, University of Electronic Science and Technology of China, Chengdu 611731, China

ARTICLE INFO

Article history:
Received 30 April 2023
Revised 20 June 2023
Accepted 15 July 2023
Available online 26 July 2023

Keywords:
Image encryption
Chaotic encryption
Compression and encryption
Frequency domain compression

ABSTRACT

This paper proposes a high-quality color image compression-encryption scheme based on chaos and block permutation. In this scheme, the color digital image is first converted and sampled in the YCbCr gamut, and then the coefficients in the sub-blocks are extracted for compression coding after 8×8 post-blocking discrete cosine transformation (DCT) to the frequency domain. Then, an image encryption algorithm using chaos-based block permutation and two-round row-column diffusion is designed for the compressed frequency domain information. In terms of security, a chaos-based block permutation module is designed, which includes the encryption operations of block scrambling, block rotation and inversion, pixel value complement and color component interchange to enhance security. In addition, a mechanism for associating plaintext and intermediate ciphertext is introduced to generate dynamic chaotic sequences to effectively resist various cryptographic attacks. Moreover, the joint compression-encryption reduces the computational complexity of the encrypted object significantly and improves the efficiency. The simulation results show that the joint compression-encryption scheme has the advantages of high compression ratio and high image recovery quality, and has a fairly high security level to resist common cryptographic attacks. Therefore, the compression-encryption scheme proposed in this paper is a preferred and promising method for protecting the privacy of digital images.

1. Introduction

The era of big data has arrived with the rapid development of computer and network communication technology (Farah et al., 2020; Zhang et al., 2020). As people enjoy the dividends of information, potential information security issues have gradually emerged (Zhou et al., 2015; Zhang et al., 2021). As the mainstream information transmission medium in today's big data network environment, digital image processing and security have become major concerns due to the vast amount of data being transmitted (Sisaudia and Vishwakarma, 2022; Zhang et al., 2023a). Thus, it is very essential to encrypt digital image before transmission (Zhang et al., 2023b; Li et al., 2022). Compared to traditional textual information, the large file size and high redundancy of digital image pose challenges for storage and transmission (Luo et al., 2022; Wang and Li, 2021; Wen et al., 2023a). In addition, traditional text encryption methods cannot be directly applied to digital image because of the unique characteristics of image (Li et al., 2022; Zhou et al., 2014). Therefore, more and more image encryption methods have been proposed, such as biological coding (Wen et al., 2022a; Wang and Li, 2021), frequency domain encryption (Wang et al., 2021a), quantum encryption (Luo et al., 2020; Singh et al., 2021), bit plane encryption (Shahna and Mohamed, 2020; Wei et al., 2023), steganography technique Abdulla et al. (2014), Abdulla et al. (2019, 2023) and so on (Yu et al., 2021; Chen, 2022a; Chen et al., 2022). Especially in the last few years, many international experts and scholars have discussed lively and achieved rich and profound results in image encryption (Gao et al., 2022a; Wang et al., 2023; Zhang et al., 2022; Chai et al., 2022a). A new encryption algorithm was proposed in 2021 which utilizes bit-level permutation and non-invertible chaotic mapping (Karawia and Elmasry, 2021). Experimental analysis shows that the proposed algorithm can resist multiple attacks. In the same

* Corresponding author at: University of Electronic Science and Technology of China, Zhongshan Institute, Zhongshan 528402, China.
E-mail addresses: wenheping@uestc.edu.cn (H. Wen), yiminghuangzsc@yeah.net (Y. Huang), Dr.YitingLin@gmail.com (Y. Lin).
Peer review under responsibility of King Saud University.

Production and hosting by Elsevier

https://doi.org/10.1016/j.jksuci.2023.101660
1319-1578/

year, a novel method for encrypting color image was proposed by some scholars (Qian et al., 2021). After comparing various performance indicators, it can be concluded that this technique is a suitable choice for image encryption. Based on the literature reviewed, it can be observed that most image encryption algorithms have achieved satisfactory confidentiality results, which greatly promote research in the field of information security (Wen et al., 2022b; Yuen and Wong, 2011). Unfortunately, most of the available studies rarely consider both high security and simultaneous optimization of encryption efficiency.

In order to address issues such as low transmission efficiency and insufficient encryption security for digital image. Driven by the big data era, some scholars have started to explore joint image compression techniques based on image encryption (Chen, 2022b; Wang et al., 2022a, Wang et al., 2022b). It has been reported that digital image encryption by joint compression can improve encryption efficiency and thus has a promising application (Gao et al., 2022b; Xian et al., 2022). A multi-image compression and encryption scheme based on quaternion discrete fractional Hartley transform and improved pixel adaptive diffusion was proposed (Ye et al., 2020a). The experimental analysis shows that the proposed scheme is feasible and has high encryption security performance. These studies are good attempts and provide some basis and insight for joint compression encryption. However, due to the lack of systematization, the existing schemes have various drawbacks and do not possess comprehensive excellent performance. There are three main problems with the existing mainstream digital image compression-encryption schemes: (1) the compression-encryption scheme ignores the security performance, and the image encryption algorithm is difficult to resist the selection of plaintext attacks; (2) the digital image cannot be restored with high quality after lossy compression and encryption, which affects the usability; (3) complex encryption operations often result in reduced efficiency, making it challenging to meet the real-time requirements of secure communication. To solve the aforementioned issues, an innovative high-quality color image compression-encryption scheme utilizing chaos and block permutation has been proposed. In this scheme, the color digital image is first converted and sampled in the color domain, and then the coefficients in sub-blocks are extracted for compression coding after 8×8 post-blocking DCT to the frequency domain. Subsequently, an image encryption algorithm using chaos-based block permutation and two-round row-column diffusion is devised for the frequency-domain information that has been compressed. The main innovative points and contributions of this paper are as follows:

i) As far as we know, The method introducing chaos-based block permutation into digital image compression-encryption was proposed by us for the first time. In our proposed scheme, the chaos-based block permutation module includes the encryption operations of block scrambling, block rotation and inversion, pixel value complement and color component interchange to enhance security.
ii) The joint compression encryption effectively reduces the computational complexity of the encrypted object. DCT and a series of compression coding methods in frequency domain processing are used to greatly reduce the redundancy of encrypted objects, thus improving the efficiency of the encryption scheme.
iii) A mechanism for associating plaintext and intermediate ciphertext is introduced to generate dynamic chaotic sequences to effectively resist various cryptographic attacks. Based on our existing research base in cryptanalysis (Wen et al., 2023b; Wen and Lin, 2023), targeted security enhancements are made to improve resistance to cryptographic attacks.
iv) The proposed encryption scheme has several advantages, including high compression rate, high image restoration quality, feasibility, ease of use, and high performance. Especially for the problem of restoration after lossy compression encryption, our experimental results verify that the scheme has the property of high quality restoration.

The following is the structure of this paper. Section 2 briefly describes the related basic principles of the algorithm. Section 3 details the proposed image compression-encryption scheme. Section 4 presents the experimental simulation results and analysis. The last section concludes this paper.

2. Related basic principles

2.1. Conversion and compression of color gamut

In traditional color image processing, RGB gamut is usually used, and the other is YCbCr gamut obtained by conversion based on the principle of three-color theory, as defined in Eq. (1)

$$\begin{cases} Y = 0.299 \times R + 0.587 \times G + 0.114 \times B \\ Cb = -0.1687 \times R - 0.3313 \times G + 0.5 \times B \\ Cr = 0.5 \times R - 0.4187 \times G - 0.0813 \times B \end{cases} \tag{1}$$

where Yrepresents the brightness of the color, while $Cb$and Crrepresent the blue and red differences of the color, respectively (Niu et al., 2019).

Because the human eyes is more likely to perceive light and dark details, it is not easy to distinguish color and chroma information. Considering this perception ability, in the sampling process, the three components of Y, Cb, and $Cr$are sampled 4:1:1, that is, the full sampling of the Ycomponent is kept, and take the pixel values on the odd rows and columns of the Cbcomponent and the even rows and columns of the Crcomponent, as shown in Fig. 1. After sampling, the amount of information in the $Cb$and Crcolor gamut is reduced to a quarter of the original, while also ensuring that the loss of visual effects is almost negligible.

DCT is one of the most important means of frequency domain compression with entropy retention, energy retention, decorrelation and energy concentration, which is commonly used in signal and digital image processing (Feng et al., 2023). Taking two-dimensional discrete cosine transform (2D-DCT) as an example, if there is a set of two-dimensional array $\{X(u, v)|u = 0, 1, \cdots, U-1; v = 0, 1, \cdots, V-1\}$, then the expression of 2D-DCT is given by

$$Y(k, l) = C(k)C(l)\sum_{u=0}^{U-1}\sum_{v=0}^{V-1}X(u, v)cos\frac{(2u+1)k\pi}{2U}cos\frac{(2v+1)k\pi}{2V} \tag{2}$$

where $k = 0, 1, 2, \cdots, U-1; l = 0, 1, 2, \cdots, V-1$.

$$C(k) = \begin{cases} \sqrt{\frac{1}{U}} & k = 0 \\ \sqrt{\frac{2}{U}} & else \end{cases} \tag{3}$$

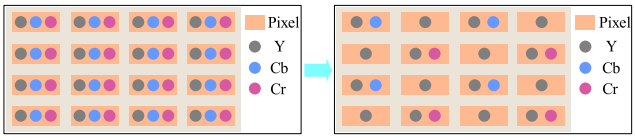


Fig. 1. An example for YCbCr gamut compression of 4×4 image matrix.

$$C(l) = \begin{cases} \sqrt{\frac{1}{V}} & l = 0 \\ \sqrt{\frac{2}{V}} & else \end{cases} \tag{4}$$

The two-dimensional inverse discrete cosine transform (2D-IDCT) is defined as

$$X(u,v) = \sum_{k=0}^{U-1}\sum_{l=0}^{V-1} C(k)C(l)Y(k,l)cos\frac{(2u+1)k\pi}{2U}cos\frac{(2v+1)l\pi}{2V} \tag{5}$$

After the DCT, the pixel values of the image in the time domain are converted to DCT coefficients in the frequency domain, unlike the fast Fourier transform (FFT), this transformation saves arithmetic power and the transformation results are all real numbers. In this paper, the image will be processed in 8×8 blocks and then DCT will be performed block by block. Fig. 2 gives an visualization examples of 8×8 matrix data before and after DCT. It can be seen that through the mapping of this function, the image energy in the frequency domain is concentrated in the first coefficient in the top left corner. This coefficient is usually called the DC coefficient, and the rest elements are called the AC coefficient. In addition, in this transformation, the low-frequency signals are concentrated in the top left corner of the DCT coefficient matrix, while the high-frequency signals are concentrated in the lower right corner. Given the insensitivity of the human eye to high-frequency information, DCT paves the way for a lossy compression step of discarding some high frequency signals in subsequent quantization.

2.2. Adaptive 4-D autonomous hyperchaotic system

Applying controllers k_1x_4, k_2x_4, k_3x_4 to the state equation of 3-D chaotic system, and setting $\dot{x_4} = -dx_1$, the following adaptive 4-D autonomous hyperchaotic system used in this paper can be constructed (Li and Yu, 2012).

$$\begin{cases} \dot{x_1} &= a(x_2 - x_1) + k_1x_4 \\ \dot{x_2} &= cx_1 - x_1x_3 + k_1x_4 \\ \dot{x_3} &= -bx_3 + x_1x_2 + k_3x_4 \\ \dot{x_4} &= -dx_1 \end{cases} \tag{6}$$

This system is 4-D and contains 2 nonlinear product terms, which satisfies the necessary conditions to generate hyperchaotic system. If the values are $a = 35, b = 3, c = 35, k_1 = 1, k_2 = 0.2, k_3 = 0.3, d = 5$, the Lyapunov exponent of the system is $LE_1 = 0.5, LE_2 = 0.2117, LE_3 = 0, LE_4 = -38.7068$, and thus the system exhibits hyperchaotic behavior at this time.

3. The proposed image compression-encryption scheme

The flowchart of the color image compression-encryption scheme proposed in this paper is shown in Fig. 3, and the specific encryption steps are described below.

3.1. Image compression-encryption

Step1: Extract the key associated with the plaintext and generate chaotic sequences By inputting the plain image and obtaining the MD5 value of the plain image, it is encoded as a key that conforms to the chaotic initial value interval. The chaotic system is generated by the key to obtain four chaotic sequences R^1, R^2, R^3, R^4, and then transformed into pseudo-random sequences suitable for block permutation after the following mathematical processing.

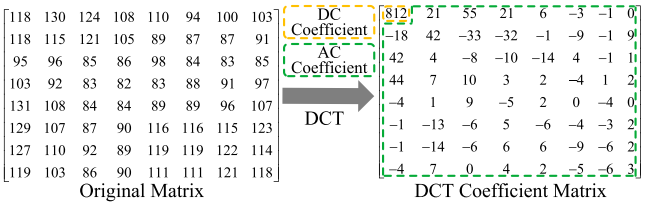


Fig. 2. Visualization examples of 8×8 matrix data before and after DCT.

$$\begin{cases} R^1 = mod(\lfloor R^1 \times 10^{10} \rfloor, \frac{L}{64}) \\ R^2 = mod(\lfloor R^2 \times 10^{10} \rfloor, 6) \\ R^3 = mod(\lfloor R^3 \times 10^{10} \rfloor, 2) \\ R^4 = mod(\lfloor R^4 \times 10^{10} \rfloor, 6) \end{cases} \tag{7}$$

where $\lfloor \cdot \rfloor$ is an integer-valued function, $mod(\cdot)$ is a modulo function, and L is the length of a chaotic sequence.

Step2: Convert color gamut and then sample.

Firstly, the plain image is converted from RGB gamut to YCbCr gamut, keeping the Y layer unchanged, and the $Cb$and Crlayers are blocked 2×2 respectively. Then take the pixel value in the top left corner of each block area in Cb, and the pixel value in the lower right corner of each block area in Cr, so that the sampled $Cb$and Crlayers are reduced to one-fourth in equal proportion to the original image.

Step3: Shift time domin and perform DCT coding.

To comply with the DCT symmetry interval, the pixel values of each layer after sampling were shifted by 128 so that the interval was distributed at $[-127, 128]$. Subsequently, the three layers are divided into multiple non-overlapping pixel blocks of 8×8 from left to right and from top to bottom respectively. Finally, the sub-blocks are DCT block by block. Through this operation, the image information is converted to the frequency domain.

Step4: Quantify The quantization is performed separately for each sub-block after DCT. As defined in Eq. (8)

$$\begin{cases} I'_Y = round(\frac{I_Y}{Q_Y}) \\ I'_C = round(\frac{I_C}{Q_C}) \end{cases} \tag{8}$$

where $round(\cdot)$ is the rounding function, I_Y, I_C are 8×8 sub-blocks on the brightness and color difference layers, respectively. Q_Y is the brightness standard quantization matrix, and Q_C is the color difference standard quantization matrix. I'_Y and I'_C are the quantized brightness and color difference matrices, respectively. The definitions of Q_Y and Q_C are as follows.

$$Q_Y = \begin{bmatrix} 16 & 11 & 10 & 16 & 24 & 40 & 51 & 61 \\ 12 & 12 & 14 & 19 & 26 & 58 & 60 & 55 \\ 14 & 13 & 16 & 24 & 40 & 57 & 69 & 56 \\ 14 & 17 & 22 & 29 & 51 & 87 & 80 & 62 \\ 18 & 22 & 37 & 56 & 68 & 109 & 103 & 77 \\ 24 & 35 & 55 & 64 & 81 & 104 & 113 & 92 \\ 49 & 64 & 78 & 87 & 103 & 121 & 120 & 101 \\ 72 & 92 & 95 & 98 & 112 & 100 & 103 & 99 \end{bmatrix} \tag{9}$$

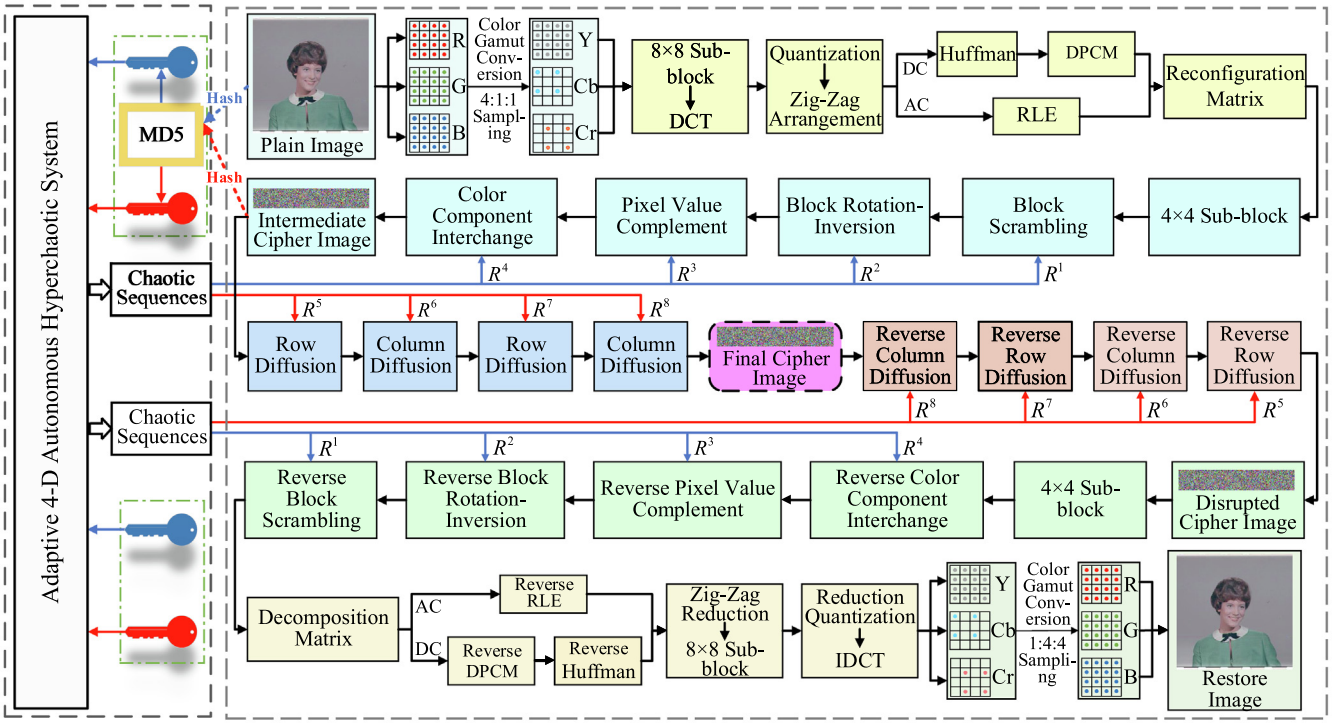


Fig. 3. The flowchart of the proposed color image compression-encryption scheme.

$$Q_C = \begin{bmatrix} 17 & 18 & 24 & 47 & 99 & 99 & 99 & 99 \\ 18 & 21 & 26 & 66 & 99 & 99 & 99 & 99 \\ 24 & 26 & 56 & 99 & 99 & 99 & 99 & 99 \\ 47 & 66 & 99 & 99 & 99 & 99 & 99 & 99 \\ 99 & 99 & 99 & 99 & 99 & 99 & 99 & 99 \\ 99 & 99 & 99 & 99 & 99 & 99 & 99 & 99 \\ 99 & 99 & 99 & 99 & 99 & 99 & 99 & 99 \\ 99 & 99 & 99 & 99 & 99 & 99 & 99 & 99 \end{bmatrix} \tag{10}$$

Step5: Extract coefficient and compress coding into binary sequences.

Zig-Zag scans each quantized sub-block into a 1-D array, taking the first digit as the DC coefficient and the remaining value as the AC coefficients. The DC coefficients of each sub-block in the same layer are taken out to form a first-order row matrix, Differential Pulse Code Modulation and Huffman Coding are performed to obtain three binary bitstreams based on DC coefficients. Similarly, after AC coefficients of the same layer is taken out to form a first-order row matrix, Run-Length Encoding is carried out, and finally three binary bitstreams based on AC coefficientds are obtained.

Step6: Reconstruct binary sequences into compressed matrice After the three layers are compressed and encoded, six binary bitstreams are spliced together to form a binary matrix 8 times the length of the plaintext column. Then every 8 columns of binary numbers are converted to 1 column of decimal numbers. After that, the matrix is divided into three parts by rows and assigned to the three channels R, G and B, forming a compression matrix as shown in Fig. 4, where *Reshape* is the reconstruction function and *two2ten* stands for binary to decimal.

Step7: Block permutation.

The reconstructed compressed matrix is divided into n sub-blocks of size 4×4, which is not overlapping each other, and processed into a five dimensional array matrix containing the chunking information. The operation is as follows.

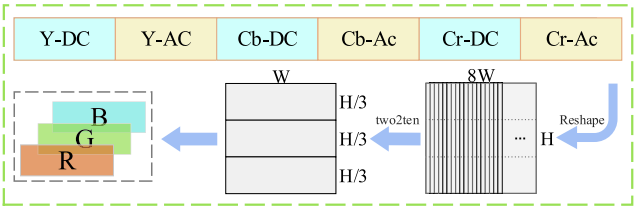


Fig. 4. The legend for reconstructing binary bitstreams into a compressed matrix.

$$P(a,b,c,d,e) = C((d-1)\times Bx+1,(e-1)\times Bx+1 : e\times Bx,c) \tag{11}$$

where a,b,c are the row, column and dimension of the pixel values in the sub-block, respectively, d,e are the row and column positions of the block, specifically. $d \times e = 1,2,\ldots,n$. Bx is the size of the pre-processing sub-block. Then, chaotic sequences R^1,R^2,R^3,R^4 generated by the plaintext associated key are used to carry out block scrambling, block rotation and inversion, pixel value complement and color component interchange for the n sub-blocks successively. As shown in Fig. 5, a 128×128 color Lena map is taken as an example to show the overall process of block permutation. The specific operation of each step is described as follows.

Firstly, block scrambling encryption is performed on the sub-blocks of P by chaotic sequence R^1 according to Eq. (12) as shown in Fig. 6.

$$\begin{cases} t = P(a,b,c,d) \\ P(a,b,c,d) = P(a,b,c,R^1(d)) \\ P(a,b,c,R^1(d)) = t \end{cases} \tag{12}$$

where $d$is the variable specified as $1,2,\ldots,n$.

The data in the sub-blocks is then encrypted by rotating and reversing it according to the integer chaos sequence R^2 with the interval [0,5], as shown in Fig. 7.

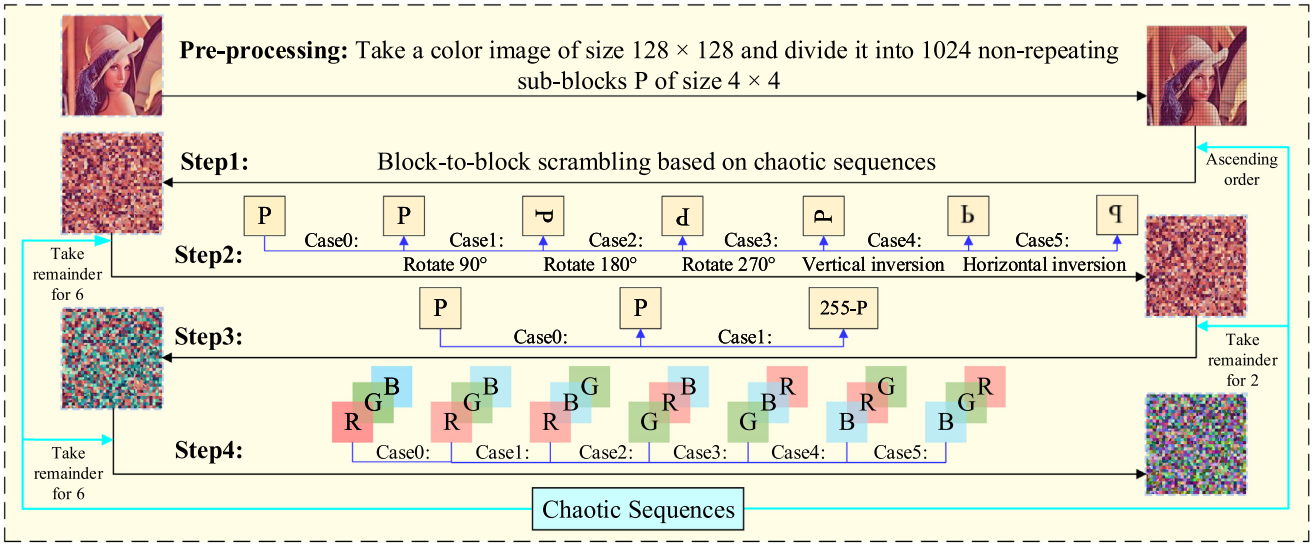


Fig. 5. The process diagram of block permutation.

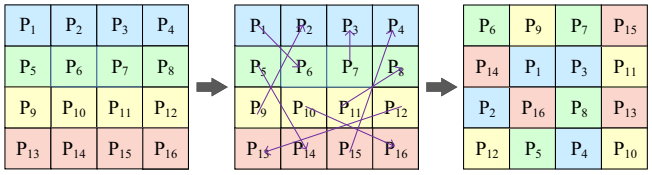


Fig. 6. An example of block scrambling of 16 sub-blocks.

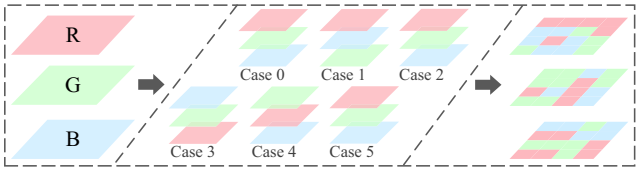


Fig. 8. An example of RGB color component interchange of 16 sub-blocks.

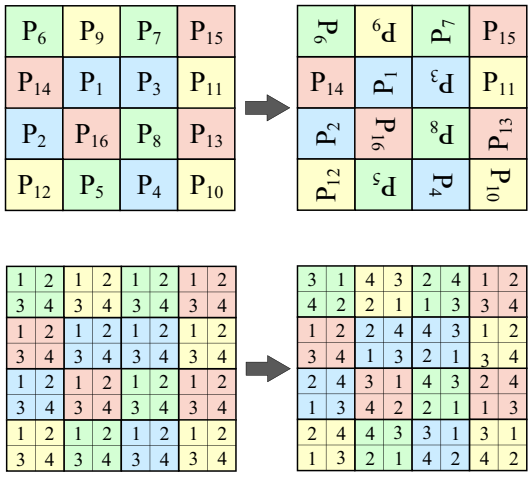


Fig. 7. An example of block rotation and inversion of 16 sub-blocks.

Next, the data in the sub-blocks is complemented with pixel values based on the binary chaotic sequence. The operation is as follows.

$$P(a,b,c,d,e) = 255 - P(a,b,c,d,e), \text{if} R^3(d \times e) = 1 \tag{13}$$

where a, b, c are the rows, columns and dimensions of the 5D array respectively. The specific value of $d \times e$ is $1, 2, \ldots, n$.

Finally, random permutations between R, G and B color stratifications are performed on the sub-block by an integer chaotic sequence R^4 with the interval [0,5], as in Fig. 8.

Step8: Extract the key associated with the ciphertext and generate chaotic sequences.

The four chaotic sequences R^5, R^6, R^7, and R^8 are obtained by inputting and associating the permutation ciphertext as shown in Step 1, and then transformed into a pseudo-random sequence suitable for rank diffusion. The operation is as follows.

$$\begin{cases} R^5 = mod\left(\lfloor R^5 \times (10^{32} - 1) \rfloor, 256\right) \\ R^6 = mod\left(\lfloor R^6 \times (10^{32} - 1) \rfloor, 256\right) \\ R^7 = mod\left(\lfloor R^7 \times (10^{32} - 1) \rfloor, 256\right) \\ R^8 = mod\left(\lfloor R^8 \times (10^{32} - 1) \rfloor, 256\right) \end{cases} \tag{14}$$

Step9: Row-column diffusion.

The four chaotic sequences are reconstructed into matrices of the same size as the dislocated image, R^5, R^6, R^7, R^8, and then the four matrices are used to perform two successive rounds of modulo and diffusion of the dislocated image (Zhu et al., 2019), and the diffusion result is denoted as D. This diffusion is defined as follows.

$$D_i = \begin{cases} (B_1 + B_T + \lfloor R \times 2^{10} \rfloor) mod 256 & if \quad i = 1 \\ (D_{i-1} + B_I + B_{i+1} + \lfloor R_i \times 2^{10} \rfloor) mod 256 & if \quad i = [2, T-1] \\ (D_{T-1} + B_T + \lfloor R_T \times 2^{10} \rfloor) mod 256 & if \quad i = T \end{cases} \tag{15}$$

for row diffusion, T is the number of rows, and B_i, D_i, and R_i represent the i-th row sequence of the permutated image, the diffused image and the chaotic matrix, respectively; while for column diffusion, T is the number of columns, and B_i, D_i and R_i represent the i-th column sequence of the scrambled image, the diffused image and the chaotic real matrix, respectively. After two rounds of row-column diffusion, the final color cipher image is obtained.

3.2. Image decryption-restoration

Using the opposite steps of compression-encryption, the cipher image is first subjected to two rounds of reverse row-column diffusion, and then reverse color component interchange, reverse pixel value complement, reverse block rotation-inversion and reverse block scrambling are performed one by one to obtain the frequency domain information before encryption. Afterwards the AC and DC coefficients of the frequency domain information are extracted for reverse compression coding and restore quantization, and then the image information in the time domain is changed by IDCT. Finally, the color difference layer is copied and relaid, and converted to RGB color gamut to obtain the restored image.

4. Results and analysis

4.1. Experimental platform

In terms of the experimental platform, we used a personal computer (PC) host with MATLAB R2022a experimental software installed. The processor of the PC is AMD Ryzen™ 9 5950X CPU; the main frequency is 3.88 GHz; the memory size is 16 GB; the hard disk size is 1 TB and the system is Windows10.

4.2. Statistical analysis

4.2.1. Histogram analysis

Given that the frequency of occurrence of the grey value of each pixel point in the image is counted in the histogram, it can easily be used by an attacker as a gateway to decrypt the image (Chai et al., 2022b). Therefore, the security performance of an image encryption scheme can be known from the histogram analysis. An excellent image encryption algorithm can manipulate the distribution of an image to resemble noise, thereby concealing the primary information of the image. As shown in Fig. 9, the selected images San Francisco and San Francisco (Bay Bridge) show a noise-like distribution in the histogram of the encrypted images after processing, eliminating the possibility of an attacker to obtain valid information from it.

4.2.2. Information entropy analysis

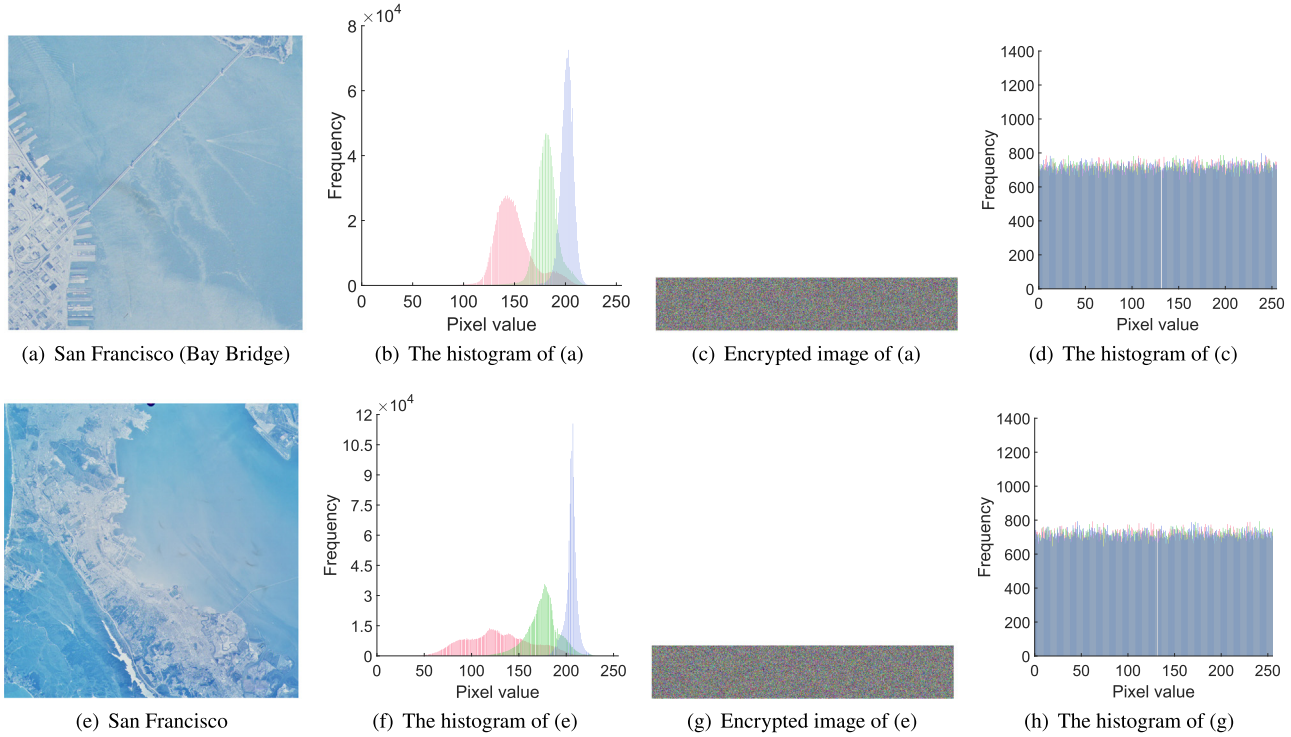
Information entropy can reflect the uncertainty of image information. The greater the uncertainty in the image it is, the greater its information entropy and the better its confidentiality will be, and vice versa (Xiang et al., 2021). The specific mathematical formula used to calculate the information entropy is as follows.

$$H(x) = -\sum_{i=1}^{L} P(x_i) log_2 P(x_i) \tag{16}$$

where L represents the total number of pixels, i represents the grayscale value of the pixel, and $P(x_i)$ represents the probability of pixel x_i. An ideal encryption system should have an encrypted information entropy very close to 8. We compared the information entropy of the plaintext and ciphertext of the three images, and the results, as shown in Table 1, show that the information entropy of the encrypted ciphertext image tends to the ideal value of 8, which indicates that the algorithm has good encryption performance.

4.2.3. Correlation analysis

As ordinary images have the characteristic of strong correlation of adjacent pixels, some attackers will use the analysis of pixel correlation as an entry point for deciphering. Therefore, image encryption algorithms need to interfere with the correlation of pixels as much as possible (Wang et al., 2022a; Wang et al., 2022b). Taking the "Peppers" image before and after encryption as an example, this paper randomly selects 6000 pairs of adjacent pixels from the horizontal, vertical and diagonal directions to analyze and compare their pixel correlation, and the pixel distribution is as shown in Fig. 10.



(a) San Francisco (Bay Bridge) (b) The histogram of (a) (c) Encrypted image of (a) (d) The histogram of (c)

(e) San Francisco (f) The histogram of (e) (g) Encrypted image of (e) (h) The histogram of (g)

Fig. 9. Original plain and encrypted images and their histograms.

Table 1
The entropy of the plain and cipher images.

Algorithm	Images	Plain image	Cipher image
Ours	Female	5.9706	7.9924
	Airplane	6.6639	7.9985
	San Diego	6.3301	7.9997
	San Francisco	6.4133	7.9997
(Wang et al., 2022a; Wang et al., 2022b)	Female	-	7.9726
	Airplane	-	7.9961
(Wen et al., 2023c)	Airplane	-	7.9959

The experimental analysis shows that the encrypted image with very high pixel correlation is completely scattered in the horizontal, vertical and diagonal directions after encryption, and almost does not have pixel correlation. Therefore, the encryption algorithm proposed in this paper has high security.

4.2.4. Analysis of image quality restoration

Peak signal-to-noise ratio (PSNR) and structural similarity (SSIM) are commonly used in image processing as a measure of the quality of reconstructed images. Of these, PSNR is used to assess the quality of the recovered image based on the visibility of errors, defined as

$$PSNR = 10 \times \log_{10}\left(\frac{255^2}{(1/M \times N)\sum_{i=1}^{M}\sum_{j=1}^{N}[P(i,j) - C(i,j)]^2}\right) \tag{17}$$

where M and N represent the length and width of the image, P and C represent the original plain image and the decrypted image, respectively. SSIM is used to evaluate the similarity between two images, and its formula can be represented as

$$SSIM(P,C) = \frac{(2\mu_p\mu_c + (0.01L)^2)(2\sigma_{pc} + (0.03L)^2)}{(\mu_p^2 + \mu_c^2 + (0.01L)^2)(\sigma_p^2 + \sigma_c^2 + (0.03L)^2)} \tag{18}$$

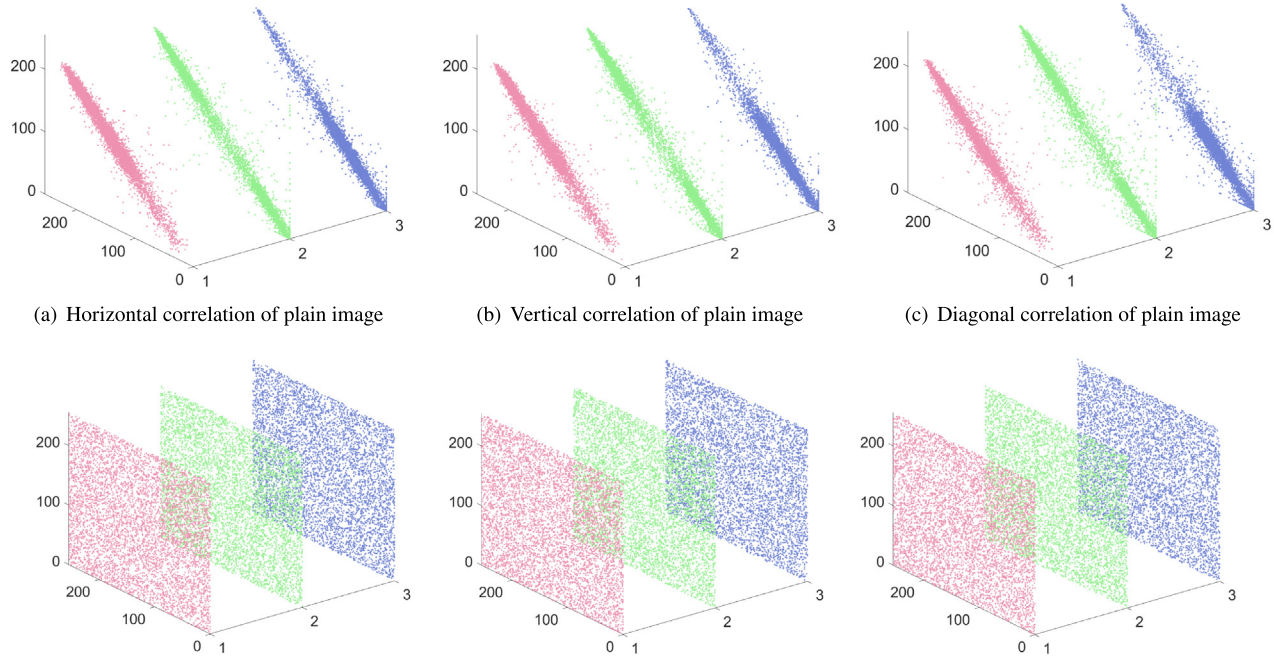
where μ_p and μ_c represent the mean value of the original plain image P and the decrypted image C, respectively, σ_p and σ_c represent the standard deviation of the images P and C, respectively, and L represents the dynamic range of the pixel value. Using the above formula to calculate the values of PSNR and SSIM, it should be noted that the experiment uses a full 1 quantization matrix, and the specific experimental data is demonstrated in Table 2. Generally speaking, the greater the PSNR it is, the better the image quality it will be. For digital images, PSNR value higher than 40 dB indicates that the image quality is good, and 30–40 dB usually indicates that the image distortion can be detected but acceptable.

4.2.5. The influence of quantization matrix on compression ratio and recovery quality

In this encryption algorithm, we can adjust the compression rate by customising the quantization matrix. The specific relationship between the custom quantization matrix and the standard quantization matrix is shown in the equation

$$\begin{cases} Q_1 = \alpha Q_Y \\ Q_2 = \alpha Q_C \end{cases} \tag{19}$$

where Q_1 is the brightness custom quantization matrix, Q_2 is the color difference custom quantization matrix, Q_Y and Q_C are the brightness standard quantization matrix and the color difference standard quantization matrix, respectively. α is the quantization scale factor, and $\alpha = 2, 1, 2^{-1}, 2^{-2}, 2^{-3}, 2^{-4}$. In general, the higher the α increases, the higher the image compression rate will be, but the quality of image recovery will be reduced. As shown in Fig. 11, taking "Couple", "Female", "Mandrill", "Airplane", "Jelly beans1" and "Jelly beans2" as examples, the image restoration quality is evaluated by adjusting the size of α and measuring PSNR. It can be seen that when the quantization matrix changes from $2Q$



(a) Horizontal correlation of plain image (b) Vertical correlation of plain image (c) Diagonal correlation of plain image

(d) Horizontal correlation of encrypted image (e) Vertical correlation of encrypted image (f) Diagonal correlation of encrypted image

Fig. 10. Correlation coefficient distribution of plain image and encrypted images of "Peppers".

Table 2
Quality analysis of image restoration.

Images	PSNR(dB)	SSIM
Female	47.7055	0.9862
Jelly beans1	43.1134	0.9867
Jelly beans2	42.0394	0.9856
Peppers	43.7469	0.9835

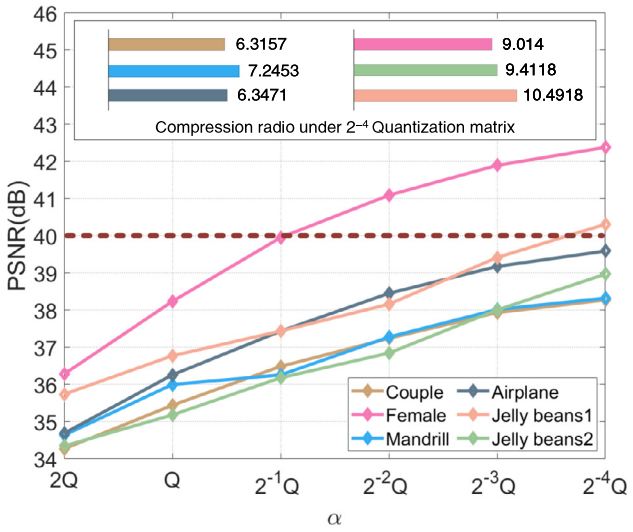


Fig. 11. Reduction quality analysis under different α conditions.

to $2^{-4}Q$ from left to right, the PSNR value also increases continuously, up to nearly 43 dB. It can be found from Fig. 11 that when $\alpha = 2^{-4}$, the PSNR of the restored image is around 40 dB, and the compression ratio is between 6.3 and 10.5. It can be seen that the algorithm also maintains an excellent compression ratio with excellent restoration quality. Therefore using $\alpha = 2^{-4}$ as the default quantization scale factor, the advantage of the high recovery quality of this algorithm is demonstrated by comparing the average PSNR of other compression algorithms in recent years. As shown in the Table 3, the average PSNR value of this algorithm is significantly higher than other algorithms. Fig. 12 shows the encrypted images and restored images when the quantization matrix α is $2^{-4}, 2^{-3}, 2^{-2}, 2^{-1}, 1, 2$, respectively.

4.3. Sensitivity analysis

This section analyzes the performance indicators of the algorithm from two aspects, key and plaintext sensitivity (Farah et al., 2020). For an ideal image encryption scheme, even if the key or plain image information used is slightly different, the result of the encryption will be completely different.

4.3.1. Analysis of sensitivity to the key

Key sensitivity refers to the significant difference, in terms of passwords obtained, between the encryption of the same image using two slightly different keys, as an important aspect of encryption technology (Wang et al., 2020). In this section, the difference between the obtained ciphertexts are compared by using the original *key* and the scrambling $key + 10^{-24}$ to encrypt the plaintext respectively, and the NPCR and UACI are calculated. Among them, NPCR and UACI are defined as follows.

$$\begin{cases} NPCR = \frac{1}{M\times N} \times \sum_{i=1}^{M}\sum_{i=1}^{N} D(i,j) \times 100\% \\ UACI = \frac{1}{M\times N} \times \sum_{i=1}^{M}\sum_{j=1}^{N} \frac{|v_1(i,j)-v_2(i,j)|}{255} \times 100\% \end{cases} \tag{20}$$

where $M \times N$ is the size of processed image, v_1 and v_2 are different cipher images, and $D(i,j)$ is defined as

$$D(i,j) = \begin{cases} 0, v_1(i,j) = v_2(i,j) \\ 1, v_0(i,j) \neq v_2(i,j) \end{cases} \tag{21}$$

where $v_1(i,j)$ represents the pixel value of the previous ciphertext pixel, and $v_2(i,j)$ represents the pixel value of the cipher image after fine-tuning the encryption key. The values of NPCR and UACI were calculated using the above formula, as shown in Table 4. Observing the following charts and data, it can be found that the two cipher images obtained after disturbing the key are very different, and their NPCR and UACI values are very close to the ideal values of 99.61% and 33.46%, which indicates that the encryption scheme is extremely sensitive to the key.

4.3.2. Analysis of plaintext sensitivity

Plaintext sensitivity refers to how much the corresponding ciphertext changes when changing the pixels of the plaintext (Li and Yang, 2022). An algorithm that is insensitive to plaintext presents a vulnerability as an attacker could exploit the difference between a given plaintext and ciphertext to decipher it. Therefore, having sufficient plaintext sensitivity is key to resisting such attacks. This section analyzes the plaintext sensitivity of the algorithm by manipulating the values of just four pixels in the image. The results are reported in Table 5, where the NPCR and UACI values from the original and the new cipher images are presented. The NPCR and UACI values are found to be close to the ideal values, which indicates that the pixel values have changed significantly. This change renders an algorithm safe against the comparison of differences between ciphertexts, and hence, makes the proposed algorithm strong enough to resist plaintext attacks.

4.4. Key space

The key space refers to the range of the size of the encryption key. A large enough key space can effectively resist exhaustive attacks. The algorithm selects two key parameters with an accuracy of 10^{16}, and generates a 128-bit hash value by introducing plaintext association and ciphertext association MD5 to amplify the key space. Therefore, it can be concluded that the key space size of the algorithm is about $10^{16\times 2} \times 2^{128} \approx 2^{234}$, which is much larger than the theoretical requirement of 2^{100}. As shown in Table 6, it is not difficult to see that the algorithm has a better key space than other algorithm.

Table 3
Comparison of the average PSNR of different compression algorithms.

Algorithm	Ours	(Chai et al., 2020)	(Wen et al., 2023c)	(Xiao et al., 2022)	(Wang et al., 2022a; Wang et al., 2022b)
PSNR(dB)	39.6445	34.1119	34.7149	32.0897	27.5537

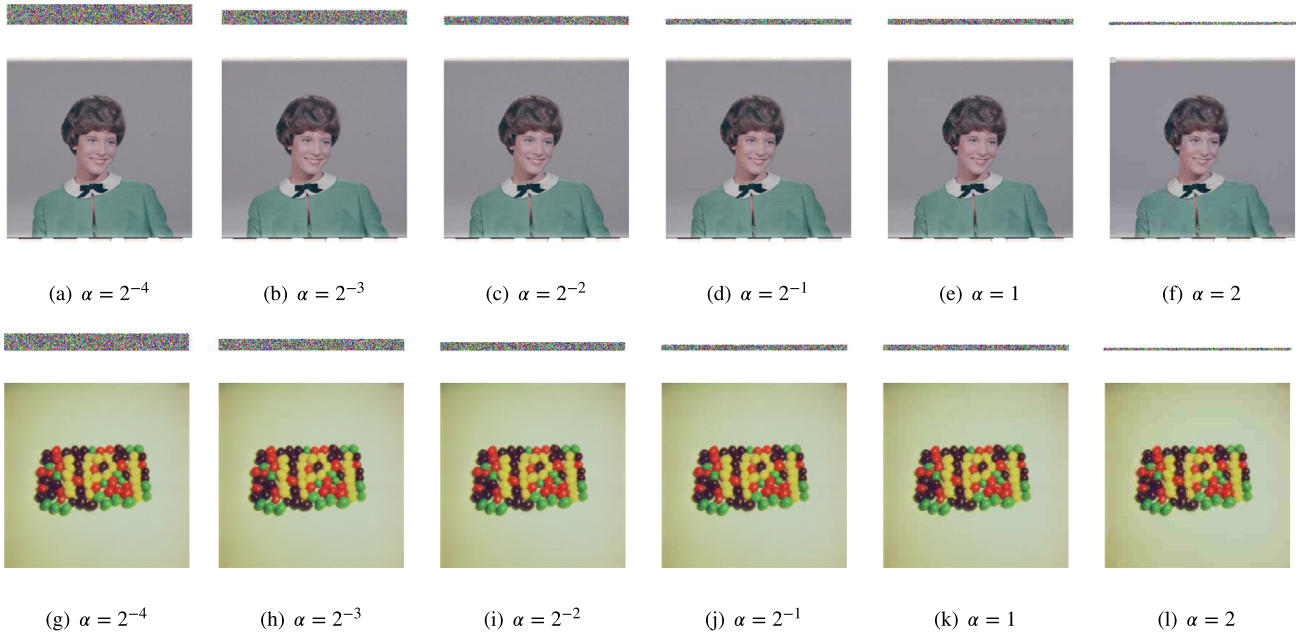


Fig. 12. Encrypted images and restored images under different α conditions.

Table 4
Key sensitivity test.

Images	NPCR(%)	UACI(%)
Couple	99.7266	33.4672
Jelly beans	99.6704	33.4927
Airplane	99.5874	33.5262
San Diego	99.6317	33.3911

Table 5
Plaintext sensitivity test.

Images	NPCR(%)	UACI(%)
$\text{SanDiego}_{(256,256)}$	99.6035	33.3713
$\text{SanDiego}_{(128,256)}$	99.6162	33.4563
$\text{SanDiego}_{(256,128)}$	99.6006	33.4686
$\text{SanDiego}_{(128,128)}$	99.5840	33.4356

4.5. Running efficiency

Operating efficiency is an important indicator to measure whether a compression encryption algorithm is feasible and practical. An algorithm with short running time is naturally more accepted. In the experimental environment shown in Section 3.1, the images with sizes of 512×512 and 256×256 are processed respectively, and the time consumption of the four main steps of hyperchaotic system generation, frequency domain compression, block permutation and row-column diffusion is tested. The results are shown in Table 7. It can be seen that the generation time of hyperchaotic system required to run an image of 512×512 and 256×256 is 0.0020s and 0.0007s respectively, and the next compression step takes 1.0433s and 0.2493s respectively. The subsequent permutation steps take 0.0263s and 0.0072s respectively, and the final diffusion steps take 0.0276s and 0.0075s respectively.

In order to facilitate comparison, we refer to the running efficiency in the literature, as shown in Table 8. In comparison with other algorithms, we can observe that our permutation and diffusion speed are at the leading, which indicates that the algorithm is satisfactory and effective, and has higher advantages in some existing algorithms.

Table 7
Encryption time statistics of each module.

Size	512×512	256×256
Chaos	0.0020s	0.0007s
Compression	1.0433s	0.2493s
Permutation	0.0263s	0.0072s
Diffusion	0.0276s	0.0075s

Table 8
Comparison results with some state-of-the-art algorithms.

Algorithm	Permutation	Diffusion
Ours(512×512)	0.0263s	0.0276s
Ours(256×256)	0.0072s	0.0075s
(Guesmi and Ben Farah, 2021) (512×512)	1.6800s	0.1400s
(Luo et al., 2019) (512×512)	1.1918s	0.2024s
(Zhou et al., 2021) (256×256)	0.0380s	0.0760s
(Wang et al., 2021b) (256×256)	0.1084s	0.0395s

Table 6
Key space comparison.

Algorithm	Ours	(Ye et al., 2020b)	(Chai et al., 2020)	(Guesmi and Ben Farah, 2021)	(Xiao et al., 2022)
Key space	2^{234}	2^{186}	2^{168}	2^{200}	2^{189}

Table 9
NIST-800-22 test results.

Statistical	P-value	Results
Frequency (Monobit) TEST	0.534146	successful
Block-Frenquency Test	0.350485	successful
Cumulative-Sums Test	0.534146	successful
Runs Test	0.066882	successful
Longest-Run Test	0.035174	successful
Binary Matrix Rank Test	0.739918	successful
Discrete Fourier Transform Test	0.213309	successful
Non-Overlapping Templates Test	0.008879	successful
Overlapping Templates Test	0.739918	successful
Maurer's Universal Statistical Test	0.739918	successful
Approximate Entropy Test	0.739918	successful
Serial Test-1	0.911413	successful
Serial Test-2	0.350485	successful
Linear-Complexity Test	0.739918	successful

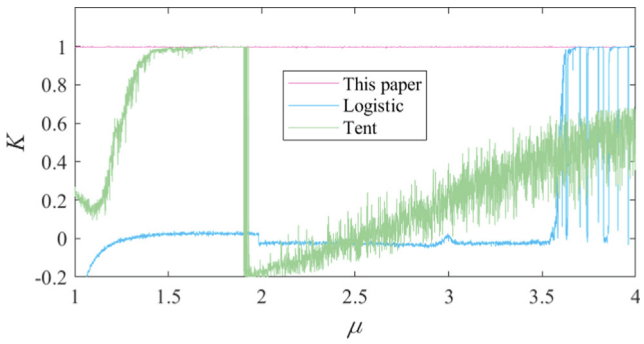


Fig. 13. 0–1 Gottwald Melbourne test.

4.6. Random characteristic test of chaotic sequences

4.6.1. NIST test

The NIST 800-22 test suite is a statistical package consisting of 16 tests that are used to test binary sequences generated by hardware-based password or pseudorandom number generators, where both the values and lengths are random. In this test, the sequence passed the test successfully, and some test results are shown in Table 9.

4.6.2. 0–1 test

The 0–1 Gottwald Melbourne test can distinguish between regular and chaotic motion by computing parameters that asymptotically tend towards 0 and 1 respectively. In the 0–1 Gottwald Melbourne test, the average of 250,000 results shown in Fig. 13 is 0.9978, which is close to the theoretical value of 1, and verifies the excellent performance of the chaotic system.

4.7. Conclusion

In this paper, we innovatively propose a high-quality color image compression and encryption scheme based on chaos and block permutation. In this scheme, the color digital images are first transformed and sampled in the color domain, and then the sub-block parameters are extracted in the DCT frequency domain to achieve compression coding. After that, an image encryption algorithm using chaos-based block permutation and two-round of row-column diffusion is designed for the compressed frequency domain information. The joint compression-encryption greatly reduces the computational complexity of the encrypted objects and improves the efficiency. Both theoretical analysis and simulation results verify that the proposed joint compression-encryption scheme has excellent cryptographic properties. The secret-key space is sufficient to resist brute force attacks with the existing arithmetic power. It has excellent statistical analysis results, including histogram, information entropy, adjacent pixel correlation, and image restoration quality. Meanwhile, it is highly sensitive to keys and plaintexts, and has low computational complexity. Also, the adopted chaotic sequences are both able to pass the NIST and 0–1 sequence tests. Therefore, the feasibility, ease of use and high performance demonstrated by the proposed joint compression-encryption scheme in this paper validate that it is a preferred and promising method for digital image privacy protection. Nevertheless, the algorithm has some shortcomings, such as the complexity of the algorithm structure and running time needs to be optimized, in the future we will explore the solution to enhance the confidential transmission performance.

CRediT authorship contribution statement

Heping Wen: Supervision, Project administration, Writing – original draft, Writing – review & editing. **Yiming Huang:** Conceptualization, Software, Investigation, Methodology, Writing - original draft, Writing - review & editing. **Yiting Lin:** Conceptualization, Methodology, Software, Formal analysis, Writing - original draft, Writing - review & editing.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgement

This work was supported in part by the National Science Foundation of China under Grant 62071088, in part by Guangdong Basic and Applied Basic Research Foundation under Grant 2023A1515011717, and in part by Project for Zhongshan Science and Technology under Grant 2021B2062.

References

Abdulla, A.A., Sellahewa, H., Jassim, S.A., 2014. Stego quality enhancement by message size reduction and fibonacci bit-plane mapping. In: Chen, L., Mitchell, C. (Eds.), Security Standardisation Research. Springer International Publishing, Cham, pp. 151–166.

Abdulla, A.A., Sellahewa, H., Jassim, S.A., 2019. Improving embedding efficiency for digital steganography by exploiting similarities between secret and cover images. Multimedia Tools Appl. 78, 17799–17823. https://doi.org/10.1007/s11042-019-7166-7.

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. https://doi.org/10.1016/j.sigpro.2020.107684.

Chai, X., Wang, Y., Gan, Z., Chen, X., Zhang, Y., 2022a. Preserving privacy while revealing thumbnail for content-based encrypted image retrieval in the cloud. Inf. Sci. 604, 115–141. https://doi.org/10.1016/j.ins.2022.05.008.

Chai, X., Wang, Y., Chen, X., Gan, Z., Zhang, Y., 2022b. TPE-GAN: Thumbnail preserving encryption based on GAN with key. IEEE Signal Process. Lett. 29, 972–976. https://doi.org/10.1109/LSP.2022.3163685.

Chen, G., 2022a. Searching for best network topologies with optimal synchronizability: A brief review. IEEE-CAA J. Automatica Sin. 9, 573–577. https://doi.org/10.1109/JAS.2022.105443.

Chen, G., 2022b. Pinning control of complex dynamical networks. IEEE Trans. Consum. Electron. 68, 336–343. https://doi.org/10.1109/TCE.2022.3200488.

Chen, Y., Zhang, C., Cui, M., Luo, Y., Wu, T., Liang, X., 2022. Joint compressed sensing and JPEG coding based secure compression scheme in OFDM-PON. Opt. Commun. 510, 127901. https://doi.org/10.1016/j.optcom.2022.127901.

Farah, M.B., Guesmi, R., Kachouri, A., Samet, M., 2020. A novel chaos based optical image encryption using fractional fourier transform and DNA sequence operation. Opt. Laser Technol. 121, 105777. https://doi.org/10.1016/j.optlastec.2019.105777.

Feng, Q., Li, P., Lu, Z., Zhou, Z., Wu, Y., Weng, J., Huang, F., 2023. DHAN: Encrypted JPEG image retrieval via DCT histograms-based attention networks. Appl. Soft Comput. 133, 109935. https://doi.org/10.1016/j.asoc.2022.109935.
Gao, X., Mou, J., Banerjee, S., Cao, Y., Xiong, L., Chen, X., 2022a. An effective multiple-image encryption algorithm based on 3D cube and hyperchaotic map. J. King Saud Univ.- Comput. Informat. Sci. 34, 1535–1551. https://doi.org/10.1016/j.jksuci.2022.01.017.
Gao, X., Mou, J., Xiong, L., Sha, Y., Yan, H., Cao, Y., 2022b. A fast and efficient multiple images encryption based on single-channel encryption and chaotic system. Nonlinear Dyn. 108, 613–636. https://doi.org/10.1007/s11071-021-07192-7.
Guesmi, R., Ben Farah, M.A., 2021. A new efficient medical image cipher based on hybrid chaotic map and DNA code. Multimedia Tools Appl. 80, 1925–1944. https://doi.org/10.1007/s00521-020-04808-8.
Karawia, A.A., Elmasry, Y.A., 2021. New encryption algorithm using bit-level permutation and Non-Invertible chaotic map. IEEE Access 9, 101357–101368. https://doi.org/10.1109/ACCESS.2021.3096995.
Li, C., Yang, X., 2022. An image encryption algorithm based on discrete fractional wavelet transform and quantum chaos. Optik 260, 169042. https://doi.org/10.1016/j.ijleo.2022.169042.
Li, L., Yu, S., 2012. A new hyperchaotic system and its adaptive tracking control. Acta Phys. Sin. 61, 22–28. https://doi.org/10.7498/aps.61.040504.
Li, C., Tan, K., Feng, B., Lu, J., 2022. The graph structure of the generalized discrete Arnold's Cat Map. IEEE Trans. Comput. 71, 364–377. https://doi.org/10.1109/TC.2021.3051387.
Luo, Y., Ouyang, X., Liu, J., Cao, L., 2019. An image encryption method based on elliptic curve elgamal encryption and chaotic systems. IEEE Access 7, 38507–38522. https://doi.org/10.1109/ACCESS.2019.2906052.
Luo, Y., Tang, S., Liu, J., Cao, L., Qiu, S., 2020. Image encryption scheme by combining the hyper-chaotic system with quantum coding. Opt. Lasers Eng. 124, 105836. https://doi.org/10.1016/j.optlaseng.2019.105836.
Luo, Y., Zhang, C., Liang, X., Peng, J., Liu, B., Qiu, K., 2022. Secure OFDM-PON using three-dimensional selective probabilistic shaping and chaos. Opt. Express 30, 25339–25355. https://doi.org/10.1364/OE.461196.
Martín, A., Hernández, A., Alazab, M., Jung, J., Camacho, D., 2023. Evolving generative adversarial networks to improve image steganography. Expert Syst. Appl. 222, 119841. https://doi.org/10.1016/j.eswa.2023.119841. URL: https://www.sciencedirect.com/science/article/pii/S0957417423003421.
Niu, Y., Li, X., Zhao, Y., Ni, R., 2019. An enhanced approach for detecting double JPEG compression with the same quantization matrix. Signal Process.-Image Commun. 76, 89–96. https://doi.org/10.1016/j.image.2019.04.016.
Qian, X., Yang, Q., Li, Q., Liu, Q., Wu, Y., Wang, W., 2021. A novel color image encryption algorithm based on three-dimensional chaotic maps and reconstruction techniques. IEEE Access 9, 61334–61345. https://doi.org/10.1109/ACCESS.2021.3073514.
Shahna, K.U., Mohamed, A., 2020. A novel image encryption scheme using both pixel level and bit level permutation with chaotic map. Appl. Soft Comput. 90, 106162. https://doi.org/10.1016/j.asoc.2020.106162.
Singh, R.K., Kumar, B., Shaw, D.K., Khan, D.A., 2021. Level by level image compression-encryption algorithm based on quantum chaos map. J. King Saud Univ.- Comput. Informat. Sci. 33, 844–851. https://doi.org/10.1016/j.jksuci.2018.05.012.
Sisaudia, V., Vishwakarma, V.P., 2022. A secure gray-scale image watermarking technique in fractional DCT domain using Zig-Zag scrambling. J. Informat. Sec. Appl. 69, 103296. https://doi.org/10.1016/j.jisa.2022.103296.
Wang, X., Li, Y., 2021. Chaotic image encryption algorithm based on hybrid multi-objective particle swarm optimization and DNA sequence. Opt. Lasers Eng. 137, 106393. https://doi.org/10.1016/j.optlaseng.2020.106393.
Wang, M., Wang, X., Wang, C., Xia, Z., Zhao, H., Gao, S., Zhou, S., Yao, N., 2020. Spatiotemporal chaos in cross coupled map lattice with dynamic coupling coefficient and its application in bit-level color image encryption. Chaos, Solitons Fractals 139, 110028. https://doi.org/10.1016/j.chaos.2020.110028.
Wang, X., Liu, C., Jiang, D., 2021a. A novel triple-image encryption and hiding algorithm based on chaos, compressive sensing and 3D DCT. Inf. Sci. 574, 505–527. https://doi.org/10.1016/j.ins.2021.06.032.
Wang, X., Yang, J., Guan, N., 2021b. High-sensitivity image encryption algorithm with random cross diffusion based on dynamically random coupled map lattice model. Chaos Solitons Fractals 143, 110582. https://doi.org/10.1016/j.chaos.2020.110582.
Wang, X., Su, Y., Xu, M., Zhang, H., Zhang, Y., 2022a. A new image encryption algorithm based on latin square matrix. Nonlinear Dyn. 107, 1277–1293. https://doi.org/10.1007/s11071-021-07017-7.
Wang, J., Zhang, M., Tong, X., Wang, Z., 2022b. A chaos-based image compression and encryption scheme using fractal coding and adaptive-thresholding sparsification. Phys. Scripta 97, 105201. https://doi.org/10.1088/1402-4896/ac8b41.
Wang, Y., Zhao, Q., Zhang, H., LI, T., Xu, W., Liu, S., Su, Y., 2023. Optical single-channel color image encryption based on chaotic fingerprint phase mask and diffractive imaging. Appl. Opt. 62, 1009–1018. https://doi.org/10.1364/AO.479983.
Wei, D., Jiang, M., Deng, Y., 2023. A secure image encryption algorithm based on hyper-chaotic and bit-level permutation. Expert Syst. Appl. 213, 119074. https://doi.org/10.1016/j.eswa.2022.119074.
Wen, H., Lin, Y., 2023. Cryptanalyzing an image cipher using multiple chaos and DNA operations. J. King Saud Univ. - Comput. Informat. Sci., 101612 https://doi.org/10.1016/j.jksuci.2023.101612.
Wen, H., Liu, Z., Lai, H., Zhang, C., Liu, L., Yang, J., Lin, Y., Li, Y., Liao, Y., Ma, L., Chen, Z., Li, R., 2022a. Secure DNA-Coding image optical communication using Non-Degenerate hyperchaos and dynamic secret-key. Mathematics 10, 3180. https://doi.org/10.3390/math10173180.
Wen, H., Chen, Z., Zheng, J., Huang, Y., Li, S., Ma, L., Lin, Y., Liu, Z., Li, R., Liu, L., Lin, W., Yang, J., Zhang, C., Yang, H., 2022b. Design and embedded implementation of secure image encryption scheme using DWT and 2D-LASM. Entropy 24, 1332. https://doi.org/10.3390/e24101332.
Wen, H., Wu, J., Ma, L., Liu, Z., Lin, Y., Zhou, L., Jian, H., Lin, W., Liu, L., Zheng, T., Zhang, C., 2023a. Secure optical image communication using double random transformation and memristive chaos. IEEE Photonics J. 15, 1–11. https://doi.org/10.1109/JPHOT.2022.3233129.
Wen, H., Chen, R., Yang, J., Zheng, T., Wu, J., Lin, W., Jian, H., Lin, Y., Ma, L., Liu, Z., Zhang, C., 2023b. Security analysis of a color image encryption based on bit-level and chaotic map. Multimedia Tools Appl. https://doi.org/10.1007/s11042-023-14921-0.
Wen, H., Kang, S., Wu, Z., Lin, Y., Huang, Y., 2023c. Dynamic rna coding color image cipher based on chain feedback structure. Mathematics 11, 3133. https://doi.org/10.3390/math11143133. URL: https://www.mdpi.com/2227-7390/11/14/3133.
Xian, Y., Wang, X., Wang, X., Li, Q., Yan, X., 2022. Spiral-Transform-Based fractal sorting matrix for chaotic image encryption. IEEE Trans. Circ. Syst. I-Regular Pap. 69, 3320–3327. https://doi.org/10.1109/TCSI.2022.3172116.
Xiang, Y., Xiao, D., Zhang, R., Liang, J., Liu, R., 2021. Cryptanalysis and improvement of a reversible data-hiding scheme in encrypted images by redundant space transfer. Inf. Sci. 545, 188–206. https://doi.org/10.1016/j.ins.2020.08.019.
Xiao, M., Tan, R., Ye, H., Gong, L., Zhu, Z., 2022. Double-color-image compression-encryption algorithm based on quaternion multiple parameter DFrAT and feature fusion with preferable restoration quality. Entropy 24. https://doi.org/10.3390/e24070941.
Ye, H., Zhou, N., Gong, L., 2020a. Multi-image compression-encryption scheme based on quaternion discrete fractional hartley transform and improved pixel adaptive diffusion. Signal Process. 175, 107652. https://doi.org/10.1016/j.sigpro.2020.107652.
Ye, G., Pan, C., Dong, Y., Shi, Y., Huang, X., 2020b. Image encryption and hiding algorithm based on compressive sensing and random numbers insertion. Signal Process. 172, 107563. https://doi.org/10.1016/j.sigpro.2020.107563.
Yuen, C., Wong, K., 2011. A chaos-based joint image compression and encryption scheme using DCT and SHA-1. Appl. Soft Comput. 11, 5092–5098. https://doi.org/10.1016/j.asoc.2011.05.050.
Yu, F., Gong, X., Li, H., Wang, S., 2021. Differential cryptanalysis of image cipher using block-based scrambling and image filtering. Inf. Sci. 554, 145–156. https://doi.org/10.1016/j.ins.2020.12.037.
Zhang, Y., Wang, P., Fang, L., He, X., Han, H., Chen, B., 2020. Secure transmission of compressed sampling data using edge clouds. IEEE Trans. Industr. Inf. 16, 6641–6651. https://doi.org/10.1109/TII.2020.2966511.
Zhang, Y., Zhou, J., Xiang, Y., Zhang, L.Y., Chen, F., Pang, S., Liao, X., 2021. Computation outsourcing meets lossy channel: Secure sparse robustness decoding service in multi-clouds. IEEE Trans. Big Data 7, 717–728. https://doi.org/10.1109/TBDATA.2017.2711040.
Zhang, Y., Zhou, W., Zhao, R., Zhang, X., Cao, X., 2022. F-TPE: Flexible thumbnail-preserving encryption based on multi-pixel sum-preserving encryption. IEEE Trans. Multimedia 14, 1–15. https://doi.org/10.1109/TMM.2022.3200310.
Zhang, Y., Chen, N., Qi, S., Xue, M., Hua, Z., 2023a. Detection of recolored image by texture features in chrominance components. ACM Trans. Multimedia Comput. Commun. Appl. 19, 1–23. https://doi.org/10.1145/3571076.
Zhang, L., Tang, C., Shen, Y., Han, R., 2023b. Optical double-image cryptosystem based on generalized singular value decomposition and five-dimensional hyperchaotic maps. Appl. Opt. 62, 665–674. https://doi.org/10.1364/AO.476236.
Zhou, Y., Bao, L., Chen, C., 2014. A new 1D chaotic system for image encryption. Signal Process. 97, 172–182. https://doi.org/10.1016/j.sigpro.2013.10.034.
Zhou, Y., Peng, J., Chen, C., 2015. Dimension reduction using spatial and spectral regularized local discriminant embedding for hyperspectral image classification. IEEE Trans. Geosci. Remote Sens. 53, 1082–1095. https://doi.org/10.1109/TGRS.2014.2333539.
Zhou, Y., Li, C., Li, W., Li, H., Feng, W., Qian, K., 2021. Image encryption algorithm with circle index table scrambling and partition diffusion. Nonlinear Dyn. 103, 2043–2061. https://doi.org/10.1007/s11071-021-06206-8.
Zhu, H., Zhao, Y., Song, Y., 2019. 2D Logistic-Modulated-Sine-Coupling-Logistic chaotic map for image encryption. IEEE Access 7, 14081–14098. https://doi.org/10.1109/ACCESS.2019.2893538.

Heping Wen is an associate professor of University of Electronic Science and Technology of China, Zhongshan Institute. He received his Ph.D. from Guangdong University of Technology in 2019. His main research interests are chaotic secure communication, image encryption and information concealment, optical access network security, and industrial data security. He has published more than 20 high-level papers in core journals at home and abroad, and served as a professional reviewer for many international journals.

Yiming Huang is a student at the School of Electronic Information, University of Electronic Science and Technology of China, Zhongshan Institute. His main research interests are image encryption, information processing and optical access network security. He has published 3 SCI papers.

Yiting Lin is a student at the School of Computing, University of Electronic Science and Technology of China, Zhongshan Institute. His main research interests are Computer Science, Cryptography, Nonlinear dynamics, Information Security, Signal Processing. He has published 7 SCI papers.