scientific reports

OPEN

High-quality restoration image encryption using DCT frequency-domain compression coding and chaos

Heping Wen[1,2,3]✉, Linchao Ma[1], Linhao Liu[1], Yiming Huang[1], Zefeng Chen[1], Rui Li[1], Zhen Liu[1], Wenxing Lin[1], Jiahao Wu[1], Yunqi Li[1] & Chongfu Zhang[2]✉

With the arrival of the age of big data, the amount and types of data in the process of information transmission have increased significantly, and the full-disk encryption mode used by traditional encryption algorithms has certain limitations of the times. In order to further improve the bandwidth efficiency of digital images in the transmission process and the information effectiveness of digital image transmission, this paper proposes an algorithm of high-quality restoration image encryption using DCT frequency-domain compression coding and chaos. Firstly, the image hash value is used for the generation of an encryption key with plaintext correlation, then lightweight chaos is generated based on the key to obtain a pseudo-random sequence. Secondly, the image is partitioned into subblock, and converted from time domain into frequency domain by employing Discrete Cosine Transform (DCT) on each block, then perform quantization operation based on frequency domain information to obtain DCT coefficient matrix. Thirdly, the direct current (DC) coefficients and alternating current (AC) coefficients are extracted in the DCT coefficient matrix and compressed by different encoding methods to obtain two sets of bitstream containing DC coefficient and AC coefficient information. Fourthly, permute the DC coefficient bit stream by the chaotic sequence, and reconstruct it with the AC coefficient bit stream to obtain the frequency domain ciphertext image. Finally, the chaotic sequence is used to diffuse ciphertext, and the processed hash value is hidden in the ciphertext to obtain the final ciphertext. The theoretical and experimental analysis showed that the key length reaches 341 bits, and the PSNR value of the restored image is close to 60, all of which satisfy the theoretical value. Therefore, the algorithm has the characteristics of high compression rate, high-quality image restoration large key space, strong plaintext sensitivity, strong key sensitivity and so on. Our method proposed in this paper is expected to provide a new idea for confidential and secure communication in the age of big data.

With the continuous development of information technology, the age of big data has arrived[1–6]. While people are enjoying the information dividends, potential information security problems are also gradually exposed. As one of the important media of information transmission in the era of big data, digital image has attracted widespread attention for its security during transmission[7,8], so it is important to conduct encryption transmission for digital image. However, compared with text information, digital image information has the characteristics of high information redundancy, strong pixel correlation and discrete distribution of key information, etc[9–11]. Most text information security enhancement methods are not appropriate for digital image. Therefore, it is very necessary to study the digital image encryption algorithm. In addition, the amount and type of data are growing rapidly in the age of big data, and the information effectiveness and system throughput in the process of information transmission should also be of concern[12–16]. Therefore, the research on image encryption algorithm under the background of big data era has certain theoretical value and practical significance[17,18].

[1]Zhongshan Institute, School of electronic information, University of Electronic Science and Technology of China, Zhongshan 528402, China. [2]School of Information and Communication Engineering, University of Electronic Science and Technology of China, Chengdu 611731, China. [3]Guangdong Provincial Key Laboratory of Information Security Technology, Sun Yat-sen University, Guangzhou 510006, China. ✉email: wenheping@uestc.edu.cn; cfzhang@uestc.edu.cn

Throughout the international research status, digital image encryption has become a hot research topic[19–22]. In recent years, many scholars have devoted themselves to research in this field and achieved good results. In 2018, Ref.[23] introduce a novel chaos-based image encryption algorithm for color images based on three-dimensional bit-plane permutation. Simulation results and security analyses demonstrate that the algorithm not only has a good encryption effect but can also resist common attacks. In 2019, Ref.[24] proposed a new algorithm of chaos optical image encryption based on fractional Fourier transform and DNA sequence operation. The experimental results and security analysis show that the algorithm has a good encryption effect and can resist most known attacks. In 2020, Ref.[25] proposed a new type of time-delay chaotic system, which has different dynamical behavior over time delay. Then based on the system design a novel approach to achieve image encryption. Final experiments illuminate that the given image encryption method has good effectiveness and higher security. In 2021, Ref.[26] by studying the difference between chaotic sequences and wavelet transform values, proposed a novel technique for digital image encryption and improved previous algorithms. Comparing various performance indexes, it shows that this technique is a suitable choice for actual image encryption. The research results of digital image encryption are far more than these, and a growing number of encryption algorithms are being proposed. From these achievements, we can see that the majority of encryption algorithms have achieved satisfactory results in some aspects, which also greatly promoted the development of information security technology. Unfortunately, in the era of big data, most of the research results have era limitations.

In order to solve the security problem of digital image transmission in the era of big data, some scholars have made continuous contributions to image encryption and compression. For example, Ref.[27–30] use a variety of different technologies to achieve. The experimental results show that the scheme has more advantages compared to the technology at that time. There are also some scholars who have made pioneering attempts in this direction. For example, in 2020, Ref.[31] proposed a new multi-image encryption scheme based on quaternion discrete fractional Hartley transform (QDFrHT) and pixel adaptive diffusion. The original images are compressed into four fusion images by Discrete Cosine Transform (DCT) and Zig-Zag operations and then the resulting four images are represented as quaternion algebra. Afterwards, the quaternion signal is processed with the proposed QDFrHT and the double random phase encoding technique. The experimental results show that the scheme is feasible and safe. Unfortunately, most of these studies have the following problems: (1) The use of comprehensive encryption, iterative encryption, multi round encryption and other methods can effectively improve the encryption quality, but there are some problems such as low encryption efficiency and high information redundancy, which have limitations under the background of big data era. (2) The quality of image restoration is often an important indicator to measure the encryption performance, and most of the research focuse on the comparison of plaintext and ciphertext, and lacks the systematic analysis of restored images.

To solve the above problems, this paper proposes an algorithm of high-quality restoration image encryption using DCT frequency-domain compression coding and chaos. Firstly, the encryption key with plaintext correlation is generated by using the image hash value, and the lightweight chaos is generated based on the key to obtain the chaotic pseudo-random sequence. Secondly, divide the image into sub-blocks, and perform DCT on all sub-blocks separately, the image is mapped from time domain to frequency domain, and the quantization operation is carried out based on frequency domain information to obtain DCT coefficient matrix. Then, the direct current(DC) coefficients and alternating current(AC) coefficients in the DCT coefficient matrix are extracted and compressed by different coding methods to obtain two groups of bit streams containing DC coefficients and AC coefficients. Then, the chaotic sequence is used to scramble the DC coefficient bit stream, and the data is reconstructed with the AC coefficient bit stream to obtain the frequency domain ciphertext image. Finally, the ciphertext is diffused using the chaotic sequence, and the processed hash value is hidden in the ciphertext to obtain the final ciphertext. Theoretical and experimental analysis shows that the algorithm has the characteristics of high compression rate, high-quality image restoration large key space, strong plaintext sensitivity, and strong key sensitivity, etc. Therefore, the method proposed in this paper can better improve the effectiveness and reliability of information in the transmission process, and is expected to provide a new idea for secure communication in the context of big data era.

In this paper, we use DCT coding, which requires less arithmetic power, and modify and improve the algorithm with reference to JPEG compression, which has improved the performance compared with traditional JPEG compression. In terms of information encryption, we choose the lightweight chaos with high generation efficiency and low arithmetic power consumption, and introduce the dynamic key associated with plaintext to realize the dynamic encryption process of "one encryption at a time". In addition, the algorithm is designed based on frequency domain, which can realize selective encryption of information and effectively improve efficiency.

Correlation theory

DCT.

DCT is a kind of orthogonal transformation[32]. Compared with fast Fourier transform (FFT) and Discrete wavelet transform (DWT), DCT can save arithmetic power and maintain good performance[7]. Let $\{X_m|m = 0, 1, \ldots, N-1\}$ be a signal sequence with length N, and 1D discrete chord transform (1D-DCT) is defined as:

$$Y(u) = C(u)\sqrt{\frac{2}{N}}\sum_{m=0}^{N-1} X(m)\cos\frac{(2m+1)u\pi}{2N}, u = 1, 2, \ldots, N-1 \tag{1}$$

where

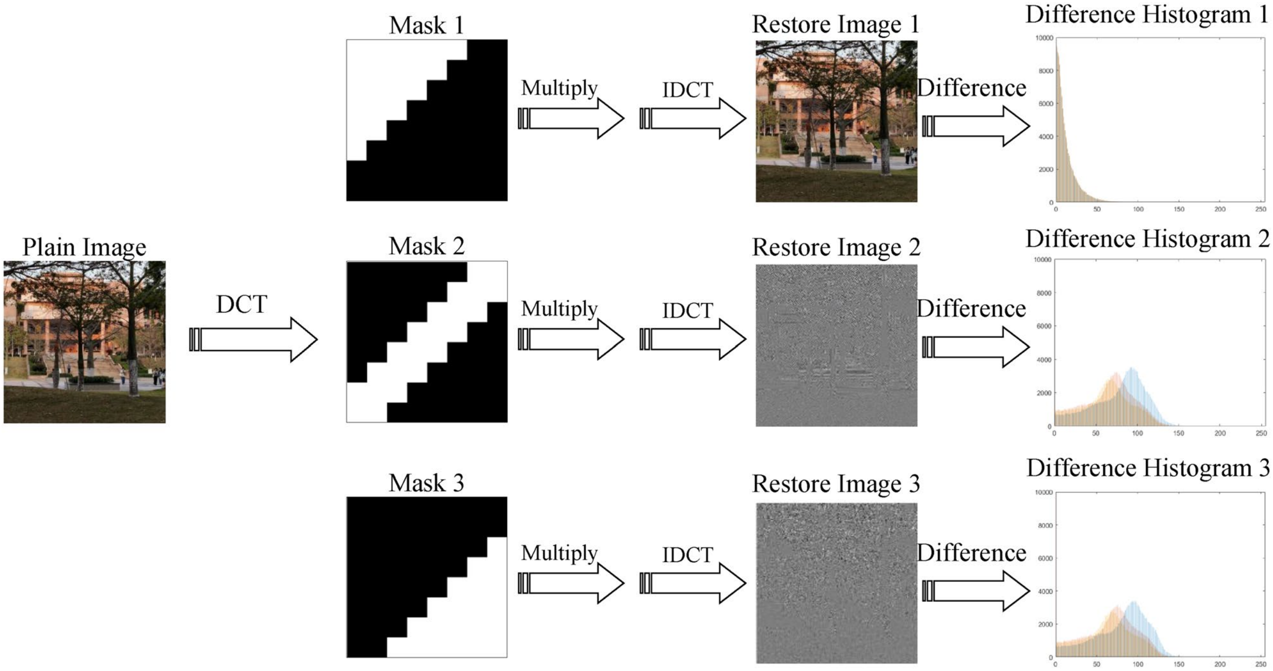


Figure 1. Differential comparison of DCT restoration results under different masks.

$$C(u) = \begin{cases} \frac{1}{\sqrt{2}}, u = 0 \\ 1, u \neq 0 \end{cases} \tag{2}$$

1D inverse discrete chord transform (1D-IDCT) is defined as:

$$X(m) = \sqrt{\frac{2}{N}} \sum_{v=0}^{N-1} C(u)Y(u)\cos\frac{(2m+1)u\pi}{2N} \tag{3}$$

Extending 1D-DCT to 2D discrete chord transform (2D-DCT)[33,34]. Let $\{X(m,n)|m = 0,1,\ldots,M-1;\, n = 0,1,\ldots,N-1\}$ be two-dimensional signal sequence of $M \times N$, 2D-DCT is defined as:

$$Y(u,v) = \frac{2}{\sqrt{M \times N}} C(u)C(v) \sum_{m=0}^{M-1}\sum_{n=0}^{N-1} X(m,n)\cos\frac{(2m+1)u\pi}{2M}\cos\frac{(2n+1)v\pi}{2N} \tag{4}$$

where $u = 1,2,\ldots,M-1$; $v = 1,2,\ldots,N-1$, and

$$C(u) = \begin{cases} \frac{1}{\sqrt{2}}, u = 0 \\ 1, u \neq 0 \end{cases} \tag{5}$$

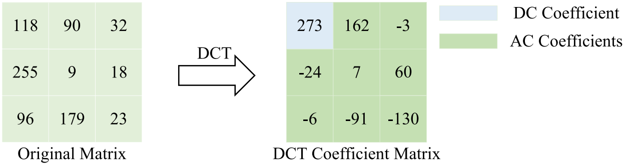
$$C(v) = \begin{cases} \frac{1}{\sqrt{2}}, v = 0 \\ 1, v \neq 0 \end{cases} \tag{6}$$

2D-IDCT is defined as:

$$X(m,n) = \frac{2}{\sqrt{M \times N}} \sum_{u=0}^{M-1}\sum_{v=0}^{N-1} C(u)C(v)Y(u,v)\cos\frac{(2m+1)u\pi}{2M}\cos\frac{(2n+1)v\pi}{2N} \tag{7}$$

Compare with Fourier Transform, DCT in real domain, so digital image processing based on DCT will be more intuitive[35]. In addition, DCT has entropy retention, energy retention, decorrelation, and energy concentration, among which energy concentration is of great significance to digital image encryption[36]. As shown in Fig. 1, the effective information mask with same area and different shape is used to multiply the 2D-DCT image, and the difference analysis is carried out on the image after 2D-DCT. The information retained by the three effective information masks is as follows: the upper left region information, the middle band region information, and the lower right region information. It can be seen from the results of the differential analysis that only Mask 1 can better restore image information, which shows that the energy of the image after DCT is mainly concentrated in the upper left region.

Further analyze the energy concentration of DCT. DCT is performed on the selected matrix. The data before and after transformation are shown in Fig. 2. The matrix on the right in the figure is the result of rounding after



118	90	32
255	9	18
96	179	23

Original Matrix

273	162	-3
-24	7	60
-6	-91	-130

DCT Coefficient Matrix

Figure 2. Data comparison before and after DCT.

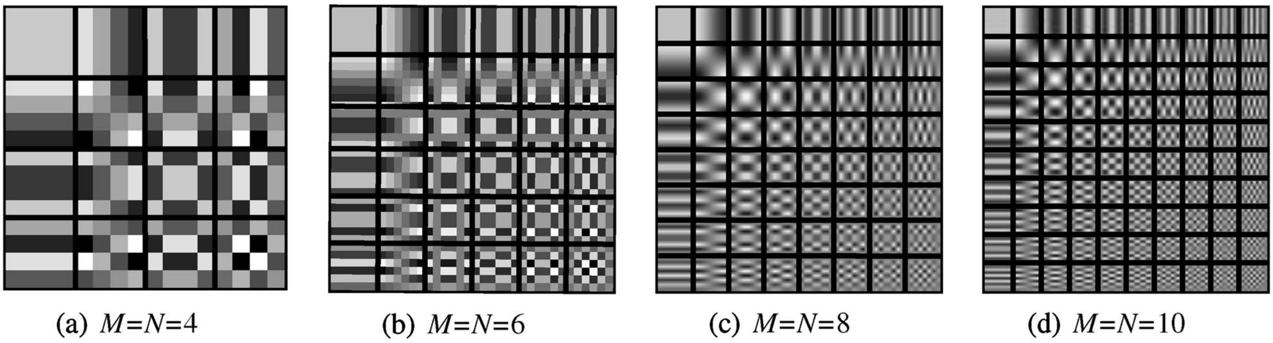


Figure 3. DCT base images.

transformation. For the matrix after DCT, it is usually called DCT Coefficient Matrix, and an element in the upper left corner is called DC coefficient, and its remaining elements are AC coefficients. For the DCT coefficient matrix in Fig. 2, the number 273 is the DC coefficient of the coefficient matrix, and it can be seen that the energy of the image after DCT is mainly concentrated in the DC coefficient[2,36]. Based on this, in the digital image encryption, focus on encrypting the DC coefficients in the frequency domain image after DCT, and the ideal encryption effect can be obtained.

In addition, when using DCT to encode the image, the mode of dividing the image into blocks and encoding the sub-blocks and then splicing the sub-blocks is usually adopted. The sub-block size has many choices, and the optimal solution of block size can be obtained from the base image of DCT. For ease of expression, rewrite Eq. (7) as:[37]

$$X(m,n) = \sum_{u=0}^{M-1}\sum_{v=0}^{N-1} Y(u,v)q(m,n,u,v) \tag{8}$$

where $m = 0, 1, \ldots, M-1$; $n = 0, 1, \ldots, N-1$. It can be seen from the above formula that $X(m, n)$ is composed of $M \times N$ frequency components, and any frequency component has a specific (u, v) corresponding to. For each specific (u, v) value, exhaustive (m, n) all cases, we will get a matrix, which is the base image of DCT, its mathematical expression is as follows:

$$X(m,n) = \begin{bmatrix} q(0,0,u,v) & q(0,1,u,v) & \cdots & q(0,N-1,u,v) \\ q(1,0,u,v) & q(1,1,u,v) & \cdots & q(1,N-1,u,v) \\ \vdots & \vdots & \vdots & \vdots \\ q(M-1,0,u,v) & q(M-1,1,u,v) & \cdots & q(M-1,N-1,u,v) \end{bmatrix} \tag{9}$$

The base images corresponding to different (u, v) values have $M \times N$ amplitudes, and they are independent of $X(m, n)$. DCT base images with different M and N values are shown in Fig. 3. The base image can reflect main features of the transformation, as can be seen when $M = N \geq 8$, the performance of DCT base image meets the expectations[38]. Therefore, the 8 × 8 block mode can reduce the computational complexity of DCT to the greatest extent under the condition of ensuring accuracy, which is the optimal solution for block size selection[39].

Chaotic system. The chaotic system was first proposed by American meteorologist Lorenz in 1963[40], which is a nonlinear system with non-divergence, non-convergence, and non-periodic characteristics. Due to the complex dynamic principle of chaotic system, the sequences generated by the system usually have strong randomness. At the same time, because the chaotic system is highly sensitive to the initial value, the sequence is usually difficult to predict, so the chaotic system is widely used in secure communication.

Lorenz chaotic system, as the first continuous chaotic system, has the advantages of simple form and high generation efficiency. However, the cryptosystem using Lorenz chaotic sequence as the key usually has the problems of small key space and poor anti-attack ability. Therefore, a general framework of 1-D chaotic maps called the Dynamic Parameter-Control Chaotic System(DPCCS) was proposed by Ref.[41]. DPCCS is able to produce a huge number of new chaotic maps. Evaluations and comparisons show that chaotic maps generated by DPCCS

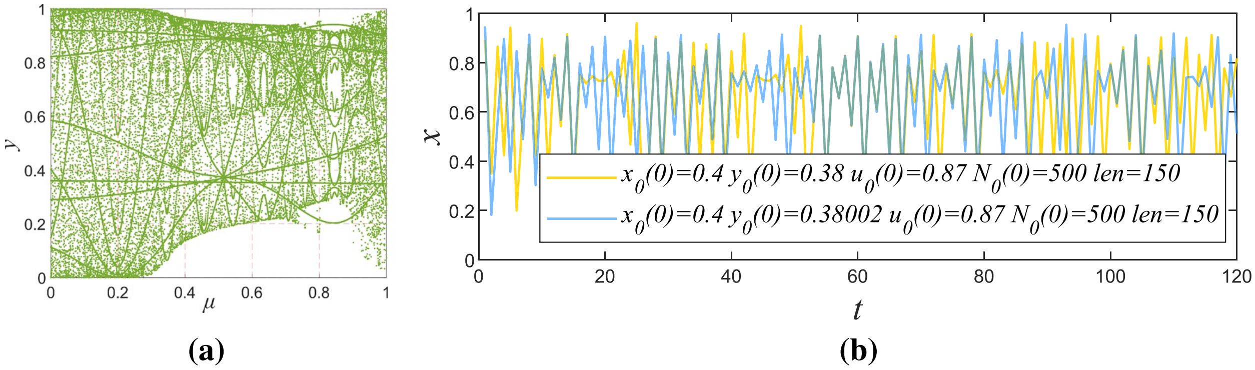


Figure 4. (**a**) Bifurcation diagrams of the SCL maps; (**b**) Sequence comparison before and after $y_0(0)$ perturbation.

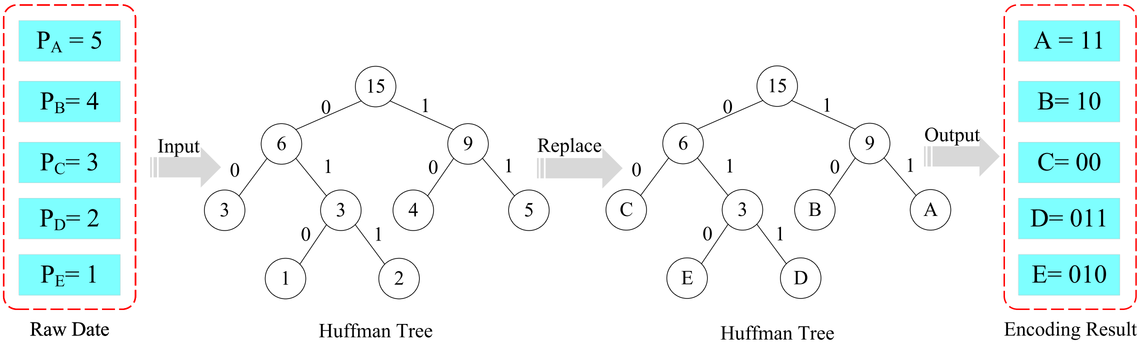


Figure 5. Huffman coding process.

are very sensitive to their initial states, and have wider chaotic ranges, better unpredictability and more complex chaotic behaviors than their seed maps.

This paper uses a sine map to control the parameter of the logistics chaotic map, the chaotic system is simply called Sine-control-Logistic(SCL). Since SCL chaos is a lightweight discrete chaotic system, it does not require sampling and other operations in use, which is more convenient than the continuous chaotic system. SCL chaotic system is defined as:

$$x_{n+1} = 4(1 - 0.1y_{n+1})x_n(1 - x_n) \tag{10}$$

where

$$y_{n+1} = \mu \sin(\pi y_n) \tag{11}$$

where n and $n+1$ are used as cell markers, x_n and y_n are system initial values, μ is the control values of y_{n+1}, y_{n+1} is the control values of x_{n+1}, x_{n+1} is the sequence generated by chaos. When $u \in (0.87, 1)$, $x_n \in (0.35, 0.45)$, $y_n \in (0.35, 0.45)$ the system is in a chaotic state. Figure 4 is the SCL maps and the initial value sensitivity of SCL system.

Compressed encoding. Digital image usually has the characteristics of a large amount of data and high information redundancy, which leads to low spectral efficiency and limited information validity in the transmission process. Therefore, it is necessary to find a method to remove image information redundancy and improve the effectiveness of transmission information. In this paper, compression coding is used to achieve this goal. There are three coding methods, namely:

Huffman Coding: Huffman Coding is a lossless compression coding[42]. The encoding steps can be summarized as follows: Firstly, the probability of image pixel values is arranged in descending order. Secondly, the pixel values are added sequentially in order until the final sum of probabilities is 1. Finally, the path of each pixel value is drawn from the probability of 1, and 0 and 1 are recorded in the order of paths. The final binary code is the Huffman code of pixels. Set A, B, C, D, E five characters, the frequency of occurrence is 5, 4, 3, 2, 1 respectively. Then the coding results are shown in Fig. 5, where P represents the frequency of the characters.

Run-Length Encoding (RLE): RLE is a lossless coding method and is commonly used in digital image compression[43]. The encoding principle is that the adjacent pixels with the same pixel value in a row are represented by two bytes. As shown in Fig. 6, the first byte records the number of repetitions of pixels, and the second byte records the specific pixel value. The effect of RLE mainly depends on the characteristics of the image itself: the larger the pixel block of the same pixel in the image, the better the compression effect and the higher the compression ratio. On the contrary, the compression effect is poor.

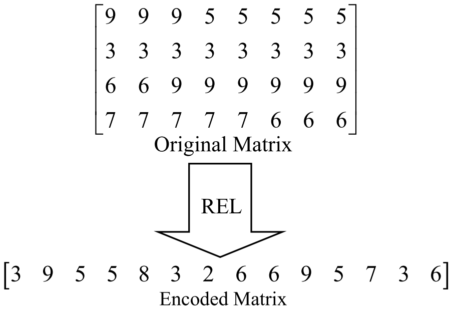


Figure 6. RLE process.

Differential Pulse Code Modulation (DPCM): DPCM is a kind of linear predictive coding and a lossy compression coding[44]. The main principle is: using the past sampling values to predict the current sampling values, and coding their difference. For image signals, the instantaneous slope of the signal is so large that it is easy to cause overload, simple increment modulation cannot be used for coding. Therefore, a modulation method that combines the characteristics of incremental modulation and pulse code modulation is usually used for coding, which is called DPCM. Assuming that the discrete-time analog signal is set X_k, the signal value at time K is X_k, and the linear combination of the past N signals is used to predict, then the predicted value $\hat{X_k}$ is:

$$\{\hat{X_k}\} = \sum_{i=1}^{N} a_i X_{K-1} \tag{12}$$

There is an information difference e_k between the actual value X_k and the predicted value $\hat{X_k}$, that is:

$$e_k = X_k - \hat{X_k} = X_k - \sum_{i=1}^{N} a_i \hat{X_{K-1}} \tag{13}$$

If appropriate N and a_i are selected to make the characteristic of e_k a white noise process with an average value of 0 and recorded as W_K, then the restored X_K is:

$$X_K = \sum_{i=1}^{N} a_i \hat{X_{K-1}} + W_K \tag{14}$$

The proposed encryption algorithm

The current chaotic encryption algorithms mostly use the static key encryption mode for complete images. Such methods usually have problems such as poor security performance and low effectiveness of information transmission, and have limitations under the background of big data era. Therefore, this paper proposes a frequency domain compression encryption algorithm based on lightweight chaos, and introduces a dynamic key with plaintext correlation. The specific process of encryption and decryption is shown in Fig. 7. This algorithm uses the dynamic key to realize the dynamic encryption mode of "one image and one encryption", and the dynamic key is hidden during the transmission process. The specific encryption steps are as follows:

Step1: Dynamic Key Generation and Chaotic Sequence Generation

Read in the plaintext and use the hash table to obtain the MD5 hash value of the plaintext image, and encode the 16-bit hash value into 4 decimal numbers that conform to the initial chaotic value interval. The specific encoding rules are as follows:

$$\begin{cases} x_1(0) = 0.35 + (m_1 \oplus m_2 \oplus m_3 \oplus m_4)/2560 \\ y_1(0) = 0.35 + (m_5 \oplus m_6 \oplus m_7 \oplus m_8)/2560 \\ x_2(0) = 0.35 + (m_9 \oplus m_{10} \oplus m_{11} \oplus m_{12})/2560 \\ y_2(0) = 0.35 + (m_{13} \oplus m_{14} \oplus m_{15} \oplus m_{16})/2560 \end{cases} \tag{15}$$

where $\oplus$ is bitwise XOR operation, m_{1-16} is the result of bitwise read for MD5 hash, $x_1(0), y_1(0), x_2(0), y_2(0)$ is the initial value of chaotic system. Generating a chaotic system by using the initial chaotic value can receive two chaotic sequences: K_1, K_2 for encryption. In addition, in order to ensure the security of the hash value, a bit-level cyclic shift is performed on the hash value, and the result after cyclic shift is re-encoded into decimal number every 8 bits. The specific formula is as follows:

$$\begin{cases} hash2 = \mathrm{circshift}(hash, [0, -7]) \\ m = \mathrm{blkproc}(hash2, [1, 8], '\mathrm{two2ten}') \end{cases} \tag{16}$$

where circshift($\cdot$) is the function for circular shift, blkproc($\cdot$) is the function for segmentation, *hash* is binary hash value and its length is 128bit, matrix [0, − 7] indicates that the cyclic shift operation is unchanged for row elements, rotate column elements 7 units to the left, *hash*2 is the circularly shifted binary hash value, 'two2ten'

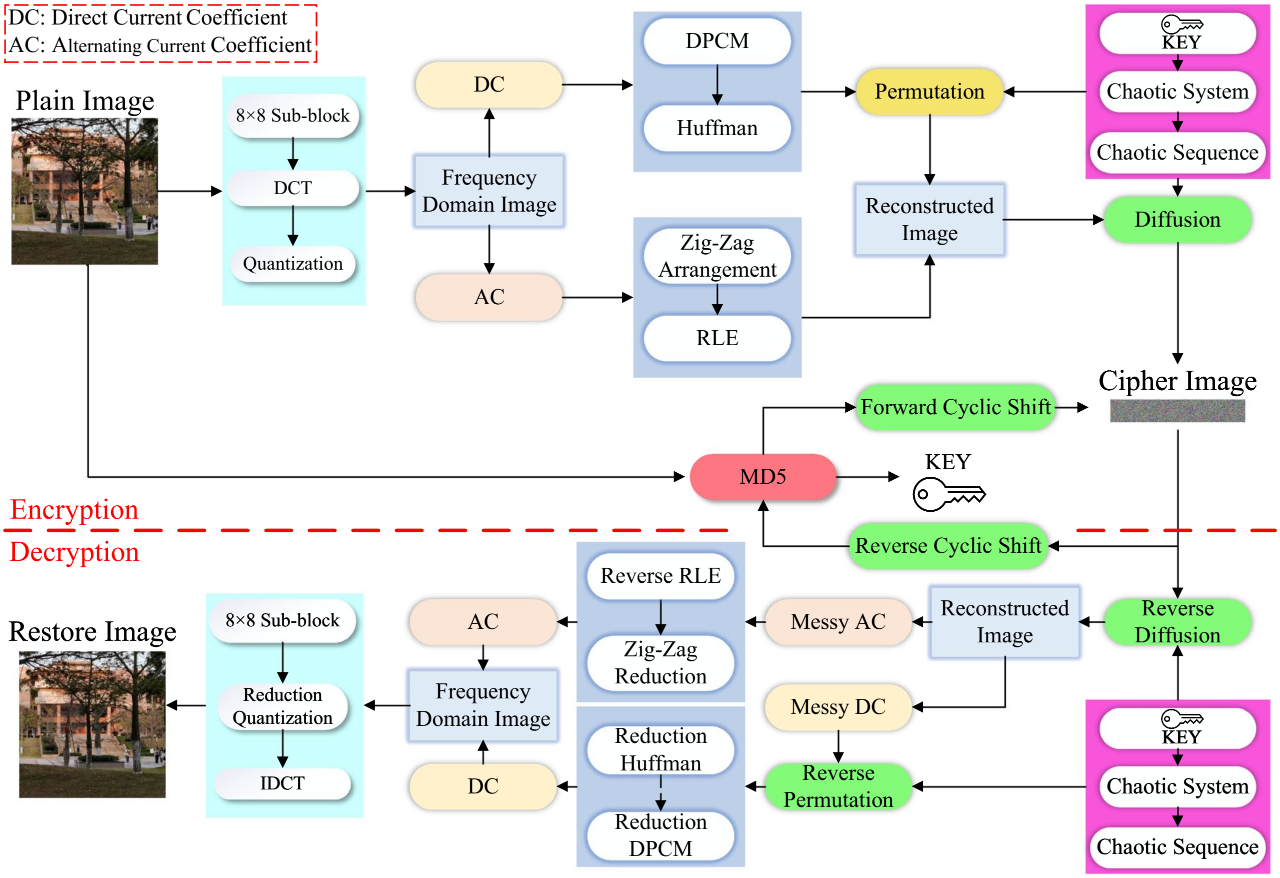
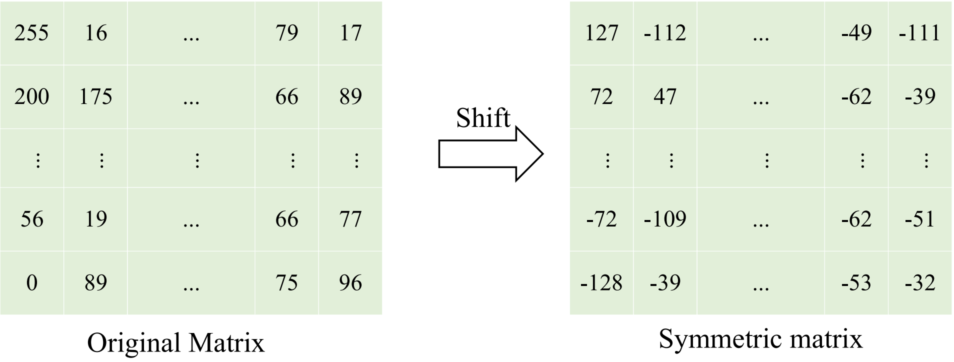


Figure 7. Principle and mechanism of image encryption.



255	16	...	79	17
200	175	...	66	89
⋮	⋮	⋮	⋮	⋮
56	19	...	66	77
0	89	...	75	96

Original Matrix

127	-112	...	-49	-111
72	47	...	-62	-39
⋮	⋮	⋮	⋮	⋮
-72	-109	...	-62	-51
-128	-39	...	-53	-32

Symmetric matrix

Figure 8. Pixel value translation.

is the customized function for shift binary to decimal, matrix [1,8] indicated encode once per 8 elements, m is the decimal number after hash value been bit cyclic shifted.

Step2: Time Domain Shifting and DCT Coding

Since DCT requires that the definition domain of the function is symmetrical, as shown in Fig. 8, since DCT requires that the definition domain of the function is symmetrical, the image pixel values are shifted right in the time domain, the shifted pixel values are distributed between -128 and 127. Subsequently, the image is divided into several 8×8 sub-blocks, and DCT is performed on these sub-blocks respectively to map the image matrix from the spatial domain to the frequency domain.

Step3: Quantify

Quantify the sub-block from **Step2** respectively. The specific formula is:

$$I' = \text{round}\left(\frac{I}{Q}\right) \tag{17}$$

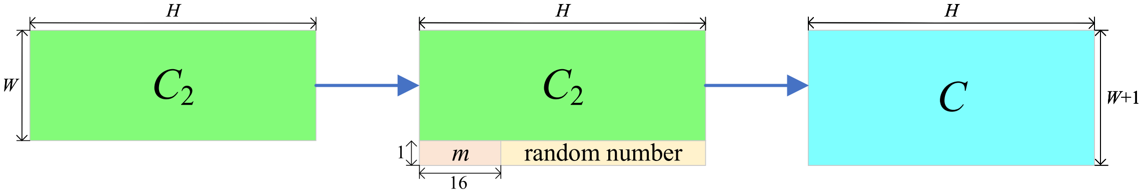


Figure 9. Hash value hiding.

where round(·) is the rounding function, I is a sub-block image of size 8 × 8, I' is the matrix after quantify, and Q is the quantization matrix. The quantization matrix is the key to controlling the compression ratio and also the image recovery after DCT. The quantization matrix can be customized according to the quality requirements of the output image. Usually, the custom quantization matrix is proportional to the standard quantization matrix. The larger the number in the matrix, the lower the image quality and the higher the compression rate. The commonly used standard quantization matrix Q_Y is:

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

Step4: Coefficient Extraction and Compression Coding

Extract the DC coefficients from each sub-block and construct these coefficients as a row matrix. Perform DPCM and Huffman Coding on the row matrix successively, and finally obtain a binary bit stream based on DC coefficients. Extract the AC coefficients from each sub-block, press Zig-Zag operations and perform RLE, and finally get a binary bit stream based on AC coefficients.

Step5: Coefficient Scrambling and Cipher Text Construction

Use the chaotic sequence K_1 to perform column permutation on the DC coefficient bit stream, the specific formula is as follows:

$$\begin{cases} [1, W] = \text{size}(DC) \\ [sW, indexW] = \text{sort}(K_1) \\ P(1, i) = DC(1, indexW(i)) \end{cases} \tag{19}$$

where size(·) is the array size read function, sort(·) is the sorting function, W is the width of the matrix, DC is the DC coefficient bit stream obtained in **Step4**, sW and $indexW$ are the sorting results and sorting index of the sort(·) function, respectively, P is the permuted DC coefficient bit stream. The replaced DC coefficient bit stream and the AC coefficient bit stream obtained in **Step4** are numerically reconstructed, and they are constructed into cipher text images with the same length and different width as the plaintext images.

Step6: Diffusion Encryption and Key Hiding

The matrix constructed in **Step5** is diffusion encrypted by using chaotic sequence K_2, the specific formula is as follows:

$$\begin{cases} [H, W] = \text{size}(C_1) \\ R = \text{floor}(\text{mod}(K_2 \times 10^{10}, 256)) \\ R_1 = \text{reshape}(R, H, W) \\ C_2 = \text{bitxor}(R_1, C_1) \end{cases} \tag{20}$$

where floor(·) and mod(·) are the integer-valued function and complementary function, bitxor(·) is the bit-level XOR function, reshape(·) is the matrix rearrangement function, C_1 is the cipher text from **Step6**, H and W are the length and width of C_1, and R is the processed chaotic sequence. The method of key hiding is shown in Fig. 9. C_2 is the ciphertext obtained by Eq. (20), C is the final output ciphertext, and m is the key value obtained in **Step1**.

Experimental verification and discussion

In this paper, the proposed encryption algorithm is verified and analyzed on MATLAB 2019. The system runs on a PC with Windows 10 64-bit operating system, Intel(R) Core(TM) i7-7700HQ CPU @ 2.80GHz 2.80 GHz processor and 16G RAM. In order to ensure the rigor of the experimental verification process, most of the test images in this paper are selected from the "USC-SIPI Image Database"[45] and "Wallpapers"[46] as the test images.

NIST 800-22 Test. Special Publication 800-22 Test Kit (NIST Randomness Test) provided by the National Institute of Standards and Technology[47]. The NIST test program is a statistical package that includes 16 test methods. These tests test the randomness of arbitrarily long binary sequences generated by hardware and software used as a confidential random or pseudo-random number generator. The binary sequence generated by the chaotic system we are using successfully passes this test, and the test results are shown in Table 1.

Statistical tests	p-values	Results
Frequency (monobit) test	0.191687	Successful
Block-frequency test	0.102526	Successful
Cumulative-sums test	0.162606	Successful
Runs test	0.657933	Successful
Longest-run test	0.637119	Successful
Binary matrix rank test	0.350485	Successful
Discrete fourier transform test	0.739918	Successful
Non-overlapping templates test	0.007694	Successful
Overlapping templates test	0.574903	Successful
Maurer's universal statistical test	0.964295	Successful
Approximate entropy test	0.834308	Successful
Random-excursions test (x = − 4)	0.000648	Successful
Random-excursions variant test (x = − 9)	0.048716	Successful
Serial test-1	0.637119	Successful
Serial test-2	0.699313	Successful
Linear-complexity test	0.616305	Successful

Table 1. NIST-800-22 test results.

	Ref.[49]	Ref.[50]	Ref.[51]	This paper
Key space (bit)	256	299	309	341

Table 2. Key space comparison.

Key space.

Since the chaotic system is highly sensitive to the initial chaotic values and control parameters, in this paper, four initial chaotic values $x_1(0), y_1(0), x_2(0), y_2(0)$ are used as the key parameters for encryption and decryption. The key parameter selects the double-precision data type with the precision of 10^{-16}, and the key space capacity is $10^{16\times4} \approx 2^{213}$. In addition, this paper introduces the MD5 hash value associated with the original image in this space to optimize the key space. The generated 128-bit hash value can expand the key space to $2^{213+128} = 2^{341}$. Finally, the key length reaches 341 bits. The results compared with other literature are shown in Table 2. It can be seen that the algorithm in this paper has a larger key space compared to other algorithms, which is sufficient to resist brute-force attacks[48].

Image restoration quality analysis.

In the compression algorithm, the information loss of the image is unavoidable, so it is necessary to analyze the quality of the decrypted and restored image. It is worth noting that the quantization matrix Q used in this section is an all-1 matrix. The reduction quality analysis in this paper is analyzed from four aspects: Unified Average Changing Intensity (UACI), Mean Square Error (MSE), Peak Signal-to-Noise Ratio (PSNR), and Structural SIMilarity (SSIM). They are as follows:

$$\begin{cases} \text{UACI} = \frac{1}{H\times W}\sum_{i=1}^{H}\sum_{j=1}^{W}\frac{|I(i,j)-C(i,j)|}{255}\times 100\% \\ \text{MSE} = \frac{1}{H\times W}\sum_{i=1}^{H}\sum_{j=1}^{W}\left(I(i,j)-C(i,j)\right)^2 \\ \text{PSNR} = 10\lg\left(\frac{MAX_I^2}{MSE}\right) \\ \text{SSIM} = \frac{[2\mu_I\mu_P+(0.01L)^2][2\sigma_{IP}+(0.03L)^2]}{[\mu_I{}^2+\mu_P{}^2+(0.01L)^2][\sigma_I{}^2+\sigma_P{}^2+(0.03L)^2]} \end{cases} \tag{21}$$

where H and W are the length and width of the image respectively, I is the plaintext, C is the image after restoration, MAX_I is the maximum value of the image pixel, and $MAX_I = 255$ in the grayscale image.μ_I and μ_P are the average values of the plaintext image and the image after restoration, σ_I and σ_P are the variances of the plaintext image and the image after restoration, σ_{IP} is the covariance of the plaintext image, and L is the dynamic range of pixel values. For two identical images, the theoretical value of UACI and MSE is 0, the theoretical value of SSIM is 1, and the PSNR should approach positive infinity. For digital images, it is generally considered that when the PSNR is 60dB, the image is numerically undistorted, and when the PSNR is 40dB, the image distortion is difficult to detect. In addition, the compression ratio defined in this paper is:

$$C = \left(1 - \frac{I_C}{I_P}\right)\times 100\% \tag{22}$$

Pictures	Size	Compression ratio (%)	UACI (%)	MSE	PSNR (dB)	SSIM
5.1.14.tiff[45]	256 × 256	22.2656	0.0331	0.0844	58.8668	0.9997
7.1.10.tiff[45]	512 × 512	31.4453	0.0328	0.0837	58.9038	0.9995
5.3.10.tiff[45]	1024 × 1024	30.2734	0.0323	0.0836	58.9064	0.9995
river.tiff[46]	3840 × 2160	33.6574	0.0177	0.0452	61.5837	0.9998

Table 3. Image restoration quality analysis.

	This paper	Ref.[52]	JPEG	JPEG2000
Pepper[45]	38.00	38.93	35.05	35.27
Baboon[45]	37.46	30.69	30.89	28.78
Boat[45]	35.66	38.26	34.52	31.32
Cameraman[45]	45.03	34.82	45.91	28.97

Table 4. PSNR at constant compression rate: 80%.

where C is the compression rate, I_C is the data of the ciphertext image, and I_P is the data of the plaintext image. In the encryption algorithm of this paper, since the plaintext and ciphertext are images of the same length and different width, and the length of each pixel is 8 bits, the above formula can be simplified as:

$$C = \left(1 - \frac{H_C}{H_P}\right) \times 100\% \tag{23}$$

where H_C is the pixel length of the ciphertext image, I_C is the pixel length of the plaintext image.

The experimental data are shown in Table 3. From the experimental results, it can be seen that the value of UACI is around 0.033, the value of MSE is around 0.084, the value of PSNR is around 58.9, and the value of SSIM is close to 1, all of which satisfy the theoretical value. Therefore, the algorithm in this paper can ensure that after encryption and compression Restore the high quality of the image.

The algorithm in this paper is compared with other algorithms and traditional JPEG and JPEG2000, some experimental results are shown in Table 4. It can be seen that this algorithm has certain advantages over other algorithms when the compression rate is constant.

Comparison of decrypted images under different compression ratios.

The quantization matrix is the key to controlling the compression ratio (encryption operations do not affect the compression ratio). The compression rate can be changed by customizing the quantization matrix. The relationship between the custom quantization matrix and the standard quantization matrix is as follows:

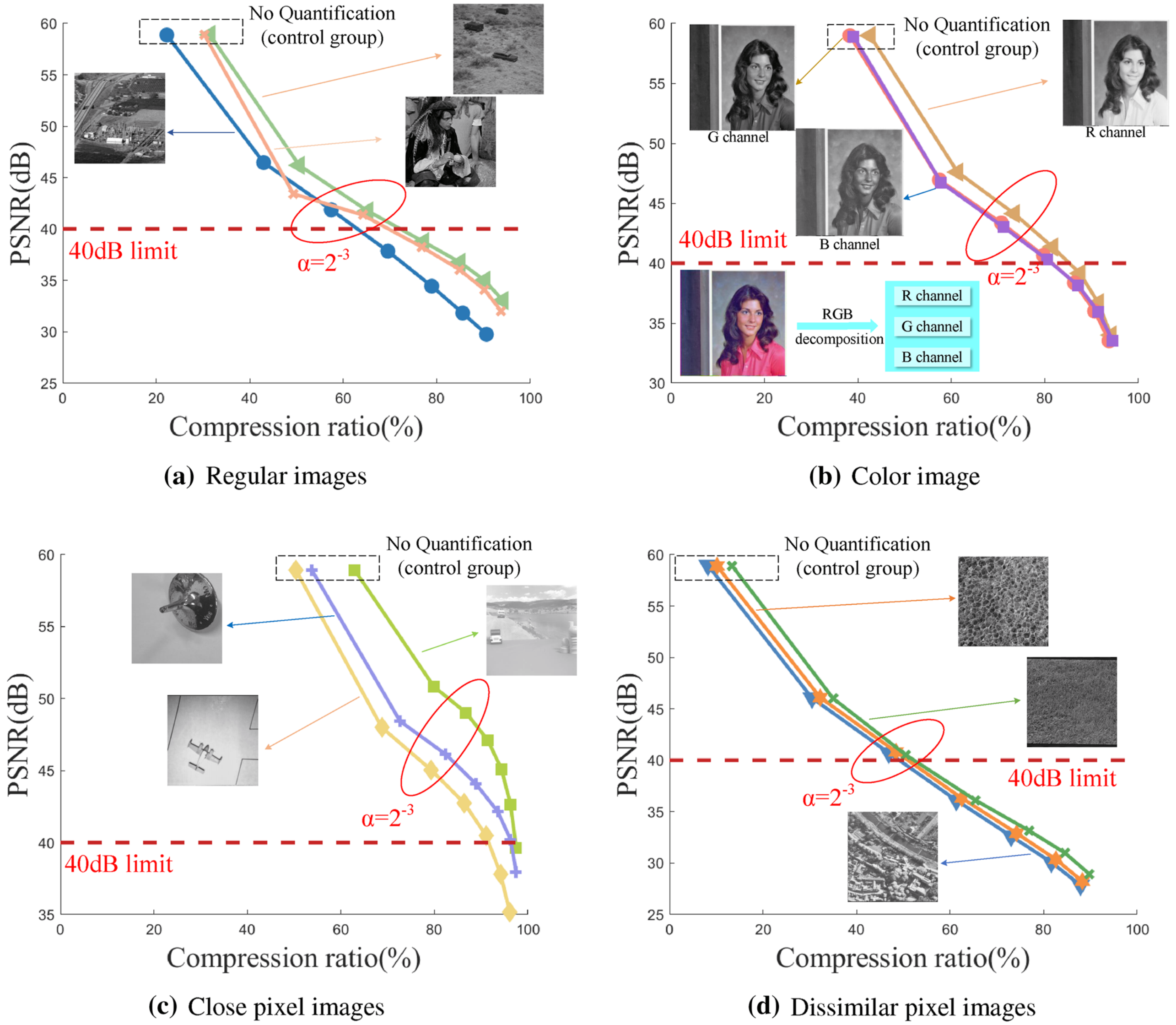
$$Q = \alpha Q_Y \tag{24}$$

where Q is the custom quantization matrix, Q_Y is the standard quantization matrix, the specific value of the matrix is given in **Step3** of the algorithm design, α is the quantization scale factor, and the value in this paper is $\alpha = \{2^{-4}, 2^{-3}, 2^{-2}, 2^{-1}, 1, 2\}$. Usually, the larger the α, the higher the compression rate, the quality of the restored image is lower. When the PSNR is 40dB, the distortion of the image is difficult to detect, so PSNR⩾40dB is used as the index of qualified image quality.

By adjusting the quantization scale factor α, observe the compression of different images, and then evaluate the quality of the decrypted image through PSNR to find the optimal value of the quantization scale factor α. The experimental results divide the images into four categories: general images, color images, images with similar pixels, and images with large pixel differences. The experimental results are shown in Fig. 10. The quantization scale factorin α in Fig. 10 is $2, 1, 2^{-1}, 2^{-2}, 2^{-3}, 2^{-4}$ from left to right. When $\alpha = 2^{-3}$, the PSNR value of the decrypted image is about 40dB, the image compression rate is between 50 and 85% at this time, and the compression rate is better. Based on the above, the subsequent experimental analysis in this paper, the value of the quantitative scale factor α is uniformly specified as 2^{-3}.

Sensitivity of the original image.

The encryption algorithm in this paper has strong plaintext sensitivity. When there is only a slight difference between two plaintext images, the encrypted ciphertext images will show a huge difference. The experimental results are shown in Fig. 11. The following is a differential analysis of the experimental results: two plaintext images with a size of 255 × 255 that differ by only one-pixel value, the encrypted ciphertext images are both 5 × 255 in size, with a total of 1275 pixels, there are 261 different pixels in total, that is, there is a 20% difference between the two ciphertexts. Experiments show that the encryption algorithm in this paper has better sensitivity to plaintext, and has better performance in blocking chosen-plaintext attacks.



(a) Regular images

(b) Color image

(c) Close pixel images

(d) Dissimilar pixel images

Figure 10. System performance analysis under different *α*.

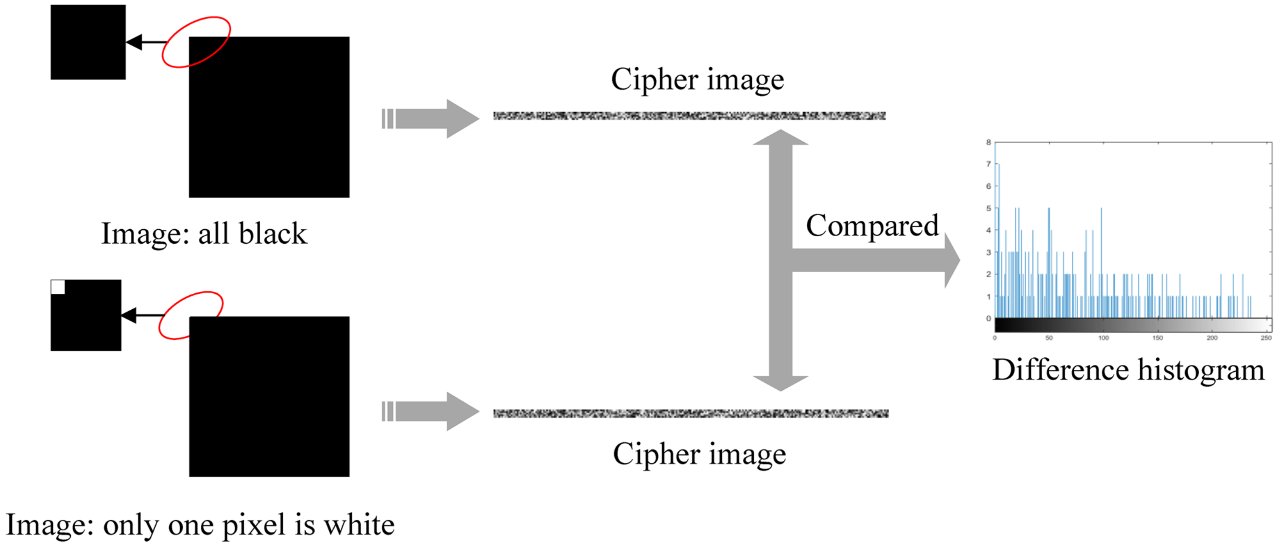
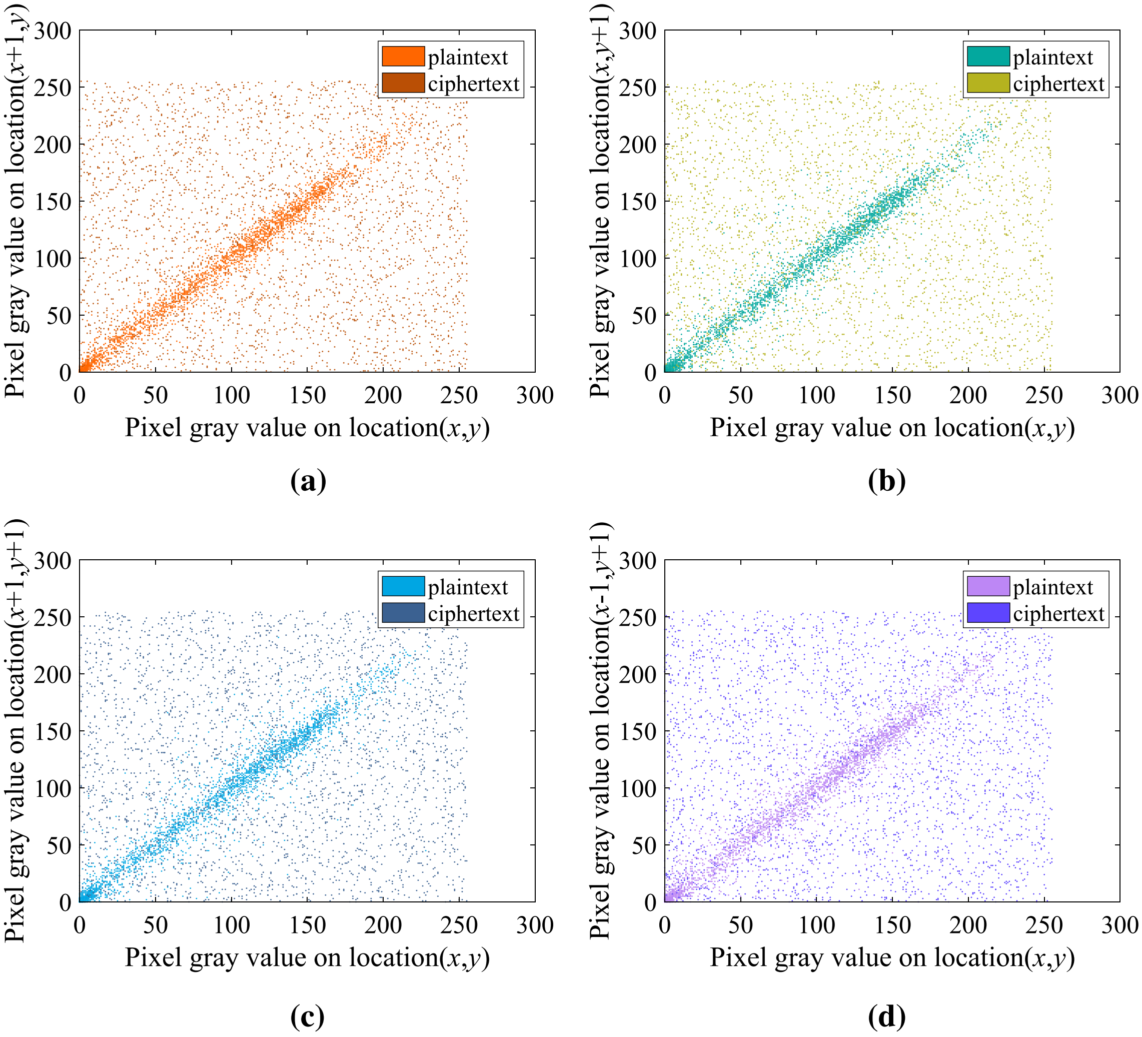


Figure 11. Plaintext sensitivity analysis.



(a)

(b)

(c)

(d)

Figure 12. Correlation coefficients distribution map of plain image and cipher image of 5.2.10.tiff (**a**) horizontal correlation; (**b**) vertically correlation; (**c**) diagonal correlation; (**d**) against angular direction correlation.

Correlation analysis of adjacent pixels. Correlation analysis is a method for judging the merits of digital image encryption algorithms in eliminating pixel correlation in plaintext images[53]. Due to the large amount of information redundancy, digital plaintext images have strong correlations between adjacent pixels in the horizontal, vertical and diagonal directions, which is unfavorable for information security. The digital image encryption algorithm is designed to eliminate the strong correlation between pixels, so the encryption algorithm usually compares the pixel correlation of the plaintext image and the ciphertext image in the horizontal, vertical, and diagonal directions when analyzing the security performance.

Taking the image 5.2.10.tiff[45] as an example, randomly select 3000 pairs of adjacent pixels in the plaintext image and the ciphertext image, and calculate the adjacent pixel correlation coefficient in the horizontal, vertical, diagonal and anti-diagonal directions respectively. The correlation scatters plot in each direction is shown in Fig. 12. From the experimental results, it can be seen that the adjacent pixels in the horizontal, vertical, diagonal, and anti-diagonal directions of the plaintext image are centrally distributed, while in the ciphertext image, the adjacent pixels in these directions are all randomly distributed. The experimental results show that the adjacent pixels of the plaintext image are highly correlated, while the adjacent pixels of the ciphertext image encrypted by this algorithm has almost no correlation, indicating that the encryption algorithm has high security.

Histogram analysis. Cryptographic images need better statistical properties to resist attacks against encrypted images[54]. Image histogram can effectively represent the information carried by digital images through the gray value distribution of pixels. Statistical decryption attacks often use this as a breakthrough point to crack encrypted images. Digital image encryption algorithm can encrypt the histogram of plaintext image to the histogram of noise style with uniform distribution characteristics to cover up the main information of plaintext digital image. The more uniform the histogram is, the better the main information of plaintext digital image is hidden.

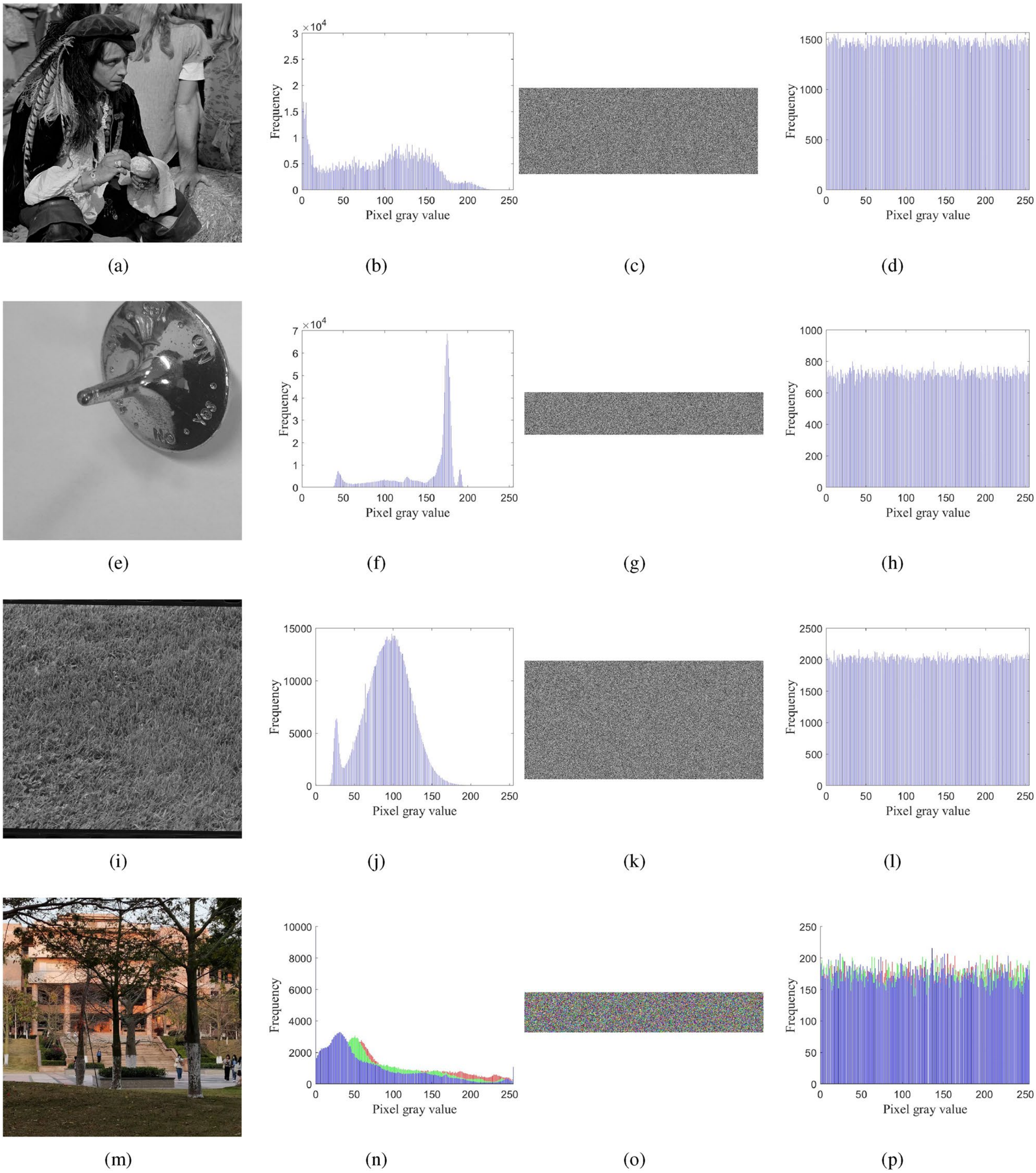


Figure 13. The histograms of images before and after encryption (**a**) 1#[45] plain image; (**b**) the histogram of (**a**); (**c**) 1# cipher image; (**d**) the histogram of (**c**); (**e**) 2# plain image; (**f**) the histogram of (**e**); (**g**) 2# cipher image; (**h**) the histogram of (**g**); (**i**) 3# plain image; (**j**) the histogram of (**i**); (**k**) 3#[45] cipher image; (**l**) the histogram of (**k**); (**m**) 4# plain image; (**n**) the histogram of (**m**); (**o**) 4# cipher image; (**p**) the histogram of (**o**).

Different images are selected as plaintext images for analysis, and the results are shown in Fig. 13. Images 1# and 3# are freely available in Image Library "USC-SIPI Image Database"[45]. Images 2# and 4# are taken by author Linchao Ma. It can be seen from the experimental results that any image after encryption processing is noise-like distribution, which shows that the encryption scheme can better resist statistical attacks and has a better encryption effect.

Picture	Plain image	Cipher image
7.1.10.tiff[45]	5.9088	7.9981
1.1.13.tiff[45]	7.2955	7.9986
5.2.10.tiff[45]	5.7056	7.9987
1.4.10.tiff[45]	6.9216	7.9996

Table 5. Information entropy of the plain image and ciphered image.

Picture	Encryption time (s)	Decryption time (s)	Compression ratio
5.1.11.tiff[45](256256)	0.963761	0.558822	79.2969 %
motion01.512.tiff[45](512512)	1.976872	0.846713	86.7188 %
1$^{\#}$(10241024)	15.394230	3.667921	82.4219 %

Table 6. Encryption time comparison.

Information entropy analysis.

Information entropy is an indicator used to measure the information content and uncertainty of digital images[55]. The greater the information entropy of digital image, the higher the information uncertainty of digital image, and the more invisible information contained in digital image. Therefore, in the digital image encryption algorithm, it is usually hoped that the ciphertext image has a large information entropy. The mathematical calculation formula of information entropy is as follows:[56]

$$H(n) = -\sum_{i=1}^{L} P(n_i) \log_2 P(n_i) \tag{25}$$

where i represents the pixel gray value, $P(n_i)$ represents the probability that the gray value appears in the digital image. Through the calculation of Eq. (25), it can be seen that for 8bit gray image, the theoretical value of information entropy is the maximum value of 8. Taking different images as test images, the test results are shown in Table 5. The experimental results show that the information entropy of both ciphertext images is above 7.998, which is close to the theoretical value of 8, indicating that the encryption algorithm has a good encryption effect and can better resist the information entropy attack.

Efficiency analysis.

There are many factors that can affect the efficiency, such as the size of the image, the compression rate, and the degree of arithmetic power consumed by the encryption operation[57]. We select three images with sizes of 256×256, 512×512, and 1024×1024, respectively, and encrypt and decrypt them respectively when the value of the quantization scale factor is $\alpha = 2^{-3}$. Table 4 is obtained by measuring the time required for encryption, the time required for decryption and the image compression rate. As shown in Table 6, when the image size is larger, the required encryption and decryption time will increase accordingly. It can be seen from the experimental results that the overall encryption efficiency is acceptable.

Conclusion

This paper proposes an algorithm of high-quality restoration image encryption using Discrete Cosine Transform (DCT) frequency-domain compression coding and chaos. Firstly, the image hash value is used for the generation of an encryption key with plaintext correlation, then lightweight chaos is generated based on the key to obtain pseudo-random sequence. Secondly, partition the image into several 8×8 subblocks, and perform DCT and quantization operations on all the subblocks respectively to obtain the DCT coefficient matrix. Next, extract the direct current (DC) coefficients and alternate current (AC) coefficients in the DCT coefficient matrix for compression coding to obtain two sets of bitstream containing DC coefficient and AC coefficient information. Then, permute the DC coefficient bit stream by the chaotic sequence, and perform ciphertext image reconstruction with the AC coefficient bitstream. Finally, the chaotic sequence is used to perform ciphertext diffusion, and the processed hash value is hidden in the ciphertext to obtain the final ciphertext. The theoretical and experimental analysis shows that the algorithm has the characteristics of high compression rate, high-quality image restoration large key space, strong plaintext sensitivity, strong key sensitivity and so on. Therefore, the method proposed in this paper can better improve the effectiveness and reliability of information in the transmission process, and is expected to provide a new idea for secure communication in the context of big data era.

Data availability

The datasets used and analysed during the current study available from the corresponding author on reasonable request.

Received: 3 June 2022; Accepted: 9 September 2022
Published online: 03 October 2022

References

1. Wen, H., Zhang, C. & Chen, P. A quantum chaotic image cryptosystem and its application in iot secure communication. *IEEE Access* **9**, 20481–20492 (2021).
2. Xian, Y. & Wang, X. Fractal sorting matrix and its application on chaotic image encryption. *Inf. Sci.* **547**, 1154–1169 (2021).
3. Ye, G., Jiao, K. & Huang, X. An image encryption scheme based on public key cryptosystem and quantum logistic map. *Sci. Rep.* **10**, 21044 (2021).
4. Wei, H., Cui, M. & Zhang, C. Chaotic key generation and application in OFDM-PON using QAM constellation points. *Opt. Commun.* **490** (2021).
5. Hu, G. & Li, B. Coupling chaotic system based on unit transform and its applications in image encryption. *Signal Process.* **178**, 107790 (2021).
6. Zhou, S., Teo, C. & Ayyer, K. An encryption cdecryption framework to validating single-particle imaging. *Sci. Rep.* **11**, 971 (2021).
7. Wu, T., Zhang, C. & Chen, Y. Compressive sensing chaotic encryption algorithms for OFDM-PON data transmission. *Opt. Express* **29**, 3669–3684 (2021).
8. Gao, X., Yu, J. & Yan, H. A new image encryption scheme based on fractional-order hyperchaotic system and multiple image fusion. *Sci. Rep.* **11**, 15737 (2021).
9. Zhang, C., Yan, Y. & Wu, T. Phase masking and time-frequency chaotic encryption for OFDM-PON. *IEEE Photonics J.* **10**, 1–9 (2018).
10. Wen, H., Zhang, C. & Huang, L. Security analysis of a color image encryption algorithm using a fractional-order chaos. *Entropy* **23**, 258 (2021).
11. He, Y., Zhang, Y. Q. & He, X. A new image encryption algorithm based onthe of-lstms and chaotic sequences. *Sci. Rep.* **11**, 6398 (2021).
12. Park, W., Lee, B. & Kim, M. Fast computation of integer dct-v, dct-viii and dst-vii for video coding. *IEEE Trans. Image Process.* **28**, 5839–5851 (2019).
13. Wen, H., Xu, J. & Liao, Y. A security-enhanced image communication scheme using cellular neural network. *Entropy* **23**, 1000 (2021).
14. Ghaffari, A. Image compression-encryption method based on two-dimensional sparse recovery and chaotic system. *Sci. Rep.* **11**, 369 (2021).
15. Ye, G., Jiao, K. & Huang, X. An image encryption scheme based on public key cryptosystem and quantum logistic map. *Sci. Rep.* **11**, 8549 (2021).
16. Wen, H. & Yu, S. Cryptanalysis of an image encryption cryptosystem based on binary bit planes extraction and multiple chaotic maps. *Eur. Phys. J. Plus* **134**, 337 (2019).
17. Wang, X., Guan, N. & Zhao, H. A new image encryption scheme based on coupling map lattices with mixed multi-chaos. *Sci. Rep.* **10**, 9784 (2020).
18. Liu, H., Kadir, A. & Xu, C. Color image encryption with cipher feedback and coupling chaotic map. *Int. J. Bifur. Chaos* **30**, 2050173 (2020).
19. Khan, N. A., Altaf, M. & Khan, F. A. Selective encryption of jpeg images with chaotic based novel s-box. *Multimed. Tools Appl.* **80**, 9639–9656 (2020).
20. Wen, H., Yu, S. & J, L. Breaking an image encryption algorithm based on dna encoding and spatiotemporal chaos. *Entropy* **21**, 246 (2019).
21. Yang, Y., Xu, P. & Yang, R. Quantum hash function and its application to privacy amplification in quantum key distribution, pseudo-random number generation and image encryption. *Sci. Rep.* **6**, 19788 (2016).
22. Audhkhasi, R. & Povinelli, M. L. Generalized multi-channel scheme for secure image encryption. *Sci. Rep.* **11**, 22669 (2021).
23. Gan, Z., Chai, X. & Han, D. A chaotic image encryption algorithm based on 3-d bit-plane permutation. *Neural Comput. Appl.* **31**, 7111–7130 (2019).
24. Farah, M., Guesmi, R. & Kachouri, A. A novel chaos based optical image encryption using fractional fourier transform and dna sequence operation. *Opt. Laser Technol.* **121**, 105777 (2019).
25. Bwa, B., Bfz, A. & Xwl, A. An image encryption approach on the basis of a time delay chaotic system - sciencedirect. *Optik* **225** (2020).
26. Pourasad, Y., Ranjbarzadeh, R. & Mardani, A. A new algorithm for digital image encryption based on chaos theory. *Entropy* **23**, 341 (2021).
27. Patel, S. & Vaish, A. A novel image coding through the chaos theory and compressed sensing. In *Proceedings of International Conference on Data Science and Applications*, 615–623 (Singapore, 2022).
28. Kumar, M. & Vaish, A. An efficient compression of encrypted images using wdr coding. In *Proceedings of Fifth International Conference on Soft Computing for Problem Solving*, 729–741 (Singapore, 2016).
29. Kumar, M. & Vaish, A. Prediction error based compression of color images using wdr coding. *AEU: Archiv fur Elektronik und Ubertragungstechnik: Electronic and Communication* **70**, 1164–1171 (2016).
30. Kumar, M. & Vaish, A. Encryption of color images using msvd in dcst domain. *Opt. Lasers Eng.* **88**, 51–59 (2017).
31. Ye, H. S., Zhou, N. R. & Gong, L. H. Multi-image compression-encryption scheme based on quaternion discrete fractional hartley transform and improved pixel adaptive diffusion. *Signal Process.* **175**, 107652 (2020).
32. Wu, T., Zhang, C. & Huang, H. Security improvement for ofdm-pon via dna extension code and chaotic systems. *IEEE Access* **8**, 75119–75126 (2020).
33. Cui, M., Zhang, C. & Chen, Y. Multilayer dynamic encryption for security ofdm-pon using dna-reconstructed chaotic sequences under cryptanalysis. *IEEE Access* **9**, 18052–18060 (2021).
34. Pan, X., Wu, J. & Li, Z. Laguerre-gaussian mode purity of gaussian vortex beams. *Optik Int. J. Light Electron Opt.* **230**, 166320 (2021).
35. Chen, L., Hao, Y. & Huang, T. Chaos in fractional-order discrete neural networks with application to image encryption. *Neural Netw.* **125**, 174–184 (2020).
36. Hua, Z., Zhu, Z. & Yi, S. Cross-plane colour image encryption using a two-dimensional logistic tent modular map. *Inf. Sci.* **546**, 1063–1083 (2021).
37. Liu, S., Li, C. & Hu, Q. Cryptanalyzing two image encryption algorithms based on a first-order time-delay system. *IEEE Multimed.* **29**, 74–84 (2021).
38. Lia, C., Lina, D. & J, L. Cryptanalyzing an image encryption algorithm based on autoblocking and electrocardiography. *IEEE Multimedia* **25**, 46–56 (2019).
39. Li, C., Lin, D. & J, L. Cryptanalyzing an image-scrambling encryption algorithm of pixel bits. *IEEE MultiMedia* **24**, 64–71 (2017).
40. Leonov, G. A. & Kuznetsov, N. V. Differences and similarities in the analysis of lorenz, chen, and lu systems. *Appl. Math. Comput.* **256**, 334–343 (2015).
41. Hua, Z. & Zhou, Y. Dynamic parameter-control chaotic system. *IEEE Trans. Cybern.* **46**, 3330–3341 (2015).
42. Li, H., Hua, Z. & Bao, H. Two-dimensional memristive hyperchaotic maps and application in secure communication. *IEEE Trans. Industr. Electron.* **68**, 9931–9940 (2021).

43. Hua, Z. & Zhou, Y. Exponential chaotic model for generating robust chaos. *IEEE Trans. Syst. Man Cybern. Syst.* **51**, 3713–3724 (2019).
44. Hua, Z., Zhou, Y. & Bao, B. Two-dimensional sine chaotification system with hardware implementation. *IEEE Trans. Ind. Inf.* **16**, 887–897 (2019).
45. Usc-sipi image database. http://sipi.usc.edu/database.
46. Wallpaper. https://wallpapers.com/.
47. Wen, H., Liu, Z. & Lai, H. Secure DNA-coding image optical communication using non-degenerate hyperchaos and dynamic secret-key. *Mathematics* **10**, 3180 (2022).
48. Midoun, M. A., Wang, X. & Talhaoui, M. Z. A sensitive dynamic mutual encryption system based on a new 1d chaotic map. *Opt. Lasers Eng.* **139**, 106485 (2021).
49. Hua, Z., Zhou, Y. & Huang, H. Cosine-transform-based chaotic system for image encryption. *Inf. Sci.* **480**, 403–419 (2019).
50. Xu, Q., Sun, K. & Cao, C. A fast image encryption algorithm based on compressive sensing and hyperchaotic map. *Opt. Lasers Eng.* **121**, 203–214 (2019).
51. Song, C. & Qiao, Y. A novel image encryption algorithm based on dna encoding and spatiotemporal chaos. *Entropy* **17**, 6954–6968 (2015).
52. Vaish, A. & Kumar, M. Wdr coding based image compression technique using pca. In *2015 International Conference on Signal Processing and Communications: 2015 International Conference on Signal Processing and Communications (ICSC 2015), 16-18 March, 2015, Noida, India*, 360–365 (Noida, 2015).
53. Xc, A., Jb, A. & Zg, B. Color image compression and encryption scheme based on compressive sensing and double random encryption strategy. *Signal Process.* **176**, 107684 (2020).
54. Chai, X., Zheng, X. & Gan, Z. Exploiting plaintext-related mechanism for secure color image encryption. *Neural Comput. Appl.* **32**, 8065–8088 (2019).
55. Chai, X., Fu, X. & Gan, Z. An efficient chaos-based image compression and encryption scheme using block compressive sensing and elementary cellular automata. *Neural Comput. Appl.* **32**, 4961–4988 (2018).
56. Hla, B., Yx, C. & Chao, M. Chaos-based image hybrid encryption algorithm using key stretching and hash feedback. *Optik* **216**, 164925 (2020).
57. Wen, H., Chen, Z. & Zheng, J. Design and Embedded Implementation of Secure Image Encryption Scheme Using DWT and 2D-LASM. *Entropy* **24**, 1332 (2022).

Author contributions

H.W. contributed to the design and conception of the study. L.M. is mainly responsible for code writing and article writing. L.L. and Z.C. are mainly responsible for code modification and experimental data collection. Y.H. is mainly responsible for Latex typesetting. R.L. and Y.L. are mainly responsible for translation and proofreading. Z.L. is mainly responsible for drawing. W.L. and J.W. are mainly responsible for literature search and format proofreading. C.Z. provides guidance. All authors reviewed the manuscript.

Funding

This work was supported in part by the National Science Foundation of China under Grant 62071088; in part by the Project for Innovation Team of Guangdong University under Grant 2018KCXTD033; in part by Opening Project Guangdong Province Key Laboratory of information Security Technology under Grant 2020B1212060078; in part by Special Projects for Key Fields of the Education Department of Guangdong Province under Grant 2021ZDZX1083; and in part by Project for Zhongshan Science and Technology under Grant 2021B2062; in part by the Science and Technology Projects of Guangdong Province under Grant 2021A0101180005; and in part by the Construction Project of Professional Quality Engineering in Guangdong Province under Grant YLZY202201.

Competing interests

The authors declare no competing interests.

Additional information

Correspondence and requests for materials should be addressed to H.W. or C.Z.