



OPEN

# Exploiting high-quality reconstruction image encryption strategy by optimized orthogonal compressive sensing

Heping Wen<sup>1,2</sup>, Lincheng Yang<sup>1</sup>, Chixin Bai<sup>1</sup>, Yiting Lin<sup>1,2</sup>, Tengyu Liu<sup>1</sup>, Lei Chen<sup>3,4</sup>✉, Yingchun Hu<sup>3</sup> & Daojing He<sup>1,4</sup>

Compressive sensing is favored because it breaks through the constraints of Nyquist sampling law in signal reconstruction. However, the security defects of joint compression encryption and the problem of low quality of reconstructed image restoration need to be solved urgently. In view of this, this paper proposes a compressive sensing image encryption scheme based on optimized orthogonal measurement matrix. Utilizing a combination of DWT and OMP, along with chaos, the proposed scheme achieves high-security image encryption and superior quality in decryption reconstruction. Firstly, the orthogonal optimization method is used to improve the chaotic measurement matrix. Combined with Part Hadamard matrix, the measurement matrix with strong orthogonal characteristics is constructed by Kronecker product. Secondly, the original image is sparsely represented by DWT. Meanwhile, Arnold scrambling is used to disturb the correlation between its adjacent pixels. Following this, the image is compressed and measured in accordance with the principles of compressive sensing and obtain the intermediate image to be encrypted. Finally, the chaotic sequence generated based on 2D-LSCM is used to perform on odd-even interleaved diffusion and row-column permutation at bit-level to obtain the final ciphertext. The experimental results show that this scheme meets the cryptographic requirements of obfuscation, diffusion and avalanche effects, and also has a large key space, which is sufficient to resist brute-force cracking attacks. Based on the sparse and reconstruction algorithm of compressive sensing proposed in this paper, it has better image restoration quality than similar algorithms. Consequently, the compressive sensing image encryption scheme enhances both security and reconstruction quality, presenting promising applications in the evolving landscape of privacy protection for network big data.

**Keywords** Frequency domain compression, Image encryption, Compressive sensing, Optimized orthogonal

In the wake of the rapid evolution of computer communication and network technologies, diverse forms of data and information are being disseminated through networks with increased frequency, broader reach, and heightened velocity<sup>1–3</sup>. The emergence of these requirements for information interchange, particularly in ensuring a more secure transmission environment, has been noteworthy<sup>4–6</sup>. As one of the most intuitive and common data types in information transmission, images contain a substantial amount of sensitive information<sup>7–9</sup>. Consequently, the utilization of image encryption techniques can effectively prevent the leakage of critical data during transmission<sup>10–12</sup>. Several encryption methods have been proposed to address this challenge, including thumbnail-preserving encryption<sup>13–15</sup>, biometric encoding<sup>16–18</sup>, Frequency domain encryption<sup>19,20</sup>, bit-plane encryption<sup>21–23</sup>, Fourier transformation<sup>24–26</sup>, and chaos theory<sup>27–29</sup>, among others<sup>30,31</sup>. In particular, chaotic algorithms have gained widespread acceptance in image encryption due to their unpredictability, pseudo-randomness, and high sensitivity to initial values<sup>32–35</sup>.

<sup>1</sup>Zhongshan Institute, University of Electronic Science and Technology of China, Zhongshan 528402, China. <sup>2</sup>School of Information and Communication Engineering, University of Electronic Science and Technology of China, Chengdu 611731, China. <sup>3</sup>GuangDong Engineering Technology Research Center of Cryptographic Product and System Evaluation, Shenzhen 518118, China. <sup>4</sup>School of Computer Science and Technology, Harbin Institute of Technology (Shenzhen), Shenzhen 518118, China. ✉email: chenlei\_security@163.com

Taking a global perspective, numerous scholars have achieved a series of significant theoretical and practical advancements in the use of chaos for image encryption<sup>36–39</sup>. Simultaneously, the field of compressive sensing theory has garnered favour among many cryptography experts due to its groundbreaking performance in signal sampling<sup>40–42</sup>. In 2021<sup>43</sup>, introduced an image encryption scheme based on four-winged hyperchaotic system, combined with compressive sensing and DNA encoding, effectively reduced the transmission cost. In 2022<sup>44</sup>, presented an image encryption approach that utilizes SHA-3 and an asymmetric key system. This method employs the RSA algorithm to encrypt the plaintext key and disclose the corresponding ciphertext key, avoiding the problem of additional transmission of the key in the channel. In 2023<sup>45</sup>, presented a secure and efficient image encryption approach that integrates parallel compression sensing with secret sharing. This method attains network system security and availability even with resource constraints. Within the ongoing exploration of compression-aware chaotic image encryption, the efficacy of chaotic sum algorithms significantly influences the security and efficiency of cryptographic systems. In contrast, most of the existing algorithms only obtain snowflake ciphertext images by scrambling at the pixel level or 2-bit, which has a coarse granularity and is susceptible to attacks from third parties. It is imperative and urgent to explore an image encryption algorithm with finer encryption granularity that utilizes chaotic mapping constructs to resist various illegal attacks.

This paper introduces a optimized orthogonal compressive sensing image encryption scheme based on 2D-LSCM. Firstly, the scheme adopts Discrete Wavelet Transform to sparsify the original image and performs Arnold scrambling on the sparse image to increase the uncorrelation between its neighbouring pixels. Secondly, based on the theory of CS, an optimized orthogonal measurement matrix is constructed by using the Kronecker product, a part Hadamard matrix and an optimized processed chaotic sequence to measure the sparse image and obtain the compressed measured matrix. Finally, odd-even interleaved diffusion and bit-level permutation is used for the measured matrix to obtain the final ciphertext image.

The main contributions of this paper are as follows:

- This paper proposes a security-enhanced, high-performance integrated image encryption scheme combining compressive sensing. Compared with most of the similar spatial domain based encryption schemes, it has lower computational complexity and improves the efficiency and security of encryption.
- A construction method for a compressive sensing measurement matrix is proposed. This method incorporates a plaintext correlation mechanism, ensuring that the measurement matrix possesses orthogonal characteristics. The orthogonal features of the measurement matrix contribute to improved reconstruction quality following decryption.
- In the image encryption algorithm, a chaotic key stream with plaintext correlation is generated. This key stream is utilized to control odd-even interleaved diffusion and row-column permutation operations at bit-level for encrypting the plaintext image. This approach offers a high granularity of encryption, effectively defending against chosen plaintext attack.
- Focusing on the sparse representation method and reconstruction algorithm of compressive sensing, this paper analyzes the impact of various parameters on recovery quality and selects the optimized combination scheme. Experimental results validate the superiority of the proposed scheme.

The organization of the remaining sections of this paper is as follows: Section "Related theory" provides a brief introduction to chaotic systems and the compressive sensing algorithm. Section "Image encryption and decryption scheme" presents the encryption algorithm designed in this paper. Section "Simulation results and performance analysis" offers experimental and simulation results. The final part concludes the paper.

## Related theory

### The used chaotic system

#### 2D-LSCM map

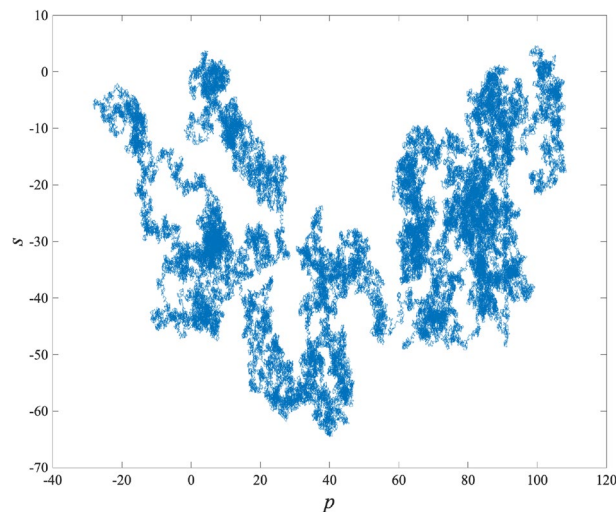
2D-LSCM is derived from two existing 1D chaotic mappings, namely the Logistic mapping and the Sine mapping<sup>46</sup>. The mapping diagrams are defined as follows:

$$\begin{cases} x_{i+1} = \sin(\pi(4\theta x_i(1-x_i) + (1-\theta)\sin(\pi y_i))) \\ y_{i+1} = \sin(\pi(4\theta y_i(1-y_i) + (1-\theta)\sin(\pi x_{i+1}))) \end{cases} \quad (1)$$

where  $\theta$  denotes the control parameter,  $\theta \in [0, 1]$ . The definition reveals the generation process, individual Logistic mapping and Sine mapping have been confirmed to have drawbacks such as simple behaviors and fragile chaotic intervals. Whereas 2D-LSCM couples both of these mappings and extends the dimension from 1D to 2D after performing a sinusoidal transformation on the coupling result. By this way, the complexity of Logistic mapping and Sinusoidal mapping can be fully mixed to obtain complex chaotic behavior.

#### 0-1 test results of chaos

The Gottwald Melbourne 0-1 test serves as a computational instrument for determining parameters in close proximity to 0 or 1, facilitating a precise differentiation between regular and chaotic motion. In our investigation, the 0–1 Gottwald Melbourne test was employed to generate 10,000 outcomes, demonstrating an average value of 0.9979. This notable result underscores the exceptional performance exhibited by the chaotic system. The graphical representation of the test outcomes is presented in Fig. 1.



**Figure 1.** The Gottwald Melbourne 0-1 test of 2D-LSCM.

### Compressive sensing

Donoho et al. proposed a novel signal sampling technique, where compression of the data is accomplished at the same time as sampling, named compressive sensing. The rationale is that if the signal is sparse, it can be accurately reconstructed by solving an optimization problem with a much smaller number of samples than required by the Nyquist sampling theorem.

In compressive sensing, whether the signal has sparse properties is a prerequisite for judging whether the signal can be reconstructed accurately. Except for a few naturally sparse signals, most signals need to be represented sparsely on some sparse basis, described as  $x = \Psi s$ , where  $\Psi$  is the sparse basis matrix, and  $s$  is the sparse coefficient. Assuming the signal  $x$  to be processed is either naturally sparse or can be sparsely represented (with size of  $N \times 1$ ), the measurement process can be shown in Fig. 2 and expressed as:

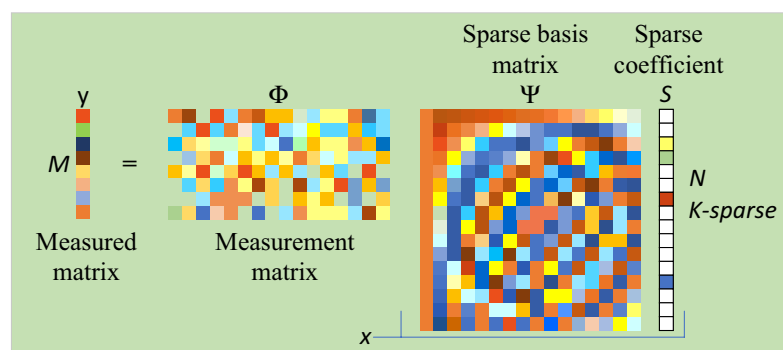
$$y = \Phi x = \Phi \Psi s = As \quad (2)$$

where  $\Psi$  denotes the measurement matrix, utilized to project the high-dimensional signal  $x$  into a low-dimensional space, with size of  $M \times N$  ( $M < N$ ). And  $y$  denotes the measured matrix, with size of  $M \times 1$ .  $A$  denotes the sensing matrix, which is the product of the measurement matrix and the sparse basis matrix, and it can be represented as  $A = \Phi \Psi$ .

In compressive sensing theory, another crucial criterion for determining whether a signal can be reconstructed is assessing whether the sensing matrix satisfies the Restricted Isometry Property (RIP). If it does, the signal can be overwhelmingly reconstructed by solving the following convex optimization problem:

$$\min \|s\|_1 \text{ s.t. } y = \Phi \Psi s \quad (3)$$

where  $\min \|s\|_1$  denotes the  $l_1$  norm of vector  $s$ . Orthogonal Matching Pursuit (OMP) and Basis Pursuit (BP) are both practical algorithms for solving such problems.



**Figure 2.** The schematic diagram of the compressive sensing process.

### Arnold map

Arnold mapping is widely used in image processing as a fast and effective scrambling method. It can be described as a stretching, folding and stitching process for a two-dimensional image matrix, the geometric interpretation of this process is shown in Fig. 3. For a image of size  $M \times N$ , the definition of Arnold map can be characterised by the following formula:

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{bmatrix} 1 & b \\ a & ab+1 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} \bmod N \quad (4)$$

where  $x_n, y_n$  denote the original image pixel position,  $x_{n+1}, y_{n+1}$  denote the scrambled pixel position,  $a, b$  denote the mapping parameters.

Arnold mapping exhibits periodicity, with the period depending on the image dimensions, which implies that repeated permutations of an image can be reverted to the original image. For a square image of size  $N \times N$ , it can also be restored using the inverse transformation formula. The inverse Arnold mapping formula is as follows:

$$\begin{bmatrix} x_n \\ y_n \end{bmatrix} = \begin{bmatrix} ab+1 & -b \\ -a & 1 \end{bmatrix} \begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} \bmod N \quad (5)$$

In image encryption algorithms combined with compressive sensing, it is crucial to perturb the image and reduce the correlation between adjacent pixels before measurement. This step can significantly enhance the reconstruction quality of the image.

### Image encryption and decryption scheme

The proposed bit-level encryption scheme based on compressive sensing in this paper comprises two primary modules: compression measurement and the encryption of the digital format image. Firstly, the Discrete Wavelet Transform is used to convert the original image from the spatial domain to the frequency domain for sparse representation. After Arnold scrambling, the sparse image is compressed and measured to obtain the intermediate image to be encrypted. Finally, the chaotic sequence generated based on 2D-LSCM is used to encrypt the image with odd-even interleaved diffusion and row-column permutation at bit-level to obtain the final ciphertext image. The overall schematic of the scheme is shown in Fig. 4.

### Generation of the chaotic sequence and preprocessing

The key utilized in this algorithm is derived from the original image's feature values obtained through a hash function. After preprocessing, these values are substituted into the chaotic system to generate the four necessary chaotic sequences.

#### Step 1: Extraction of image feature values

Use the hash SHA-256 to read the image feature value, which consists of a fixed 64-bit length of the hexadecimal number, and in order every four digits in a group to decimal representation, denoted as  $K = \{k_1, k_2, \dots, k_{16}\}$ . Depending on the value of  $k_5$ , different arrangement methods are chosen to surround these 16 numbers in order into a square matrix of size  $4 \times 4$ .

#### Step 2: Preprocessing of image feature values

For the obtained  $4 \times 4$  matrix, according to certain rules, each four-number group is processed and an initial key is generated. There are four groups, and the initial keys obtained are denoted as  $z_1, z_2, z_3, z_4$ . The specific processing methods and schematics are shown in Fig. 5.

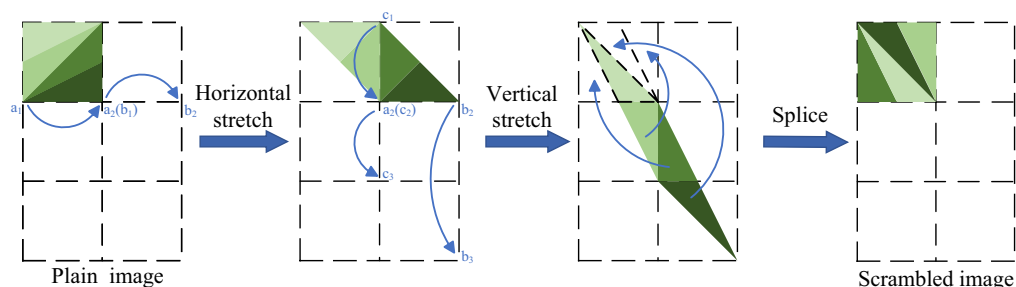
#### Step 3: Key perturbation and chaotic initialization generation

The initial value of the key is perturbed using Eq. (6) and ensures that its range falls between  $[0,1]$  as the initial parameter of the chaotic system.

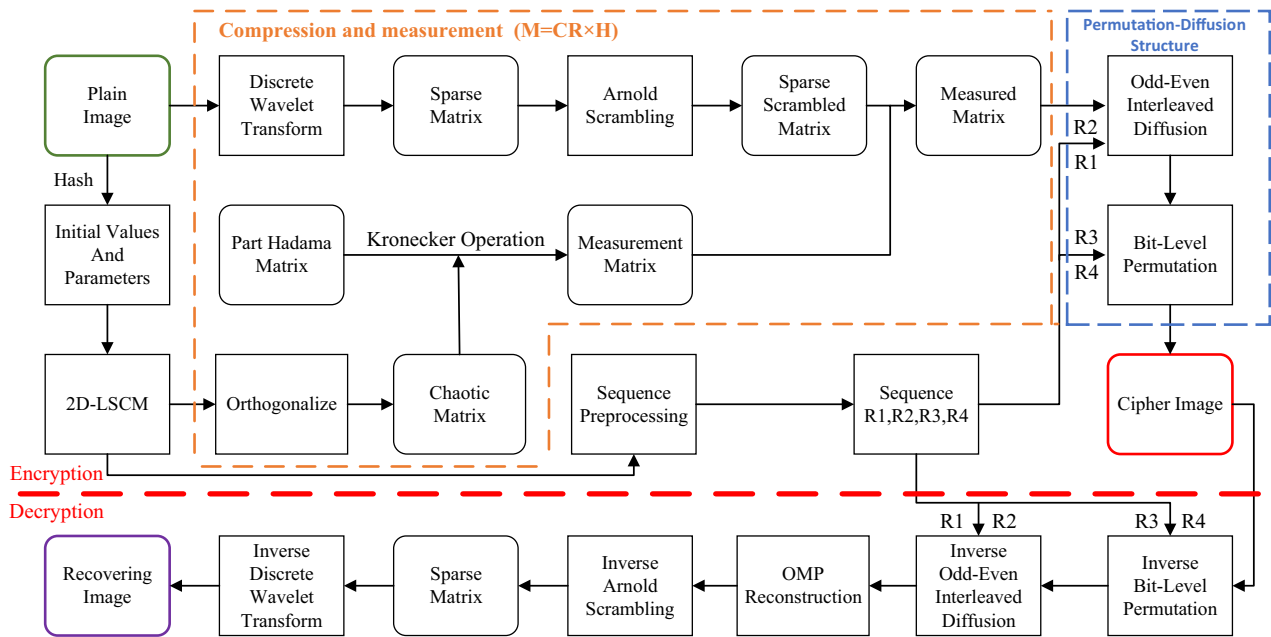
$$key_i = \frac{z_i}{10^{len_{z_i}}} \quad (6)$$

where  $key_i$  denotes the initial values of chaotic system,  $len_{z_i}$  denotes the length of  $z_i$ ,  $i = \{1, 2, 3, 4\}$ .

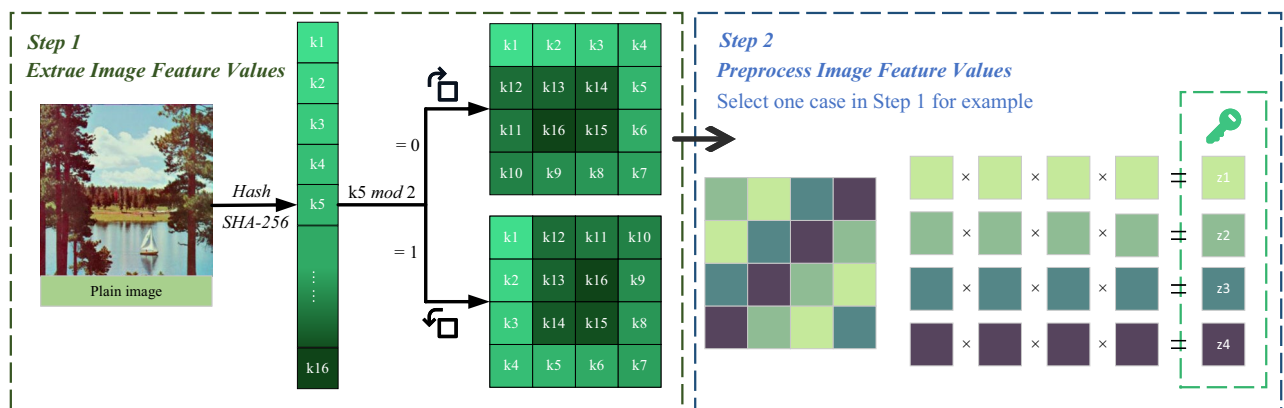
#### Step 4: The preprocessing of the chaotic sequences



**Figure 3.** The geometric interpretation of Arnold Map.



**Figure 4.** The overall schematic of the encryption and decryption scheme.



**Figure 5.** Schematic diagram of image feature values extraction and preprocessing.

By selecting any two combinations from  $key_1, key_2, key_3$  and  $key_4$ , there are  $C_4^2 = 6$  different possible combinations. Choosing any four of these combinations and substituting them into the 2D-LSCM chaotic system for iteration, while discarding the initial 1000 values, results in four distinct pseudorandom sequences denoted as  $R_1, R_2, R_3, R_4$  respectively. The sequences  $R_1$  and  $R_2$  are used for odd-even interleaved diffusion.  $R_3$  and  $R_4$  are used to generate chaotic sort indexes for row-column permutation. The specific processing methods are as follows:

$$\begin{cases} R_1 = \text{abs}(R_1 \times 10^{15}) \bmod 256 \\ R_2 = \text{abs}(R_2 \times 10^{15}) \bmod 256 \\ R_3 = \text{abs}(R_3 \times 10^{15}) \bmod 1 \\ R_4 = \text{abs}(R_4 \times 10^{15}) \bmod 1 \end{cases} \quad (7)$$

where  $a \bmod b$  denotes the remainder of  $a$  over  $b$ ,  $\bmod 1$  denotes that only take valid numbers after the decimal point.

#### Generation of measurement matrix

In the compressive sensing based image encryption scheme, the measurement matrix is also transmitted to the receiver as one of the keys. To reduce the storage burden and transmission bandwidth required during transmission, this scheme uses Kronecker product operations to construct the measurement matrix. If two matrices of sizes  $q \times p$  and  $u \times v$  are both linearly independent low-dimensional orthogonal matrices, a linearly independent high-dimensional orthogonal matrix of size  $uq \times pv$  can be obtained through the Kronecker product. The specific construction process is as follows:

**Step 1:** Arbitrarily select a set of keys and substitute them into the 2D-LSCM for  $4 \times 4 \times n + 1000$  iterations, and discard the first 1000 values to obtain two sequences  $X$  and  $Y$  of length  $4 \times 4 \times n$ , where  $n$  is the sampling interval.

**Step 2:** Disturb sequence  $X$  and sequence  $Y$  to obtain a new sequence  $Z$ , as follows:

$$Z_i = \frac{M \times X_i + W \times Y_i}{2 \times (M + W)} \quad (8)$$

where  $i = [1, 2, 3, \dots, 4 \times 4 \times n]$ ,  $M$  denotes the height of the compressed image,  $W$  denotes the width of the compressed image.

**Step 3:** Arrange and reconstruct the obtained sequences in the following way:

$$A = \text{orth} \left( \sqrt{\frac{2}{M}} \times \begin{pmatrix} Z_{1+0 \times n} & Z_{1+4 \times n} & Z_{1+8 \times n} & Z_{1+12 \times n} \\ Z_{1+1 \times n} & Z_{1+5 \times n} & Z_{1+9 \times n} & Z_{1+13 \times n} \\ Z_{1+2 \times n} & Z_{1+6 \times n} & Z_{1+10 \times n} & Z_{1+14 \times n} \\ Z_{1+3 \times n} & Z_{1+7 \times n} & Z_{1+11 \times n} & Z_{1+15 \times n} \end{pmatrix} \right) \quad (9)$$

where  $\text{orth}(\bullet)$  denotes orthogonalization. The pseudo-code for the orthogonalization function is given in algorithm 1.

**Input:**  $A, tol$

**Output:**  $Q$

- 1:  $[Q, s] = \text{svd}(A, 'econ')$ ; // Decompose  $A$  using svd, obtain the left singular vector matrix  $Q$  and the singular value vector  $s$
- 2:  $s = \text{diag}(s)$ ; // Extracting singular values from a singular value matrix
- 3: **if**  $\text{nargin} == 1$  **then**
- 4:    $tol = \max(\text{size}(A)) * \text{eps}(\text{norm}(s, \text{inf}))$ ;
- 5: **end if**
- 6:  $r = \text{sum}(s > tol)$ ; // Truncate the singular values according to the set  $tol$  and truncate the corresponding column vectors
- 7:  $Q(:, r+1 : \text{end}) = []$ ;

#### Algorithm 1. Orth.

**Step 4:** Perform Kronecker product operation on matrix  $A \in \mathbb{R}^{4 \times 4}$  and Part Hadama Matrix  $B \in \mathbb{R}^{\frac{M}{4} \times \frac{W}{4}}$  to obtain the measurement matrix  $\Phi \in \mathbb{R}^{M \times W}$ .

$$\Phi = A \otimes B = \begin{pmatrix} B_{11}A & B_{12}A & \cdots & B_{1\frac{W}{4}}A \\ B_{21}A & B_{22}A & \cdots & B_{2\frac{W}{4}}A \\ \vdots & \vdots & \ddots & \vdots \\ B_{\frac{M}{4}1}A & B_{\frac{M}{4}2}A & \cdots & B_{\frac{M}{4}\frac{W}{4}}A \end{pmatrix} \quad (10)$$

The high-dimensional measurement matrix constructed through Kronecker product still maintains the non-correlation and orthogonality properties of the original matrices, which has been confirmed as an equivalent condition for *RIP*. To ensure the quality of reconstruction, the measurement matrix, such as Gaussian matrix, will be all sent to the decrypting party as a key under the traditional scheme, compared with the measurement matrix constructed by the method in this paper, the size of the matrix that needs to be transmitted additionally is only 6.25% of the traditional one.

#### Encryption step

This paper uses a grayscale image as an example to illustrate the encryption process. For colour images, the encryption can be performed separately on the  $R, G, B$  channels. Assuming the input is an original image  $P$  with size  $H \times W$ , the specific compression measurement and encryption process are as follows:

**Step 1:** Sparsify the original image.

Using the Discrete Wavelet Transform, the original image is sparsely represented in the wavelet domain from the spatial domain, and obtain a sparse image of size  $H \times W$ . Additionally, in order to enhance the sparse characteristics, the pixel values in the sparse image are set to 0 if they are smaller than the threshold value.

**Step 2:** Scramble the sparse image.

In order to enhance the compression-aware reconstruction effect, this paper adopts Arnold scrambling to reduce the correlation between neighbouring pixels of the sparse image, and obtains the scrambled sparse image  $P'_{DWT}$ . Let the parameter  $a = b = 1$  in Eq. (11), then the scrambling process can be described as follows:

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} \bmod H \quad (11)$$

**Step 3:** Compression measurement.

Substitute the measurement matrix  $\Phi$  generated in Section "Generation of measurement matrix" and  $P'_{DWT}$  into Eq. (2) to obtain the measured matrix  $Y$  of size  $M \times N$ .

**Step 4:** Normalization.



Using the maximum value  $Y_{max}$  and minimum values  $Y_{min}$  of the pixels in the measurement result matrix, map the pixel values to the  $[0, 255]$  interval to obtain an intermediate image  $C_1$  in digital image format.

$$C_1 = \text{round}\left(255 \times \frac{Y - Y_{min}}{Y_{max} - Y_{min}}\right) \quad (12)$$

Step 5: Odd-even interleaved diffusion.

- (1) Construct two matrices containing only the odd pixel point locations and even pixel point locations in image  $C_1$ , respectively<sup>47</sup>.

$$\begin{cases} Q_1(a) = C_1(2a - 1) \\ Q_2(a) = C_1(2a) \end{cases} \quad (13)$$

where  $a \in \{1, 2, 3, \dots, M \times W/2\}$ .

- (2) Diffusion matrix  $C_{21}$  calculated from Eqs. (14) and (15).

$$C_{21}(1) = Q_1(1) \oplus C_{21}(M \times W/2) \oplus R_1(1) \quad (14)$$

$$\begin{cases} C_{21}(a) = Q_1(a) \oplus C_{21}(a - 1) \oplus R_1(a), & a \text{ is an odd number} \\ C_{21}(a) = Q_2(a) \oplus C_{21}(a - 1) \oplus R_1(a), & a \text{ is an even number} \end{cases} \quad (15)$$

- (3) Diffusion matrix  $C_{22}$  calculated from Eqs. (16) and (17).

$$C_{22}(1) = Q_2(1) \oplus C_{22}(M \times W/2) \oplus R_2(1) \quad (16)$$

$$\begin{cases} C_{22}(b) = Q_2(b) \oplus C_{22}(b - 1) \oplus R_2(b), & b \text{ is an odd number} \\ C_{22}(b) = Q_1(b) \oplus C_{22}(b - 1) \oplus R_2(b), & b \text{ is an even number} \end{cases} \quad (17)$$

where  $b \in \{1, 2, 3, \dots, M \times W/2\}$ .

Step 6: Bit-level row and column permutation.

Generate the corresponding sort indexes  $index_3$  and  $index_4$  according to the chaotic sequences  $R_3$  and  $R_4$ . Convert each pixel point in the diffused image  $C_2$  to an 8-bit binary number, newly named  $C_{2\_BIT}$  and perform the row-column permutation operation on  $C_{2\_BIT}$  as follows:

$$C_{3\_BIT}(i, j) = C_{2\_BIT}(index_3(i), index_4(j)) \quad (18)$$

where  $i = [1, 2, 3, \dots, M \times 8]$  and  $j = [1, 2, 3, \dots, W \times 8]$ .

Finally, the binary image  $C_{3\_BIT}$  is converted to decimal format to obtain the final ciphertext image  $C$ .

### Decryption step

Image decryption is the inverse process of encryption. Taking the cipher image  $C$  as input, the decryption process is briefly described as follows:

Step 1: Decryption of row and column permutation.

The same method to get the index sequence  $index_3$  and  $index_4$ , then convert the cipher image  $C$  to binary format  $C_{3\_BIT}$ . The decryption process of row-column permutation is as follows:

$$C_{2\_BIT}(index_3(i), index_4(j)) = C_{3\_BIT}(i, j) \quad (19)$$

Step 2: Decryption of odd-even interleaved diffusion.

Similar to the encryption process, sequences  $R_1$  and  $R_2$  are obtained using Eq. (7). After converting the inverse permuted image  $C_{2\_BIT}$  to decimal format image  $C_2$ , decryption is performed through odd-even interleaved diffusion using the following formula:

$$\begin{cases} Q_1(a) = C_{21}(a) \oplus C_{21}(a - 1) \oplus R_1(a), & a \text{ is an odd number} \\ Q_2(a) = C_{21}(a) \oplus C_{21}(a - 1) \oplus R_1(a), & a \text{ is an even number} \end{cases} \quad (20)$$

$$\begin{cases} Q_2(b) = C_{22}(b) \oplus C_{22}(b - 1) \oplus R_2(b), & b \text{ is an odd number} \\ Q_1(b) = C_{22}(b) \oplus C_{22}(b - 1) \oplus R_2(b), & b \text{ is an even number} \end{cases} \quad (21)$$

$$\begin{cases} Q_1(1) = C_{21}(1) \oplus Q_1(M \times H/2) \oplus R_1(1) \\ Q_2(1) = C_{22}(1) \oplus Q_2(M \times H/2) \oplus R_2(1) \end{cases} \quad (22)$$

Step 3: Inverse normalization.

The inverse normalization operation is performed on the matrix  $C_2$  to obtain the matrix  $C_1$ . The formula for this process is as follows:

$$C_1 = \frac{C_2 \times (Y_{max} - Y_{min})}{255} + Y_{min} \quad (23)$$

**Step 4:** OMP reconstruction.

Using the measurement matrix generated in Section "Generation of measurement matrix", we can reconstruct the sparsely scrambled image  $P_{DWT}$  from the matrix  $C_1$  using the OMP algorithm. This process can be represented as follows and the pseudo-code is given in algorithm 2:

$$P_{DWT} = omp(C_1, \Phi, H) \quad (24)$$

---

**Input:**  $C_1, \Phi, H$

**Output:**  $P_{DWT}$

```

1:  $n = \text{length}(C_1)$ ;
2:  $s = \text{floor}(n/4)$ ;
3:  $P_{DWT} = \text{zeros}(1, H)$ ;
4:  $Aug_t = []$ ;
5:  $r_n = C_1$ ;
6: for  $times = 1 : s$  do
7:    $product = \text{abs}(\Phi' * r_n)$ ;
8:    $[val, pos] = \text{max}(product)$ ;
9:    $Aug_t = [Aug_t, \Phi(:, pos)]$ ;
10:   $\Phi(:, pos) = \text{zeros}(n, 1)$ ;
11:   $Vaug_x = (Aug_t' * Aug_t)^{-1} * Aug_t' * C_1$ ;
12:   $r_n = C_1 - Aug_t * Vaug_x$ ;
13:   $pos\_array(times) = pos$ ;
14: end for
15:  $P_{DWT}(pos\_array) = Aug_x$ ;

```

---

**Algorithm 2.** OMP reconstruction.

**Step 5:** Decryption of Arnold scrambling and inverse DWT.

Based on the definition of Arnold scrambling in Eq. (5), the reverse operation process can be deduced, allowing the recovery of the sparsely scrambled image  $P_{DWT}$ . Finally, applying the inverse Discrete Wavelet Transform operation to the sparse image results in the reconstruction of the image  $P$  of size  $H \times W$ .

$$P = iDWT(P_{DWT}) \quad (25)$$

## Simulation results and performance analysis

### Experimental environment

We employed an 11th Gen Intel(R) Core(TM) i5-11400H CPU in a mainframe PC with MATLAB R2022a experimental software loaded as the experimental platform. A selection of experimental images was made from the USC-SIPI repository<sup>48</sup>.

### Statistical analytics

#### Histogram analysis

The histogram can visualize the distribution of all pixels in the image, and for the given plain image Fig. 6a and the corresponding cipher image Fig. 6c, their 2D histograms are shown in Fig. 6b and d, respectively. Additionally, the 3D histogram corresponding to Fig. 7a is given in Fig. 7b–d, which show that the plaintext image presents a certain statistical regularity, whereas the statistical properties of the encrypted histogram of the image present a noise-like distribution, which well hides the grey-value information of the image, and thus improves the ability of resisting the attack of statistical analysis.

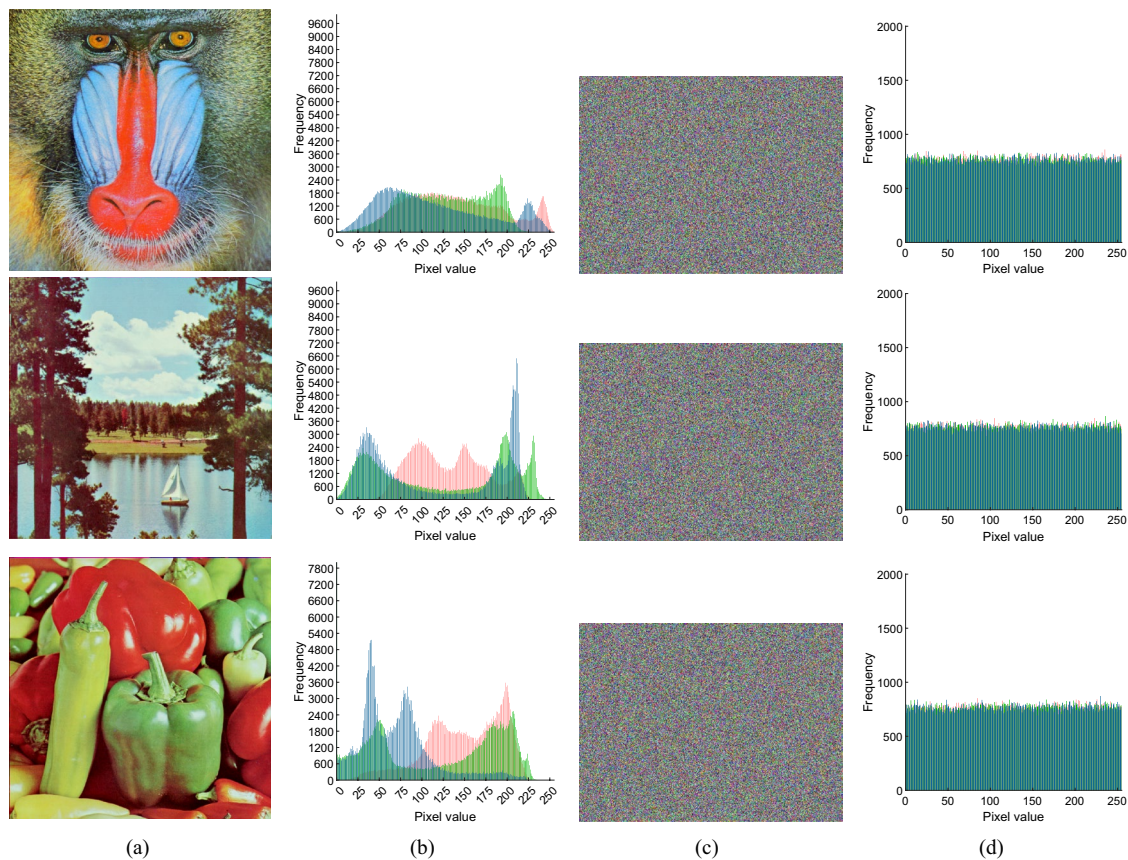
#### Adjacent pixel correlation analysis

For plaintext picture pixels, neighboring pixel correlation is typically a notable feature, and the ciphertext through the encryption algorithm will make the adjacent pixels not associated with any pixels. This algorithm aims to generate ciphertext, in which the correlation between adjacent pixels can be ignored. The correlation coefficient calculation formula is as follows:

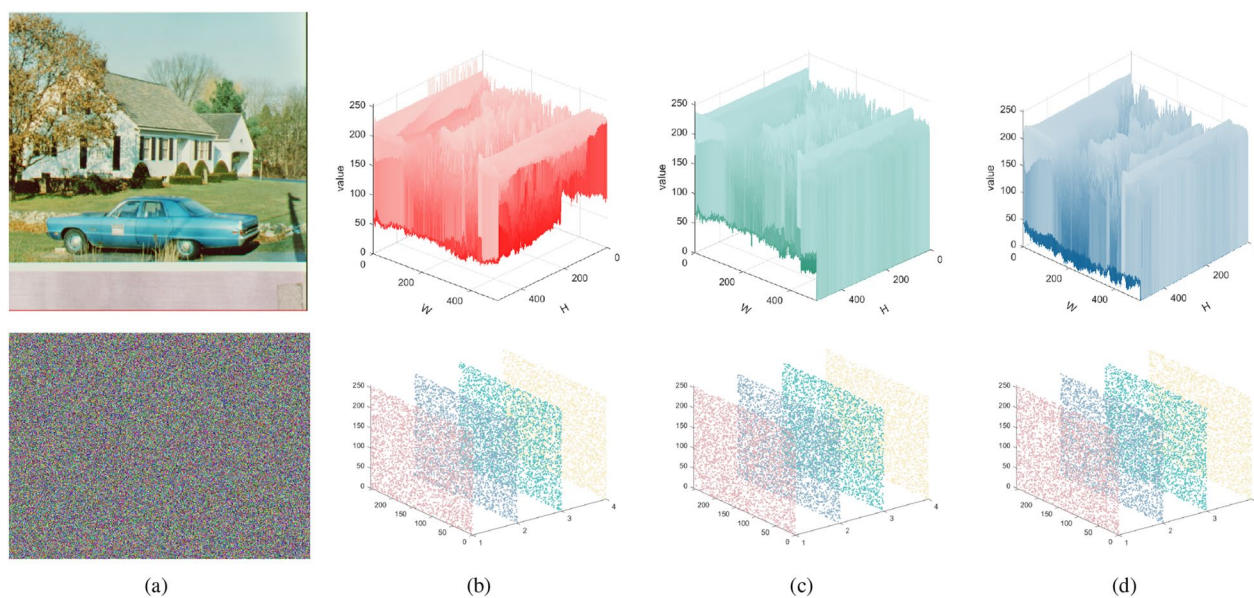
$$r_{xy} = \frac{\sum_{i=1}^M (x_i - \frac{1}{M} \sum_{j=1}^M x_j)(y_i - \frac{1}{M} \sum_{j=1}^M y_j)}{\sqrt{\sum_{i=1}^M (x_i - \frac{1}{M} \sum_{j=1}^M x_j)^2} \sqrt{\sum_{i=1}^M (y_i - \frac{1}{M} \sum_{j=1}^M y_j)^2}} \quad (26)$$

where  $x_i$  and  $y_i$  make up the first pair of adjacent pixels that are horizontal, vertical, diagonal, or anti-angle.  $M$  is the total number of pixels. In order to visualize the correlation between adjacent pixels in plaintext and ciphertext, we calculate and compare the difference between the two, as shown in Fig. 8. It appears that the plaintext pixels have a significant degree of association, but the ciphertext pixels show almost no correlation at all. This finding demonstrates how robust the method is against statistical attacks.

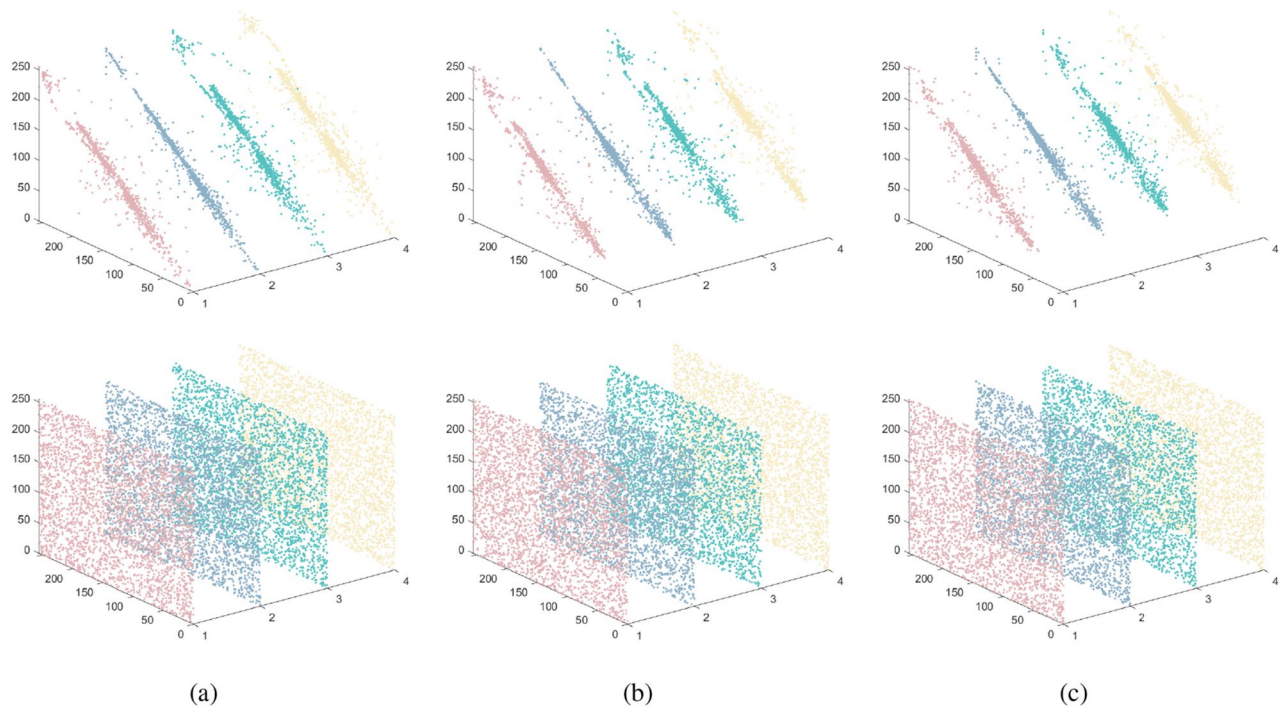




**Figure 6.** Images before and after encryption: (a) Original image; (b) Histogram of original image; (c) Encrypted image at CR=0.75; (d) Histogram of encrypted image.



**Figure 7.** 3D visualization of the encrypted image simulation shown: (a) plaintext image and ciphertext image; (b) red channel; (c) green channel; (d) blue channel.



**Figure 8.** Horizontal, vertical, diagonal and antidiagonal correlation test results: (a) R-channel; (b) G-channel; (c) B-channel.

*Differential statistical analysis*

The difference between the two images can be quantified using two criteria: The Unified Average Changed Intensity (UACI) and the Number of Pixels Change Rate (NPCR) are the measures of interest. In differential attacks, attackers often make slight changes to the plaintext image, using a specific algorithm to encrypt it before and after the adjustments, aiming to reveal their relationship. The explanation of UACI and NPCR is as follows:

$$\begin{cases} NPCR = \frac{1}{H \times W} \times \sum_{i=1}^H \sum_{j=1}^W D(i,j) \times 100\% \\ UACI = \frac{1}{H \times W} \times \sum_{i=1}^H \sum_{j=1}^W \frac{|v_1(i,j) - v_2(i,j)|}{255} \times 100\% \end{cases} \tag{27}$$

where  $v_1, v_2$  respectively for plaintext image change a pixel before and after the ciphertext image.  $D$  has the following definition:

$$D = \begin{cases} 0, & v_1(i,j) = v_2(i,j) \\ 1, & v_1(i,j) \neq v_2(i,j) \end{cases} \tag{28}$$

Table 1 presents the NPCR and UACI values of various picture sizes that have been encrypted using the algorithm. These outcomes demonstrate the algorithm’s strong encryption capabilities.

Pictures	Description	Size	Type	NPCR(%)		UACI(%)	
				Ours	LICM-IEA <sup>49</sup>	Ours	LICM-IEA <sup>49</sup>
5.1.09	Moon surface	256	Gray	99.6412	99.6126	33.4232	33.4029
5.1.10	Aerial	256	Gray	99.5988	99.6184	33.4122	33.3627
4.1.01	Female	256	Color	99.5941	99.6027	33.5322	33.4625
4.1.02	Couple	256	Color	99.6123	99.6238	33.3684	33.4221
7.1.01	Truck	512	Gray	99.5689	99.5991	33.4012	33.3977
7.1.02	Airplane	512	Gray	99.6211	99.5899	33.4972	33.3386
2.1.09	San Diego(Point Loma)	512	Color	99.6321	99.6381	33.3979	33.4123
2.1.10	San Diego(Shelter Island)	512	Color	99.6411	99.6128	33.4265	33.4235
7.2.01	Airplane(U-2)	1024	Gray	99.6040	99.6352	33.4188	33.4266
2.1.10	San Francisco(Bay Bridge)	1024	Color	99.6132	99.5901	33.3979	33.4115

**Table 1.** The value of NPCR and UACI.

Entropy of information

In order to assess the distribution of gray values in images and measure the degree of unpredictability in picture data, information entropy is essential. This is its definition:

$$H(x) = - \sum_{i=1}^L P(x_i) \log_2 P(x_i) \tag{29}$$

where  $x$  denotes the pixel value and  $p(n_x)$  denotes the probability of the symbol. Taking the pixel value of 8 bits as an example, the theoretical value is 8. It can be seen from Table 2 that the experimental results are very close to 8, indicating that the algorithm has good information entropy characteristics.

Recovery image quality analysis

The mean square error (MSE) of the encrypted image’s plaintext and ciphertext, as well as its db expression (PSNR) in signal processing, are used in this experiment. The expression is as follows:

$$PSNR = 10 \times \log_{10} \left( \frac{Q^2}{(1/HW) \sum_{i=1}^H \sum_{j=1}^W [X(i,j) - Y(i,j)]^2} \right) \tag{30}$$

where  $Q$  represents the pixel level of the image.

For digital images, the PSNR value higher than 40 dB indicates that the image quality is good. Table 3 displays the testing results and Table 4 demonstrates the comparison results of the proposed algorithm with other advanced algorithms, both of which prove the high recovery quality of the algorithm.

Pictures	Description	Size	Type	Plain image	Cipher image	LICM-IEA <sup>49</sup>
4.1.03	Female(from Bell Labs)	256	Color	5.9709	7.9986	7.9998
4.1.05	House	256	Color	7.0686	7.9988	7.9986
4.2.05	Airplane(F-16)	512	Color	6.6639	7.9997	7.9985
4.2.06	Sailboat on lake	512	Color	7.7622	7.9997	7.9981
2.2.07	Oakland	1024	Color	6.4492	7.9999	7.9989
2.2.12	San Francisco and Oakland	1024	Color	6.9619	7.9999	7.9992

Table 2. Plaintext and ciphertext information entropy of different images.

Pictures	Description	Size	Type	PSNR(dB)
5.1.09	Moon surface	256	Gray	39.4465
5.1.11	Airplane	256	Gray	42.9522
4.1.03	Female(from Bell Labs)	256	Color	44.0599
4.1.05	House	256	Color	42.4047
4.2.05	Aerial	512	Gray	38.0820
4.2.05	Airplane(F-16)	512	Color	41.4172
4.2.06	Sailboat on lake	512	Color	41.4166
2.2.07	Oakland	1024	Color	40.3476
2.2.12	San Francisco and Oakland	1024	Color	39.3316

Table 3. Image recovery quality analysis of different images under CR=0.5.

Algorithms	Compression ratio		
	0.25	0.5	0.75
Ours	32.7133	39.5172	42.3821
<sup>50</sup>	–	23.3608	34.7149
<sup>51</sup>	32.3566	36.1892	37.4529
<sup>52</sup>	30.1022	36.8294	41.2933

Table 4. Comparison results on PSNR between the recovered image and plain image.

### Impact of different key parameters on recovery quality

In the image encryption algorithm based on compressive sensing, there are several key parameters that affect its reconstruction quality, such as compression rate, reconstruction algorithm, sparse representation method, etc. In this section we aim to show the impact of different reconstruction algorithms and three commonly used sparse representation methods on the recovery quality. The test image is a picture of jelly beans taken at USC. of size  $256 \times 256$ . The specific two sections are as follows.

#### Impact of reconstruction algorithms on recovery quality

First, we analyze the impact of reconstruction algorithms on restored image quality under different compression rates. It can be seen from the Fig. 9 that both the OMP algorithm and the IRLS algorithm have good performance in reconstructing the measurement image. When the compression rate is only 0.125, the PSNR value of both has reached more than 30dB, and when the compression rate is 0.5, both PSNRs reach 40dB. This shows that the size of the secret image transmitted to the receiver through the channel only needs to be half that of the ordinary algorithm, and the recovered image obtained by decryption has a very excellent recovery effect and looks the same as the original image to the naked eye.

#### Impact of different sparse representations on recovery quality

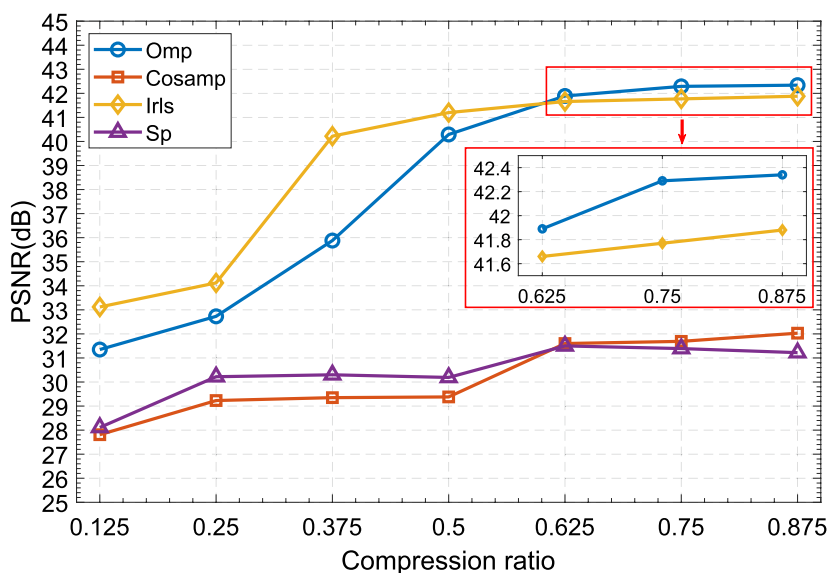
The results in Section "Impact of reconstruction algorithms on recovery quality" show that the OMP and IRLS algorithms have outstanding contributions to image reconstruction, so in this section we choose these two as reconstruction algorithms to analyze three common sparse representation methods: Discrete Wavelet Transform, Integer Wavelet Transform and the effect of Discrete Cosine Transform on the quality of restored images. The test results are shown in Fig. 10. At the same time, Fig. 11 shows the restored images under the combination of different sparse representation methods and different reconstruction algorithms when the compression rate is 0.5. The experimental results show that the three sparse representation methods all have good restoration performance effects. The choice of sparse method has little impact on reconstruction, but in comparison, it is not difficult to see that Discrete Wavelet Transform has better numerical statistical results and visual performance effects. Therefore, it is reasonable to choose Discrete Wavelet Transform as the sparse representation method in this scheme. Table 5 show the recovered images of the proposed algorithm at different compression ratios.

### Key space

The 2D-LSCM chaotic system used in this algorithm has a key space of  $\{n, m, z, SHA - 256\}$ , where the accuracy of  $n, m, z$  is  $10^{-16}$ , and  $SHA - 256$  is a hash of 256 bits. It can be obtained that the key space of this algorithm is about  $10^{3 \times 16} \times 2^{256} \approx 2^{415}$ , and the key length reaches 415 bits. Compared with other literature, as shown in Table 6, this algorithm can resist any form of violent attack.

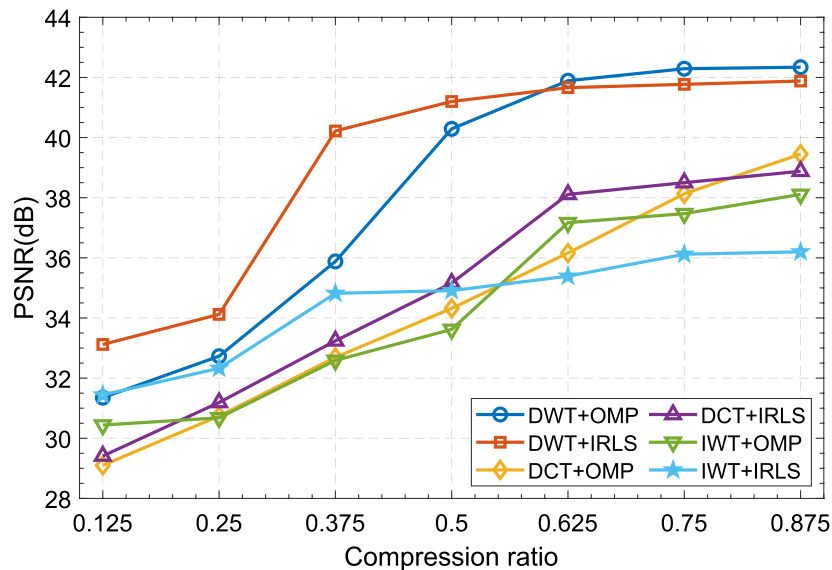
#### Key sensitivity analysis

Analyzing the ciphertext generated by encrypting the same picture with two slightly different keys is known as key sensitivity. This section will contrast the encryption using the proper key with the use of a slightly different key (add  $10^{-12}$ ,  $10^{-13}$ ,  $10^{-14}$  and  $10^{-15}$ ). The results of the analysis are shown in Fig. 12. We find that the average values of UACI and NPCR are 33.456% and 99.6105%, respectively, after adding perturbations to the key. This implies that there is a significant difference between the two cipher pictures.

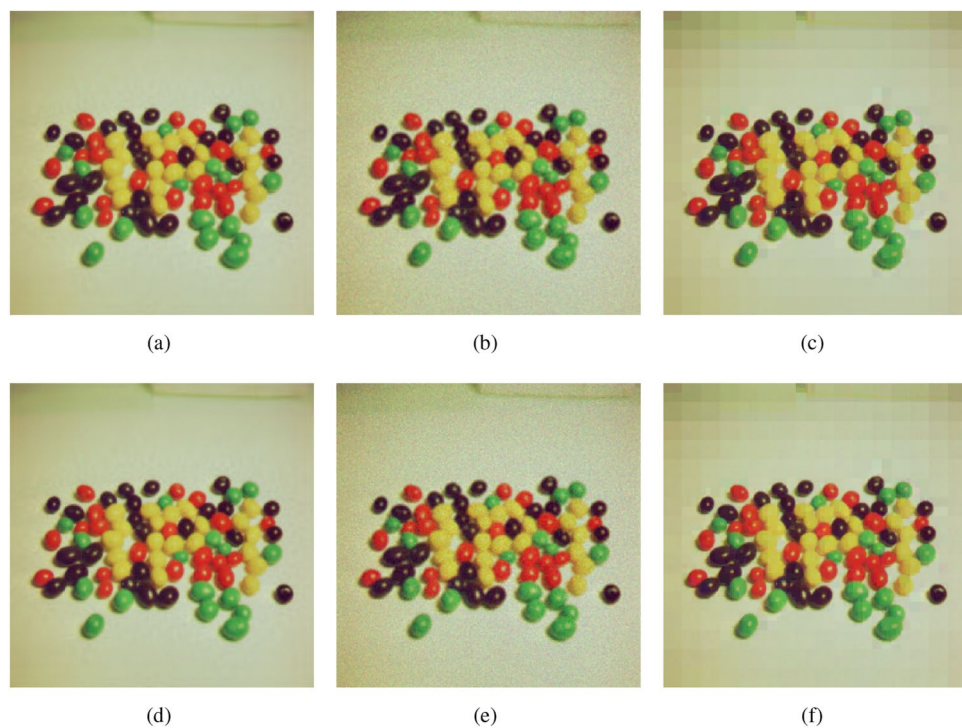


**Figure 9.** PSNR of recovered images with different reconstruction algorithms.





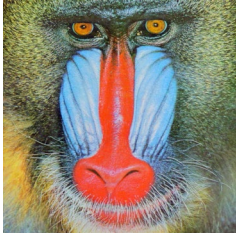

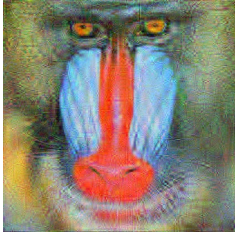

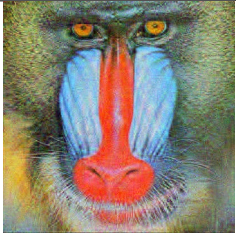

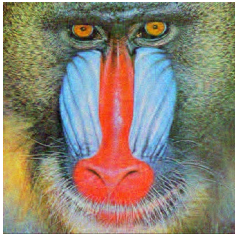

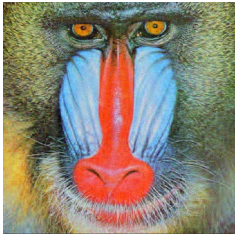


**Figure 10.** PSNR of recovered images with different sparse representations in combination with different reconstruction algorithms.



**Figure 11.** Reconstructed images under different sparse representations at CR = 0.5: (a) DWT+OMP; (b) DCT+OMP; (c) IWT+OMP; (d) DWT+IRLS; (e) DCT+IRLS; (f) IWT+IRLS.

#### Analysis of explicit sensitivities

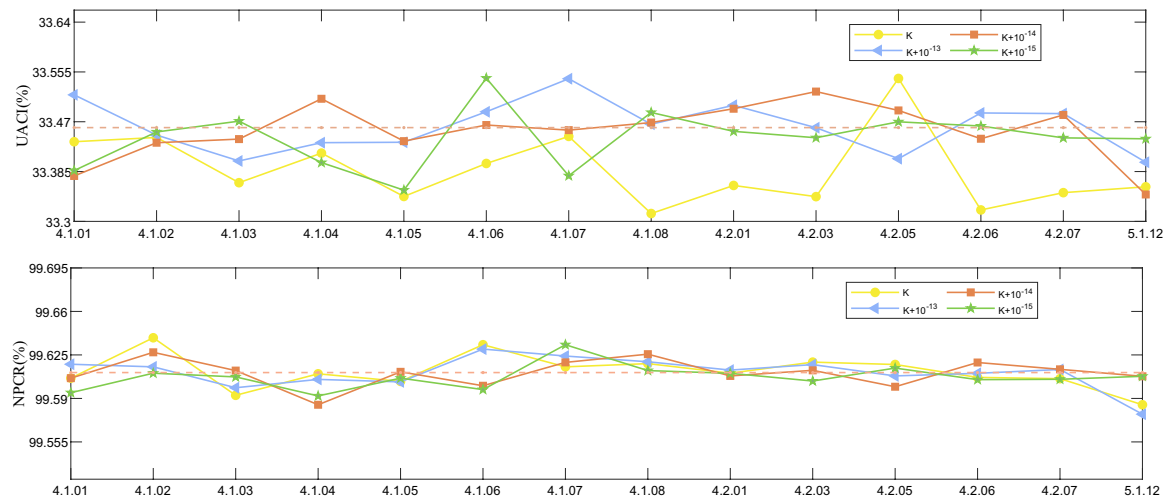
This section will examine how sensitive the method is to plaintext changes by setting the value of a single pixel in a common picture to 1. The pixel values at  $(H/3, W/3)$ ,  $(2 \times H/3, W/3)$ ,  $(H/3, 2 \times W/3)$  and  $(2 \times H/3, 2 \times W/3)$  are added with 1 for comparing the size of the difference. The analysis results are presented in the accompanying Fig. 13. As can be seen from the graph, NPCR and UACI are close to the ideal values of 99.62% and 33.41%, respectively. This shows that the proposed algorithm is sufficient to resist plaintext attacks.

Plain image	CR	Cipher image	Decrypted image
	0.125		
	0.25		
	0.375		
	0.5		
	0.75		

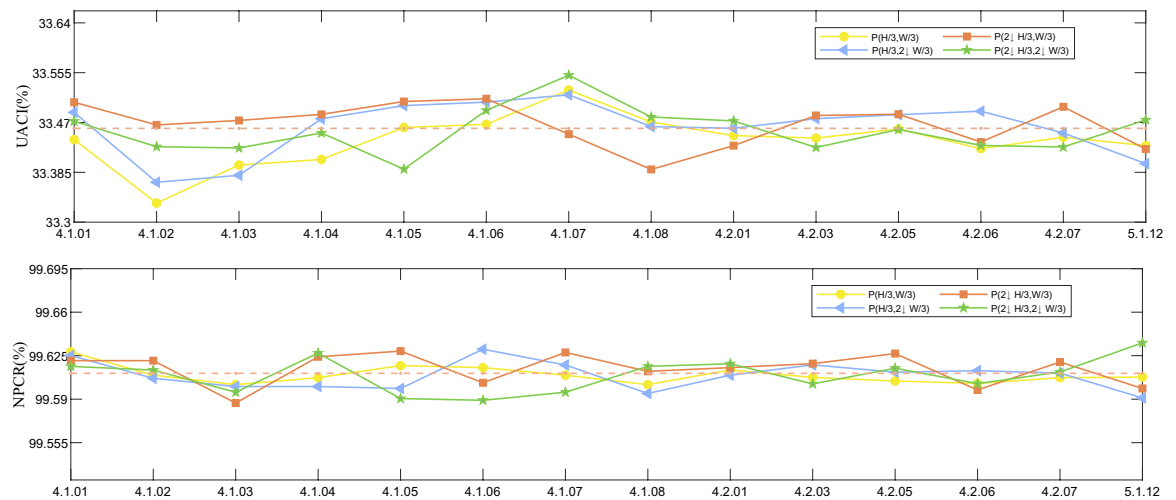
**Table 5.** Recovery quality of proposed algorithm at different CR.

Papers	Key space value
Proposed method	287
<a href="#">53</a>	154
<a href="#">54</a>	166
<a href="#">18</a>	224
<a href="#">20</a>	234

**Table 6.** Key space.



**Figure 12.** Key sensitivity test results.



**Figure 13.** Plaintext sensitivity test results.

## Conclusion

This paper proposes a compressive sensing image encryption scheme based on optimized orthogonal measurement matrix. The algorithm employs discrete wavelet transform for a sparse representation of the image, and through Arnold scrambling, effectively reduces the correlation between adjacent pixels. After compressive sensing measurement, the odd-even interleaved diffusion and bit-level row and column permutation are performed respectively. The experimental results show that the PSNR of the restored image under the conventional compression size is above 40 dB, which indicates that this scheme has higher recovery performance than other advanced compressive sensing algorithms. Additionally, the scheme incorporates a plaintext correlation mechanism, demonstrating strong robustness against various cryptanalysis methods such as chosen plaintext attacks and differential attacks. This feature enables the scheme to effectively withstand different approaches to cryptographic analysis. A comprehensive analysis indicates that the method proposed in this paper is considered effective in enhancing the accuracy and reliability of information exchange, particularly in the context of the big data era, where it holds significant implications for image encryption.

Despite the progress made, there are still some limitations. During the experiments, we observed that for images with a compression ratio lower than 0.25, particularly those with low adjacent pixel correlation, manual adjustment of specific parameters was necessary to achieve satisfactory reconstruction results. Since parameter selection is closely tied to the image type, this process could significantly increase the cost of practical applications. In future work, we plan to conduct a thorough comparative analysis of the performance of algorithms in image reconstruction, such as coded compression and block compressive sensing. We will explore whether techniques like edge detection could be used to assess pixel correlation, automatically identify image types, and accordingly adapt the encryption parameters to ensure optimal image recovery. Moreover, the encryption framework will be further refined, enhancing both the algorithm's security and efficiency.



## Data availability

The datasets used and analysed during the current study available from the corresponding author on reasonable request. All data generated or analysed during this study are included in this published article.

Received: 18 January 2024; Accepted: 9 April 2024

Published online: 16 April 2024

## References

- Ding, Y., Liu, W., Wang, H. & Sun, K. A new class of discrete modular memristors and application in chaotic systems. *Eur. Phys. J. Plus* **138**, 638 (2023).
- Liu, X., Sun, K., Wang, H. & He, S. A class of novel discrete memristive chaotic map. *Chaos Solitons Fractals* **174**, 113791 (2023).
- Gao, Z. *et al.* Experimental demonstration of synchronous privacy enhanced chaotic temporal phase en/decryption for high speed secure optical communication. *Opt. Express* **30**, 31209 (2022).
- Huang, X., Dong, Y., Ye, G. & Shi, Y. Meaningful image encryption algorithm based on compressive sensing and integer wavelet transform. *Front. Comput. Sci.* **17**, 173804 (2022).
- Yuan, X. & Cai, Z. Ichv: A new compression approach for industrial images. *IEEE Trans. Ind. Inform.* **18**, 4427–4435 (2022).
- Erkan, U., Toktas, A. & Lai, Q. 2d hyperchaotic system based on Schaffer function for image encryption. *Expert Syst. Appl.* **213**, 119076 (2023).
- Zou, C., Wang, X., Zhou, C., Xu, S. & Huang, C. A novel image encryption algorithm based on DNA strand exchange and diffusion. *Appl. Math. Comput.* **430**, 127291 (2022).
- Feng, W., Qin, Z., Zhang, J. & Ahmad, M. Cryptanalysis and improvement of the image encryption scheme based on Feistel network and dynamic DNA encoding. *IEEE Access* **9**, 145459–145470 (2021).
- Lu, D., Li, M., Liao, Y., Tao, G. & Cai, H. Verifiable privacy-preserving queries on multi-source dynamic DNA datasets. *IEEE Trans. Cloud Comput.* **11**, 1927–1939 (2023).
- Teng, L., Wang, X., Yang, F. & Xian, Y. Color image encryption based on cross 2d hyperchaotic map using combined cycle shift scrambling and selecting diffusion. *Nonlinear Dyn.* **105**, 1859–1876 (2021).
- Lai, Q., Hu, G., Erkan, U. & Toktas, A. A novel pixel-split image encryption scheme based on 2d Salomon map. *Expert Syst. Appl.* **213**, 118845 (2023).
- Wu, T. *et al.* Secure turbulence-resistant coherent free-space optical communications via chaotic region-optimized probabilistic constellation shaping. *Opt. Lett.* **48**, 684–687 (2023).
- Ye, X., Zhang, Y., Xiao, X., Yi, S. & Lan, R. Usability enhanced thumbnail-preserving encryption based on data hiding for jpeg images. *IEEE Signal Process. Lett.* **30**, 793–797 (2023).
- Zhou, W., Zhang, Y., Zhao, R., Yi, S. & Lan, R. Adversarial thumbnail-preserving transformation for facial images based on GAN. *IEEE Signal Process. Lett.* **30**, 1147–1151 (2023).
- Ma, Y., Chai, X., Gan, Z. & Zhang, Y. Privacy-preserving TPE-based jpeg image retrieval in cloud-assisted internet of things. *IEEE Internet Things J.* <https://doi.org/10.1109/JIOT.2022.3142933> (2023).
- Wen, H. *et al.* Secure DNA-coding image optical communication using non-degenerate hyperchaos and dynamic secret-key. *Mathematics* **10**, 3180 (2022).
- Chen, X., Mou, J., Cao, Y., Yan, H. & Jahanshahi, H. A chaotic color image encryption scheme based on improved Arnold scrambling and dynamic DNA encoding. *Multimed. Tools Appl.* **82**, 43797–43818 (2023).
- Wen, H., Kang, S., Wu, Z., Lin, Y. & Huang, Y. Dynamic RNA coding color image cipher based on chain feedback structure. *Mathematics* **11**, 3133 (2023).
- Luo, Y., Liang, Y., Zhang, S., Liu, J. & Wang, F. An image encryption scheme based on block compressed sensing and Chen's system. *Nonlinear Dyn.* **111**, 6791–6811 (2022).
- Wen, H., Huang, Y. & Lin, Y. High-quality color image compression-encryption using chaos and block permutation. *J. King Saud Univ. Comput. Inf. Sci.* **35**, 101660 (2023).
- Huang, H. & Cai, Z. Duplex color image encryption system based on 3-d nonequilateral Arnold transform for IIOT. *IEEE Trans. Ind. Inform.* **19**, 8285–8294 (2023).
- Lu, Q., Liao, X., Xiang, T., Li, H. & Huang, T. Privacy masking stochastic subgradient-push algorithm for distributed online optimization. *IEEE Trans. Cybern.* **51**, 3224–3237 (2021).
- Erkan, U., Toktas, A., Memiş, S., Lai, Q. & Hu, G. An image encryption method based on multi-space confusion using hyperchaotic 2d Vincent map derived from optimization benchmark function. *Nonlinear Dyn.* **111**, 20377–204054 (2023).
- Feng, W. *et al.* Image encryption algorithm based on plane-level image filtering and discrete logarithmic transform. *Mathematics* **10**, 2751 (2022).
- Feng, W., Zhang, J. & Qin, Z. A secure and efficient image transmission scheme based on two chaotic maps. *Complexity* **2021**, 1–19 (2021).
- Wen, H. *et al.* Secure optical image communication using double random transformation and memristive chaos. *IEEE Photonics J.* **15**, 1–11 (2023).
- Lai, Q., Yang, L. & Liu, Y. Design and realization of discrete memristive hyperchaotic map with application in image encryption. *Chaos, Solitons Fractals* **165**, 112781 (2022).
- Zhou, S., Qiu, Y., Qi, G. & Zhang, Y. A new conservative chaotic system and its application in image encryption. *Chaos, Solitons Fractals* **175**, 113909 (2023).
- Zhou, S., Wang, X. & Zhang, Y. Novel image encryption scheme based on chaotic signals with finite-precision error. *Inf. Sci.* **621**, 782–798 (2023).
- Liu, W., Sun, K., He, S. & Wang, H. The parallel chaotification map and its application. *IEEE Trans. Circuits Syst. I Regular Pap.* **1–10** (2023).
- Kocak, O., Erkan, U., Toktas, A. & Gao, S. Pso-based image encryption scheme using modular integrated logistic exponential map. *Expert Syst. Appl.* **237**, 121452 (2024).
- Wen, H., Lin, Y., Kang, S., Zhang, X. & Zou, K. Secure image encryption algorithm using chaos-based block permutation and weighted bit planes chain-diffusion. *iScience* **27**, 108610 (2023).
- Toktas, A., Erkan, U., Gao, S. & Pak, C. A robust bit-level image encryption based on Bessel map. *Appl. Math. Comput.* **462**, 128340 (2024).
- Hua, Z., Liu, X., Zheng, Y., Yi, S. & Zhang, Y. Reversible data hiding over encrypted images via preprocessing-free matrix secret sharing. *IEEE Trans. Circuits Syst. Video Technol.* <https://doi.org/10.1109/TCSVT.2023.3270882> (2023).
- Wen, H. & Lin, Y. Cryptanalyzing an image cipher using multiple chaos and DNA operations. *J. King Saud Univ. Comput. Inf. Sci.* **35**, 101612 (2023).
- Luo, Y., Zhang, C., Wang, X., Liang, X. & Qiu, K. Robust key update with controllable accuracy using support vector machine for secure OFDMA-PON. *J. Lightwave Technol.* **41**, 4663–4671 (2023).

37. Liang, X., Zhang, C., Luo, Y., Wang, X. & Qiu, K. Secure encryption and key management for Ofdm-Pon based on chaotic Hilbert motion. *J. Lightwave Technol.* **41**, 1619–1625 (2023).
38. Wen, H. & Lin, Y. Cryptanalysis of an image encryption algorithm using quantum chaotic map and DNA coding. *Expert Syst. Appl.* **237**, 121514 (2024).
39. Wen, H., Lin, Y., Yang, L. & Chen, R. Cryptanalysis of an image encryption scheme using variant Hill cipher and chaos. *Expert Syst. Appl.* <https://doi.org/10.1016/j.eswa.2024.123748> (2024).
40. Chai, X. *et al.* Exploiting semi-tensor product compressed sensing and hybrid cloud for secure medical image transmission. *IEEE Internet Things J.* **10**, 7380–7392 (2023).
41. Ye, G., Liu, M., Yap, W.-S. & Goi, B.-M. Reversible image hiding algorithm based on compressive sensing and deep learning. *Nonlinear Dyn.* **111**, 13535–13560 (2023).
42. Wang, X., Liu, C. & Jiang, D. A novel visually meaningful image encryption algorithm based on parallel compressive sensing and adaptive embedding. *Expert Syst. Appl.* **209**, 118426 (2022).
43. Wang, X. & Su, Y. Image encryption based on compressed sensing and DNA encoding. *Signal Process. Image Commun.* **95**, 116246 (2021).
44. Chen, Z. & Ye, G. An asymmetric image encryption scheme based on hash sha-3, rsa and compressive sensing. *Optik* **267**, 169676 (2022).
45. Liang, J. *et al.* A secure and effective image encryption scheme by combining parallel compressed sensing with secret sharing scheme. *J. Inf. Secur. Appl.* **75**, 103487 (2023).
46. Hua, Z., Jin, F., Xu, B. & Huang, H. 2d logistic-sine-coupling map for image encryption. *Signal Process.* **149**, 148–161 (2018).
47. Wang, X. & Wang, Y. Multiple medical image encryption algorithm based on scrambling of region of interest and diffusion of odd-even interleaved points. *Expert Syst. Appl.* **213**, 118924 (2023).
48. The USC-SIPI image database. <https://sipi.usc.edu/database/>.
49. Cao, C., Sun, K. & Liu, W. A novel bit-level image encryption algorithm based on 2d-LICM hyperchaotic map. *Signal Process.* **143**, 122–133 (2018).
50. Wang, X. Image encryption based on compressed sensing and DNA encoding. *Signal Process. Image Commun.* **95**, 116246 (2021).
51. Chai, X. *et al.* An efficient visually meaningful image compression and encryption scheme based on compressive sensing and dynamic lsb embedding. *Optics Lasers Eng.* **124**, 105837 (2020).
52. Zhang, C. *et al.* Plaintext-related image encryption scheme without additional plaintext based on 2dcs. *Optik* **272**, 170312 (2023).
53. Mansouri, A. & Wang, X. A novel block-based image encryption scheme using a new sine powered chaotic map generator. *Multimed. Tools Appl.* **80**, 21955–21978 (2021).
54. Su, Y., Wang, X., Xu, M., Zou, C. & Liu, H. A three-dimensional (3d) space permutation and diffusion technique for chaotic image encryption using Merkel tree and dna code. *Sens. Imaging* **24**, 5 (2023).

## Acknowledgements

This work was supported 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, and in part by Special Projects for Key Fields of the Education Department of Guangdong Province under Grant 2023ZDZX1041.

## Author contributions

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

## Competing interests

The authors declare no competing interests.

## Additional information

**Correspondence** and requests for materials should be addressed to L.C.

**Reprints and permissions information** is available at [www.nature.com/reprints](http://www.nature.com/reprints).

**Publisher's note** Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.



**Open Access** This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit <http://creativecommons.org/licenses/by/4.0/>.

© The Author(s) 2024