Chaos, Solitons and Fractals 163 (2022) 112584

Contents lists available at ScienceDirect

Chaos, Solitons and Fractals

journal homepage: www.elsevier.com/locate/chaos

High-quality visually secure image cryptosystem using improved Chebyshev map and 2D compressive sensing model☆

Shufeng Huang [a], Donghua Jiang [b], Qianxue Wang [a], Mingwei Guo [a], Linqing Huang [c], Weijun Li [d,*], Shuting Cai [d,*]

[a] School of Automation, Guangdong University of Technology, Guangzhou 510006, China
[b] School of Computer Science and Engineering, Sun Yat-sen University, Guangzhou 511400, China
[c] School of Advanced Manufacturing, Guangdong University of Technology, Guangzhou 510006, China
[d] School of Integrated Circuits, Guangdong University of Technology, Guangzhou 510006, China

ARTICLE INFO

Keywords:
Improved Chebyshev map
Two-dimensional compressive sensing
Image encryption
Visual security
Simulated annealing algorithm

ABSTRACT

In this paper, we propose an improved Chebyshev map and a visually meaningful image encryption (VMIE) algorithm based on two-dimensional compressive sensing (2DCS). First, the adoption of 2DCS compresses the plain image, wherein the measurement matrix is processed by the simulated annealing algorithm to improve the quality of the reconstructed image. Second, a diffusion operation is performed on the sample data. Furthermore, a matrix encoding matrix is employed to insert the cryptographic image into the host image to obtain a visually meaningful steganographic image. The experimental results and comprehensive analyses show that the proposed scheme has feasible performance and stands up to various attacks. Eventually, the comparison with existing related schemes demonstrates that the proposed image encryption system has the advantages of visual security and reconstruction quality.

1. Introduction

With the advancement of applications supported by the Internet of Things (IoT), the transmission of images and videos on public networks has been growing rapidly [1–3]. Taking medical images as an example, the E-health care IoT can track patients' medical history, physical examinations, treatment records, drug allergy records, and other electronic health files and assist clinicians in formulating treatment plans. In addition, there is sensitive content involving personal privacy. However, they are vulnerable to various security attacks when these data are sent through public channels. Currently, the security risks of transmitting and accessing images in the network restrict the development of remote monitoring and resource sharing. How to guarantee the security of image transmission and access in the network has become a popular topic in academic teams [4,5].

Many image encryption (IE) schemes have recently been developed employing a variety of theories and technologies, such as chaos theory [6,7], DNA coding [8,9], quantum theory [10], and cellular automata mechanism [11,12]. These schemes transform the plain image into a random or noise-like image, which masks the characteristics of the original image. The unexpected behavior of chaotic systems, and their sensitivity to initial values, make them ideal for developing a highly secure and sensitive IE system. From the international cryptanalysis of digital IE algorithms, the insecurities of the above algorithms can be caused by the chaotic behavior of the chaotic system [13,14]. As studied in [15,16], the chaotic system utilized in the IE scheme was inefficient. According to [17], the dynamics of some chaotic systems used for encryption are not sufficiently complicated, resulting in an increased chance of being estimated or detected. Therefore, it is necessary to design new chaotic systems with more complex behaviors.

Compressive sensing (CS) was introduced to the realm of IE to decrease the quantity of data processing and deal with restricted bandwidth [18–21]. In [18], researchers performed DWT on plain images. To reduce the storage space, they used the measurement matrix to perform linear projection on sparse images. Zhou et al. [19] proposed an IE scheme based on 2DCS and the Merlin transform based on the transform domain. For different plain images, the decryption key is the same as others, which causes the system to be easily deciphered by chosen plaintext attacks. In [21], Gan et al. proposed an IE scheme based on 2DCS. Moreover, by combining information entropy, a new diffusion method was proposed. As noted in [20], an IE scheme based

☆ This work was supported by the National Natural Science Foundation of China (61801127), the Science Technology Planning Project of Guangdong Province, China (No. 2019B010140002, No. 2020B111110002), and the Guangdong-Hong Kong-Macao Joint Innovation Field Project, China (No. 2021A0505080006).
* Corresponding authors.
E-mail addresses: weijunli@gdut.edu.cn (W. Li), shutingcai@gdut.edu.cn (S. Cai).

https://doi.org/10.1016/j.chaos.2022.112584
Received 21 May 2022; Received in revised form 2 July 2022; Accepted 17 August 2022
Available online 5 September 2022

on 2DCS was proposed, in which the method of embedding the cipher image into the host image is adopted using the method of embedding based on integer wavelet transform in the spatial domain. However, the measurement matrix was utilized as the decryption key, and since the measurement matrix was not subjected to any special processing, the decrypted image exhibited poor reconstruction quality [22].

The above algorithms all realize the encryption of a plain image. To protect the cipher image and reduce the risk of being attacked by the hacker, researchers have proposed visually meaningful encryption schemes [23]. In [24,25], the compressed data were inserted into a carrier image to produce a visually secure cipher image. These schemes adopted lossy embedding methods based on the transform domain. Although these existing VIE encryption algorithms may have good performance in certain indicators, the quality of reconstructed and encrypted images still suffers from many performance restrictions. In addition, in [26], a lossless least significant bit embedding method was employed to embed the cipher image into the carrier image. However, in the embedding process, the bit change in the carrier image was relatively large, which reduced the processing efficiency.

To overcome the above issues, a high-quality visually secure IE algorithm based on 2DCS and an improved Chebyshev map is introduced. There are two stages to the proposed scheme. In the first stage, the 2DCS and diffusion operation are implemented in the plain image to obtain the compressed secret image. The cipher image is embedded into a host image using matrix-encoded embedding to create a visually secure image in the following procedure. Additionally, the proposed scheme can protect the information security of images and can be applied to multimedia equipment. The private images can be stored and displayed through the transmit and receive end. The images are encrypted at the sender and transmitted through open channels. On the receiving side, only authorized users can decrypt the images. In summary, the following are the contributions and novelties of this work:

1. Based on the Chebyshev map, a new chaotic map is proposed. Performance analyses demonstrate that the proposed system has more chaotic behaviors and a more exhaustive control parameter interval than existing 1D chaotic maps;
2. The simulated annealing algorithm is used to optimize the index sequence for scrambling the measurement matrix to reduce the distortion of the reconstructed image;
3. To reduce the data loss of the secret image and the total number of changed bits in the embedding process, the matrix coding embedding method is exploited;
4. Relative to other schemes, the experimental results reveal that the proposed scheme is more efficient and can provide higher quality reconstructed images and cipher images with higher visual security;

The following is a breakdown of the remaining sections. Section 2 introduces preliminaries such as 2DCS, matrix encoding embedding and the construction of the measurement matrix. Section 3 describes the improved map and analyzes its chaotic characteristics. Section 4 details the specific implementation of the proposed scheme. In Section 5, simulated trials and a performance assessment are carried out. Finally, we conclude this work.

2. Preliminaries

2.1. Two-dimensional compressive sensing (2DCS)

Compressive sensing (CS) uses the signal sparseness to compress the original one-dimensional data x, which can be described as

$$y = \Phi x, \tag{1}$$

where y is the one-dimensional compressed signal of length N, and Φ with a size of $N \times N$ denotes the measurement matrix.

The above 1DCS to process a 2D image can be redefined as follows [27]:

$$Y = \Phi_1 X \Phi_2^T, \tag{2}$$

where $\Phi_1, \Phi_2 \in \mathbb{R}^{M\times N}$ denotes the row and column measurement matrix of CS, Y is the $M \times M$ measurement value matrix, and X is a 2D image of size $N \times N$.

If Φ_1 and Φ_2 are standard Gaussian random matrices, X can be accurately reconstructed from Y with a probability close to 1. This means that Y can be regarded as a feature describing the 2D original signal X.

Similarly, the signal X with the size $N \times N$ is transformed in the Ψ domain and measured with Φ_1,

$$\chi_1 = \Phi_1 \Psi^T X, \tag{3}$$

where Ψ is the $N \times N$ orthogonal basis.

Then, χ_2 is the sparse coefficient of χ_1 in the Ψ domain as

$$\chi_2 = \Psi^T \chi_1^T = \Psi^T X^T \Psi \Phi_1^T = \chi \Phi_1^T, \tag{4}$$

where $\chi = \Psi^T X^T \Psi$.

The 2D compressed encrypted result Y is obtained by another measurement matrix Φ_2 as

$$Y = \Phi_2 \chi_2 = \Phi_2 \chi \Phi_1^T, \tag{5}$$

where Y is an $M \times M$ measurement value matrix.

Assuming Φ_1 and Φ_2 satisfy the restricted isometry property (RIP), the original signal X may be reconstructed accurately from Y by solving the following optimal problem:

$$\chi = \arg\min \|\chi\|_0 \quad s.t.\ Y = \Phi_2 \chi \Phi_1^T, \tag{6}$$

where $\|\chi\|_0$ denotes the ℓ_0-norm, i.e., number of nonzero components in χ.

In recent years, many 2DCS reconstruction methods have been proposed, including 2D SL_0 [28], 2D OMP [29], and 2D projected gradient [30]. Herein, the reconstruction algorithm is a 2D projected gradient with embedding decryption (2DPG-ED) [31]. The reconstructed images not only have higher peak-signal-to-noise (PSNR) values than other reconstruction methods but also have superior visual effects.

2.2. Matrix encoding embedding

In the proposed VMIE algorithm, the encrypted data are embedded into the host image using matrix encoding embedding to reduce the data loss during the embedding process. Specifically, the main idea of this method is to represent more bits of information with fewer bits. A triple (n, k, t) can be used to define it, where n denotes the representing bit number, k represents the bit number to be represented, and t denotes the maximum altered bit number. The detailed encoding method can be described as follows [32]:

Assuming that the original data $b = \{b_1 b_2 \dots b_n\}$ are the bits that can be altered, $x = \{x_1 x_2 \dots x_k\}$ denotes the secret bits, and $b' = \{b_1' b_2' \dots b_n'\}$ is the modified host data with encrypted bits encoded in it.

Step 1: Defining a function

$$f(b) = (b_1 \times 1) \oplus (b_2 \times 2) \oplus \cdots \oplus (b_n \times n) \tag{7}$$

where $\oplus$ denotes the xor operation.

Step 2: The bit has to be altered at position s, which is calculated by

$$s = f(b) \oplus x \tag{8}$$

Step 3: The host data b are changed according to the following rule:

$$b' = \begin{cases} b & \text{if} \quad s = 0 \\ \{b_1 b_2 \dots 1 - b_i b_n\} & \text{if} \quad s = i \end{cases}. \tag{9}$$

Step 4: Step $1 \sim 3$ must be repeated until $f(b) = x$.

Herein, n, k, and t are set to 3, 2 and 1, respectively. This signifies that two bits of the cipher image are embedded in the lowest three bits of a pixel in the host image, and the number of bits has changed by no more than one after the embedding procedure.

2.3. Chaos-based sequence and measurement matrix

To construct the measurement matrix, the sequences are generated by the one-dimensional improved Chebyshev chaotic map (1-DICS) described in the next section. To avoid the transitory effect, the previous N_0 outputs of the 1-DICS are ignored. Then, the sequences X and Y may be obtained by using different initial values and control parameters for 1-DICS at every sampling interval d. c is the compression rate. This means that 1-DICS is iterated $dcMN + N_0$ times. Next, the sequences X and Y are processed according to the following equation to obtain two sequences X_n and Y_n:

$$\begin{cases} X_n = 1 - 2 \bmod (X, 1) \\ Y_n = 1 - 2 \bmod (Y, 1) \end{cases} \tag{10}$$

Using Eq. (11) on the sequences X_n, Y_n, one can obtain the matrix $\boldsymbol{\Phi}_a$, $\boldsymbol{\Phi}_b$.

$$\begin{aligned} \boldsymbol{\Phi}_a &= \sqrt{\frac{2}{M}} \begin{pmatrix} X_n(1) & \cdots & X_n(cM(N-1)+1) \\ \vdots & \vdots & \vdots \\ X_n(cM) & \cdots & X_n(cMN) \end{pmatrix} \\ \boldsymbol{\Phi}_b &= \sqrt{\frac{2}{M}} \begin{pmatrix} Y_n(1) & \cdots & Y_n(cM(N-1)+1) \\ \vdots & \vdots & \vdots \\ Y_n(cM) & \cdots & Y_n(cMN) \end{pmatrix} \end{aligned} \tag{11}$$

Next, to improve the equality of reconstruction, the matrices $\boldsymbol{\Phi}_a$ and $\boldsymbol{\Phi}_b$ are shuffled by the index sequences, which are optimized by the simulated annealing algorithm. Two sequences with sizes of $1 \times cM$ and $1 \times N$ named X_{cM} and X_N are selected from X_n. The same process is performed on X_n to obtain Y_{cM} and Y_N. Execute Algorithm 1 with the input X_{cM} and Y_{cM} to attain X_r, and Y_c can be obtained by using X_N and Y_N in the same way.

Algorithm 1 The procedure of optimizing chaotic sequences by using a simulated annealing algorithm

Input: Chaotic sequences x_n and y_n with the same size
Output: Optimized sequence O_p

Given chaotic sequences x_n, y_n
$X_n \leftarrow \text{floor}(\text{mod}(x_n \times 10^{14}, a)) + 1$
$Y_n \leftarrow \text{floor}(\text{mod}(y_n \times 10^{14}, a)) + 1$
$O \leftarrow \text{zeros}(1, a)$
$O_p \leftarrow \text{zeros}(1, a)$
for all $i \leftarrow 1 : a$ **do**
  $O(i) \leftarrow X_n(i) - Y_n(i)$
  if $O(i) \geq 0$ **then**
    $O_p(i) \leftarrow O(i)$
  else
    $P_c \leftarrow e^{-\frac{|O|}{i}}$
    $P_t \leftarrow e^{-\frac{1}{i}}$
    if $P_c \geq P_t$ **then**
      $O_p(i) \leftarrow O(i)$
    else
      $O_p(i) \leftarrow \text{mod}(X_n(i) \oplus Y_n(i), a) + 1$
    end if
  end if
end for
return O_p

According to X_r and Y_c, the matrices $\boldsymbol{\Phi}_a$ and $\boldsymbol{\Phi}_b$ are scrambled to obtain the measurements $\boldsymbol{\Phi}_1$ and $\boldsymbol{\Phi}_2$. The scrambling formulas are shown as

$$\begin{aligned} \boldsymbol{\Phi}_a([1, X_r(i)], :) &= \boldsymbol{\Phi}_a([X_r(i), 1], :) \\ \boldsymbol{\Phi}_a(:, [1, Y_c(\text{j})]) &= \boldsymbol{\Phi}_a(:, [Y_c(\text{j}), 1]) \\ \boldsymbol{\Phi}_1 &= \boldsymbol{\Phi}_a, \end{aligned} \tag{12}$$

where $i \in [1, cM]$, $j \in [1, N]$. Similarly, the above formula processing is also performed on $\boldsymbol{\Phi}_b$ to obtain $\boldsymbol{\Phi}_2$.

3. The proposed chaotic map

Here, the original definition of the Chebyshev map is shown as $x_{n+1} = \cos(n \times \arccos x_n)$ with a degree n in [33], where n is a positive integer and x is a real number in $[-1, 1]$.

Then, a new 1-DICS is presented and defined as Eq. (13):

$$x_{n+1} = f(x_n, \alpha) = \cos(\|x\|^{\alpha+0.5} \times \arccos x_n) \tag{13}$$

where $x = \{x_1 x_2 \ldots x_n\}$, and $\alpha > 0$ is a control parameter. Compared to the Chebyshev map, for the majority of α values, the 1-DICS map exhibits exceptionally high chaotic behavior. In what follows, several dynamical system tests are conducted on the 1-DICS map to evaluate its performance.

3.1. Lyapunov exponent

The Lyapunov exponent (LE) describes the average separation and divergence of two trajectories with similar initial values, which is a widely accepted measure of the sensitivity of a system to small changes in initial values. For the chaotic system $f(x_n)$, LE is defined as:

$$LE = \lim_{N \to \infty} \frac{1}{N} \sum_{n=0}^{N} \ln \left| f'(x) \right| \tag{14}$$

A positive LE value implies the occurrence of chaotic activity. Fig. 1 illustrates the LE test results of the 1-DICS, Chebyshev, 1-DFCS [34] and 1-DCP [35] maps. One can see that the proposed map has a more extensive parameter range where LE is greater than 0, and the values are larger compared to other systems.

Furthermore, the sensitivity of the 1-DICS map to its initial values and control parameter is evaluated according to the number of iterations. In Fig. 2, two pairs of initial values and control parameters with minor discrepancies are selected. Subsequently, the 1-DICS map is used to create chaotic sequences and compare their trajectories. It can be shown that the new map diverges with a precision of 10^{-16} for x_0 and 10^{-14} for μ after just 3 iterations, demonstrating that the proposed map has a high sensitivity to the initial condition.

3.2. Bifurcation analysis

A bifurcation diagram is a visual representation of the long-term behavior of a dynamical system based on the values of control parameters. Fig. 3 displays the bifurcation diagrams of the 1-DICS, Chebyshev, 1-DFCS and 1-DCP maps. The output values of the 1-DICS map are randomly distributed across the entire phase plane, indicating that the proposed map has a significant chaotic propensity.

3.3. Sample entropy

To measure the complexity of a time series on a single scale, the sample entropy (SE) [36] is exploited. For time series $\{x_1, x_2, \ldots x_N\}$, temple vector $X_m(i) = \{x_i, x_{i+1}, \ldots x_{i+m-1}\}$, dimension m, and acceptance tolerance r, SE is described as

$$SE(m, r, N) = -\log \frac{A_{m+1}}{A_m} \tag{15}$$

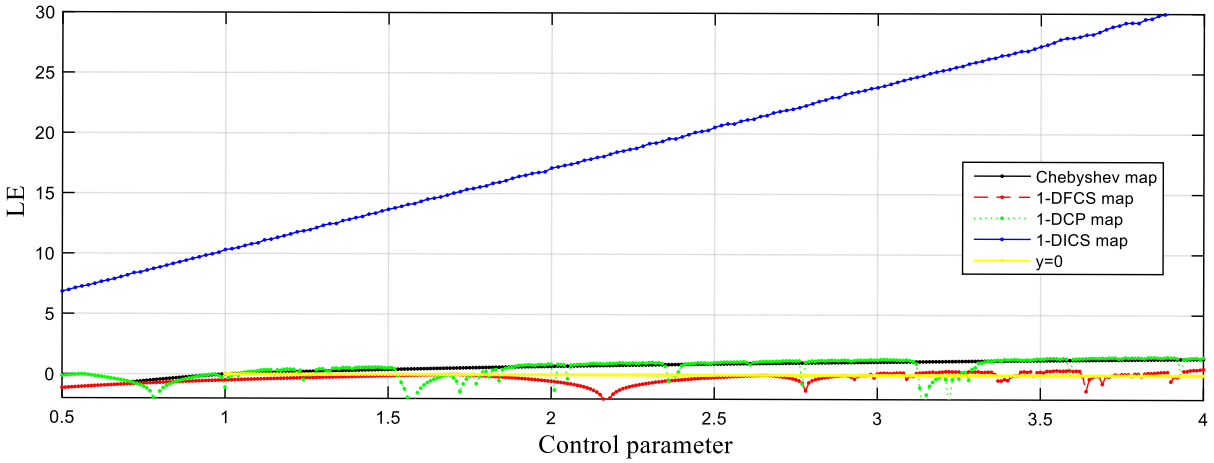
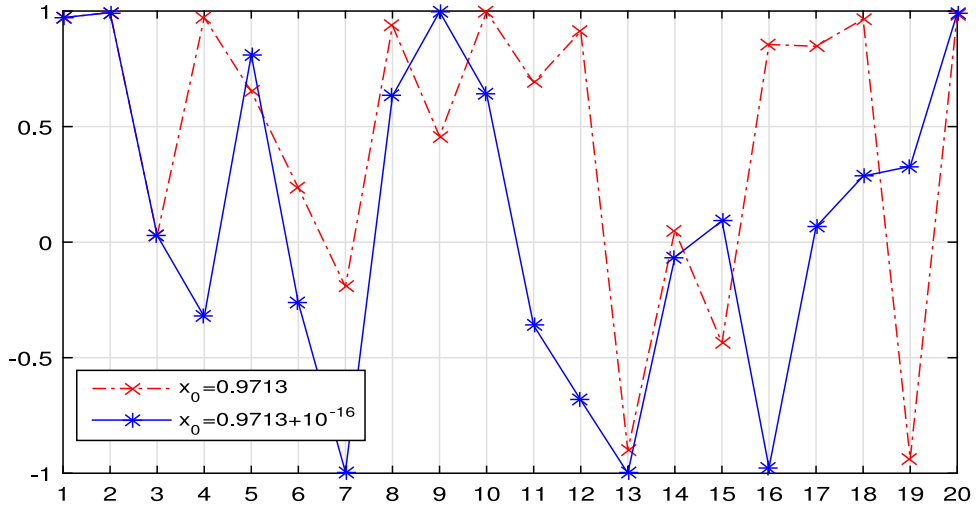
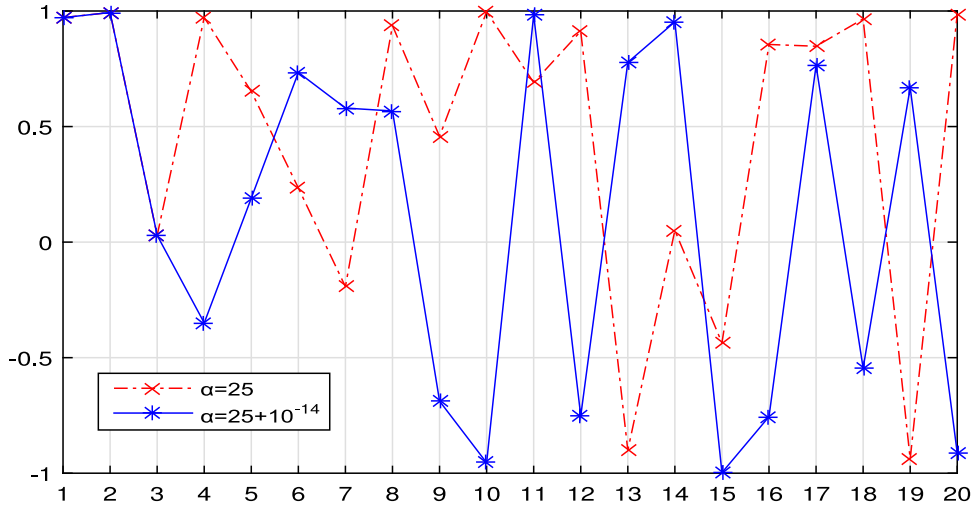


Fig. 1. The LE test results of different maps.

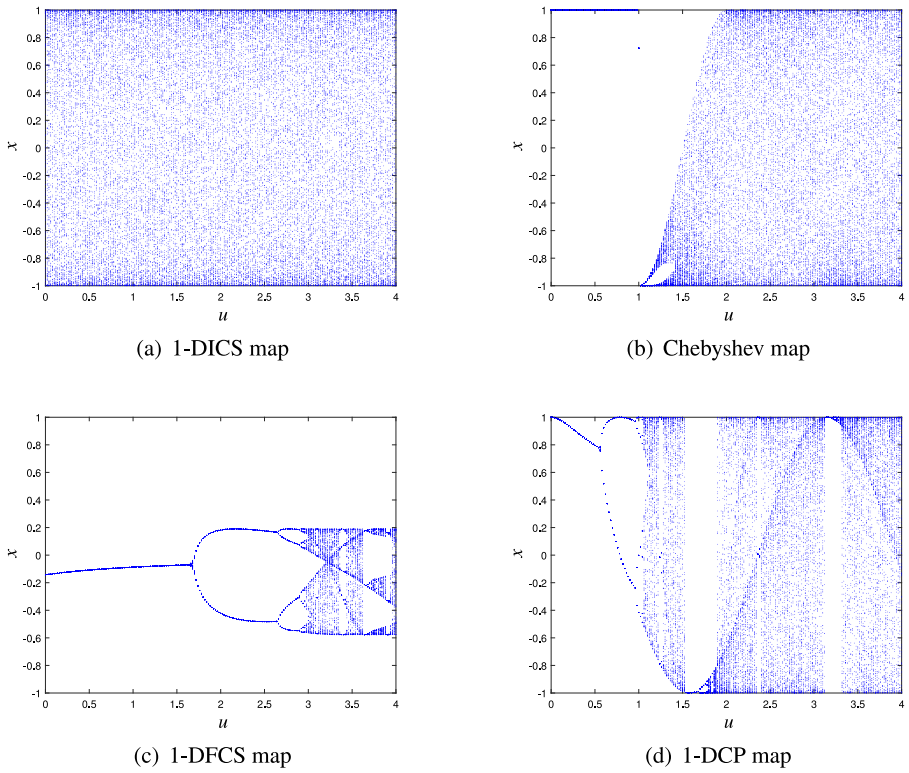


(a)



(b)

Fig. 2. Sensitivity of 1-DICS to minor changes at: (a) initial value x_0; (b) parameter value α.



(a) 1-DICS map (b) Chebyshev map

(c) 1-DFCS map (d) 1-DCP map

Fig. 3. Bifurcation diagram of 1-DICS and other chaotic maps.

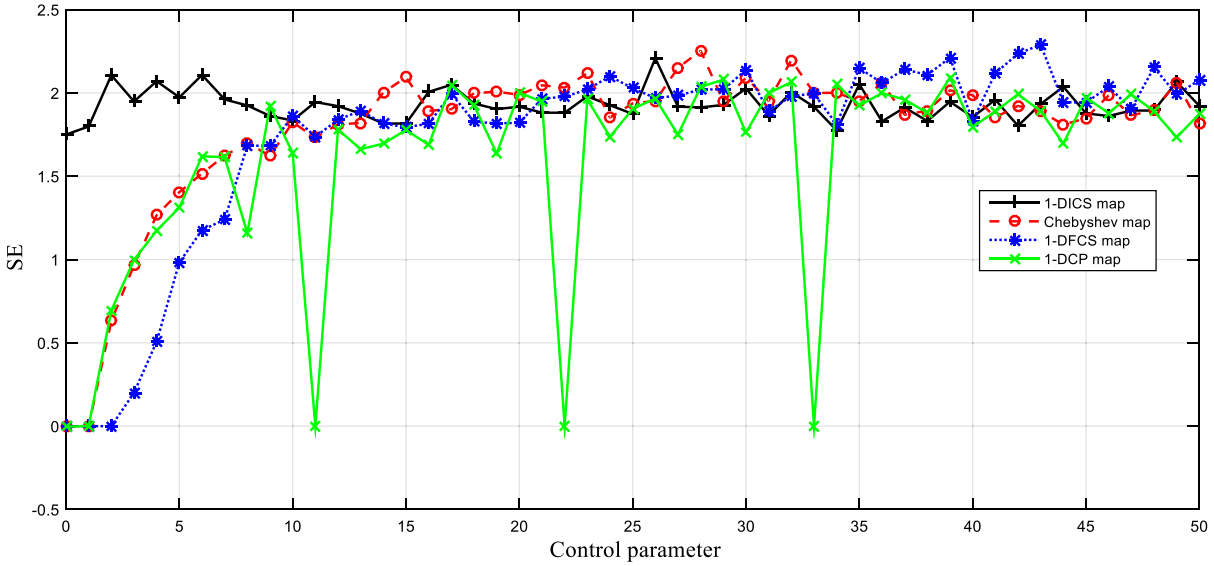


Fig. 4. SE results of the proposed 1-DICS map and other chaotic maps.

A_m denotes the number vectors for $d[X_m(i), X_m(j)] < r$, which is the Chebyshev distance between $X_m(i)$ and $X_m(j)$. A higher SE indicates a lesser amount of regularity and consequently a higher complexity in the sequence. In this experiment, $m = 2$ and $r = 0.2 \times std$ are chosen based on the guidelines [16]. As shown in Fig. 4, the outputs generated by the 1-DICS map have larger SE values than those derived from other maps, which means that the proposed map can construct chaotic sequences with high complexity.

3.4. The 0–1 test

Several studies [37] have examined the 0–1 test as a method for identifying chaotic systems. Unlike the LE, the 0–1 test does not require phase space reconstruction, and the chaotic phenomenon can be judged by whether the output result is close to 1. For real constant $c \in (0, \pi)$, the number of rounds n and sequences S_j, $j \in (1, 2, \ldots, n)$, K is calculated as follows:

$$K = \frac{\log M_c(n)}{\log n} \tag{16}$$

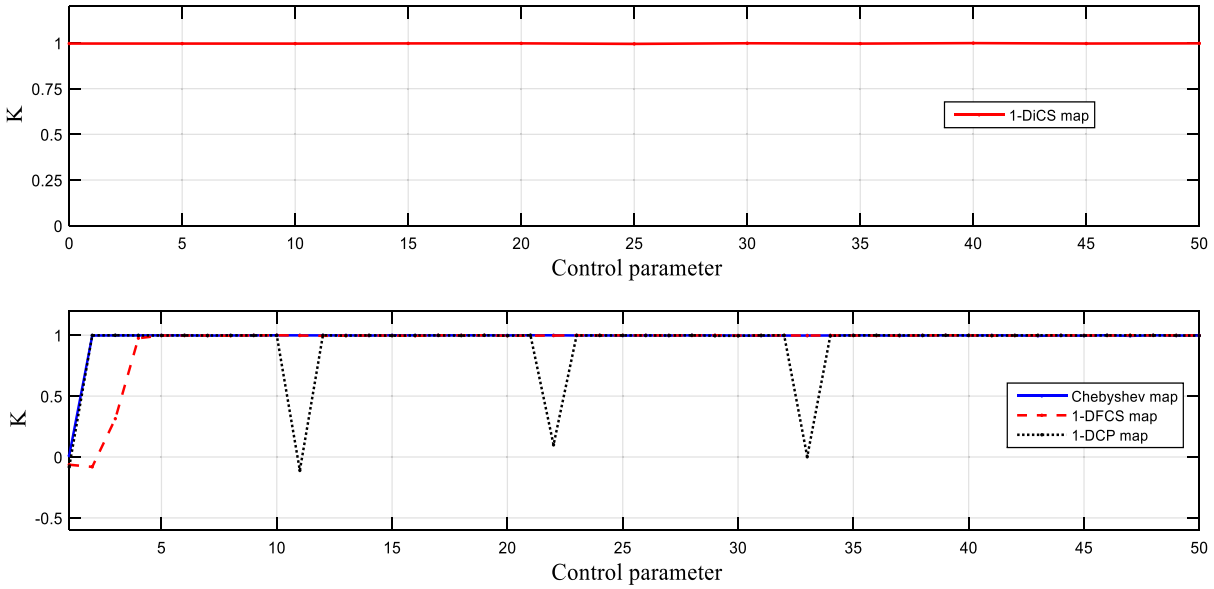


Fig. 5. The 0–1 test of different maps.

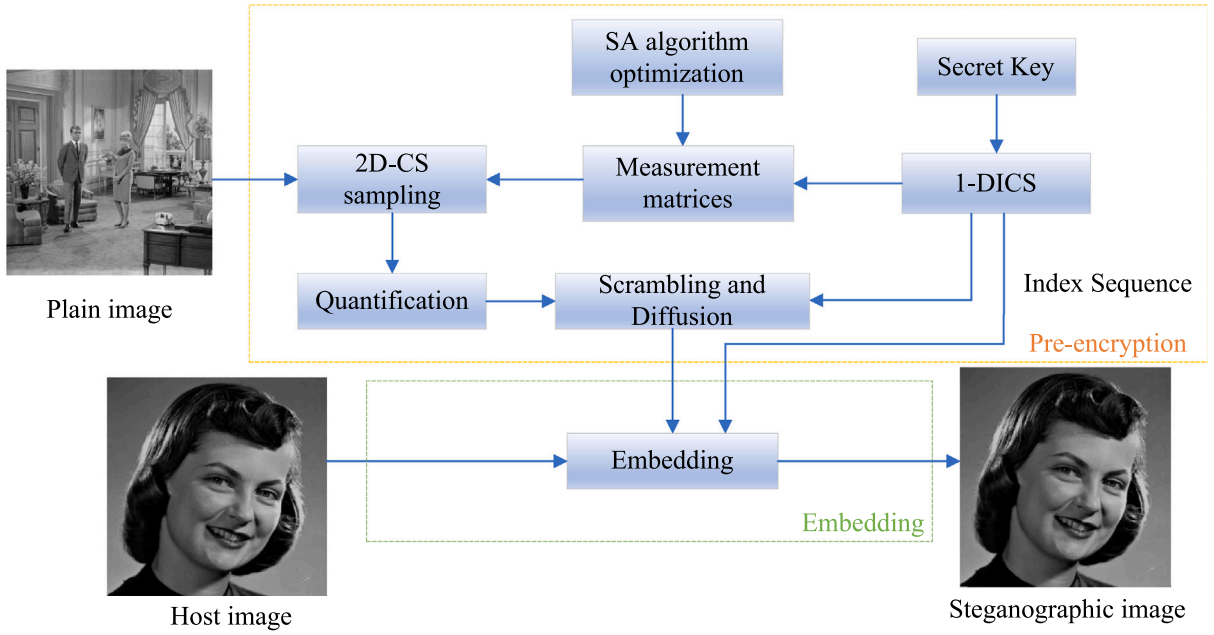


Fig. 6. The flow chart of the encryption process.

where

$$M_c(n) = \lim_{N\to\infty} \frac{1}{N} \sum_{j=1}^{n} [p_c(j+n) - p_c(j)]^2 + [q_c(j+n) - q_c(j)]^2, \quad (17)$$

and

$$p_c(n) = \sum_{j=1}^{n} S_j \cos(ir) \quad (18)$$

$$q_c(n) = \sum_{j=1}^{n} S_j sin(ir). \quad (19)$$

The chaotic phenomenon can be judged by whether the output result K is close to 1. Fig. 5 shows the 0–1 test of the 1-DICS, Chebyshev, 1-DFCS and 1-DCP maps for $r = 2$ and $N = 200$. It can be observed that the K value of the Chebyshev map approaches 1 when the control parameter is greater than 1.4, while the results of the 1-DICS map are always close to 1. For other maps, the results are not sufficiently ideal.

3.5. NIST SP 800-22 test

Among the numerous standard tests for pseudorandomness, an effective method for proving the quality of the chaotic sequences is to compare them with the NIST (National Institute of Standards and Technology) Statistical Test Suite SP 800-22. The output of 1-DICS is compared with the threshold value of 0.707 to generate a bit stream. In our experiments, 100 sequences ($s = 100$) of 1,000,000 bits are tested by NIST. If the P-value of any test is smaller than 0.0001, the sequences are considered insufficient, and the generator is unsuitable. Table 1 lists the P-value of 1-DICS. We can conclude that all outputs of 1-DICS have successfully passed the NIST statistical test suite. These results prove that the proposed 1-DICS has high randomness behavior.

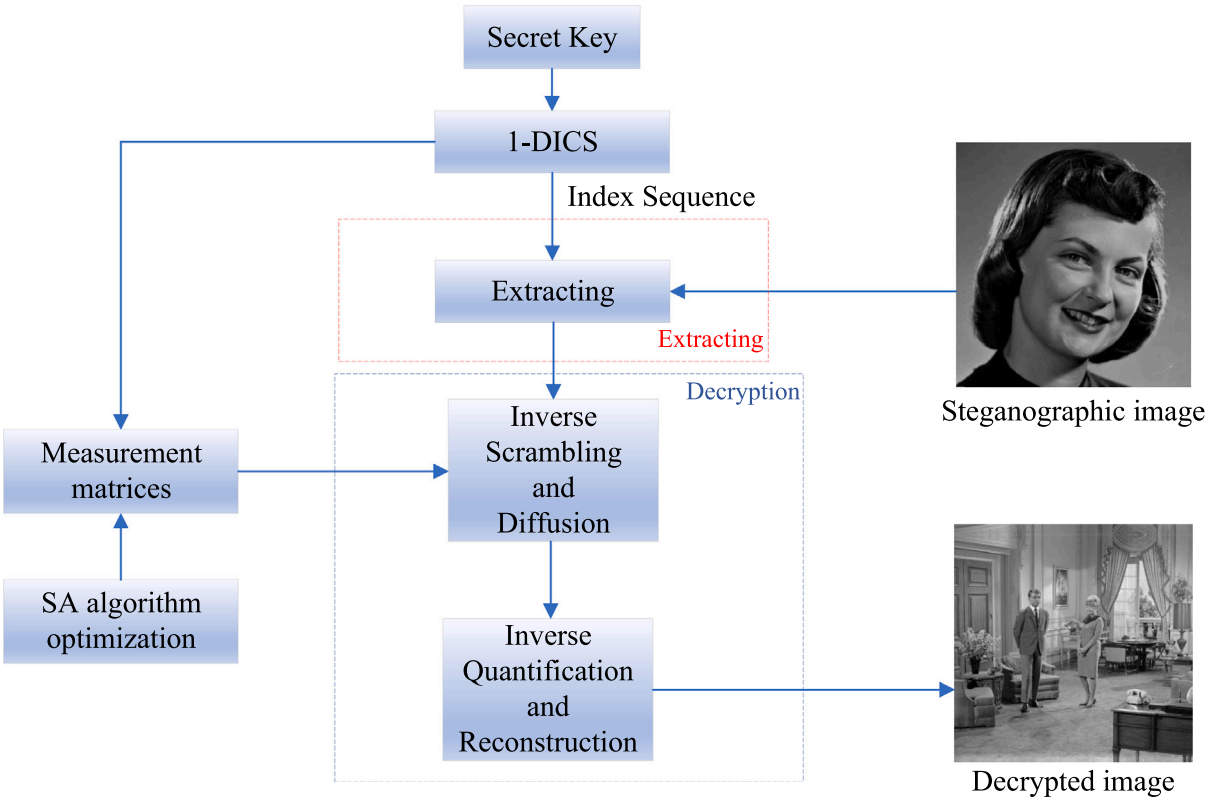


Fig. 7. The flow chart of decryption process.

Table 1
The results of the NIST test.

Test index	*P*-value	Result
Frequency (Monobit) Test	0.350485	PASS
Frequency Test within a Block	0.494392	PASS
Runs Test	0.779188	PASS
Longest Run of Ones in a Block Test	0.474986	PASS
Binary Matrix Rank Test	0.657933	PASS
Discrete Fourier Transform (Spectral) Test	0.224821	PASS
Non-overlapping Template Matching Test	0.637119	PASS
Overlapping Template Matching Test	0.213309	PASS
Maurers Universal Statistical Test	0.574903	PASS
Linear Complexity Test	0.202268	PASS
Serial Test (m = 10)	0.387511	PASS
Approximate Entropy Test (m = 10)	0.911413	PASS
Cumulative Sums (Cusums) Test	0.447795	PASS
Random Excursions Test	0.395937	PASS
Random Excursions Variant Test	0.370639	PASS

Based on the above analyses, the conclusions can be summarized as follows:

- The 1-DICS map generates chaotic sequences with a high sensitivity to initial values.
- The proposed map has a more extensive range of control parameters and is more equally distributed than prior one-dimensional chaotic maps.
- The chaotic sequences derived from the 1-DICS map have excellent pseudorandomness, so they can be used for image encryption.

4. The VMIE algorithm

4.1. Description of the encryption process

This section illustrates a VMIE algorithm based on 2DCS and 1-DICS map, and its flowchart is displayed in Fig. 6. The scheme is categorized into two stages: the pre-encryption stage and the embedding stage. In Fig. 6, one can see that after performing 2DCS on the plain image to obtain the compressed data in the first stage, they are diffused and quantified in the second step to produce a noise-like compressed image. After that, the quantified encrypted data are embedded into the host image to create the steganographic image.

Incidentally, the plain image chosen is $PI \in \mathbb{R}^{M\times N}$, the host image is $HI \in \mathbb{R}^{M\times N}$, the resulting steganographic image is $SI \in \mathbb{R}^{M\times N}$, the decrypted image is $DI \in \mathbb{R}^{M\times N}$ and c is the preset compression rate. Next, the encryption process is introduced in detail.

4.1.1. The pre-encryption stage

Step 1. The measurement matrices $\Phi_1, \Phi_2 \in \mathbb{R}^{cM\times N}$ are constructed by using a 1-DICS map (Section 2.3 describes the process in detail).

Step 2. 2DCS is conducted on PI to obtain compressed data $imgC$:

$$imgC = \Phi_1 \times PI \times \Phi_2^T \tag{20}$$

Step 3. The measured data $imgC$ need to be quantified into the range of $[0, 255]$, and the result is denoted as $imgQ$.

$$imgQ = \left\lfloor \frac{255 \times (imgC - imgC_{\min})}{imgC_{\max} - imgC_{\min}} \right\rfloor \tag{21}$$

where $imgC_{\max}$ and $imgC_{\min}$ are the maximum and minimum values of the elements in $imgC$, and $\lfloor\bullet\rfloor$ denotes the function that rounds numbers to integers.

Step 4. The plain image can be compressed and encrypted simultaneously by using compressive sensing technology. However, it cannot disguise the statistical properties of the image. Thus, another procedure is designed to diffuse the pixel value at random and spread the change across the entire data. In what follows, detailed diffusion is introduced.

Step 4.1. The auxiliary matrix T is created by combining Φ_1 and Φ_2 generated in the previous steps. Then, the product with the elements in the matrix PI is calculated to obtain its average value, denoted as S_{mean}. The following are the formulas for this step:

$$T = [\Phi_1; \Phi_2] \tag{22}$$

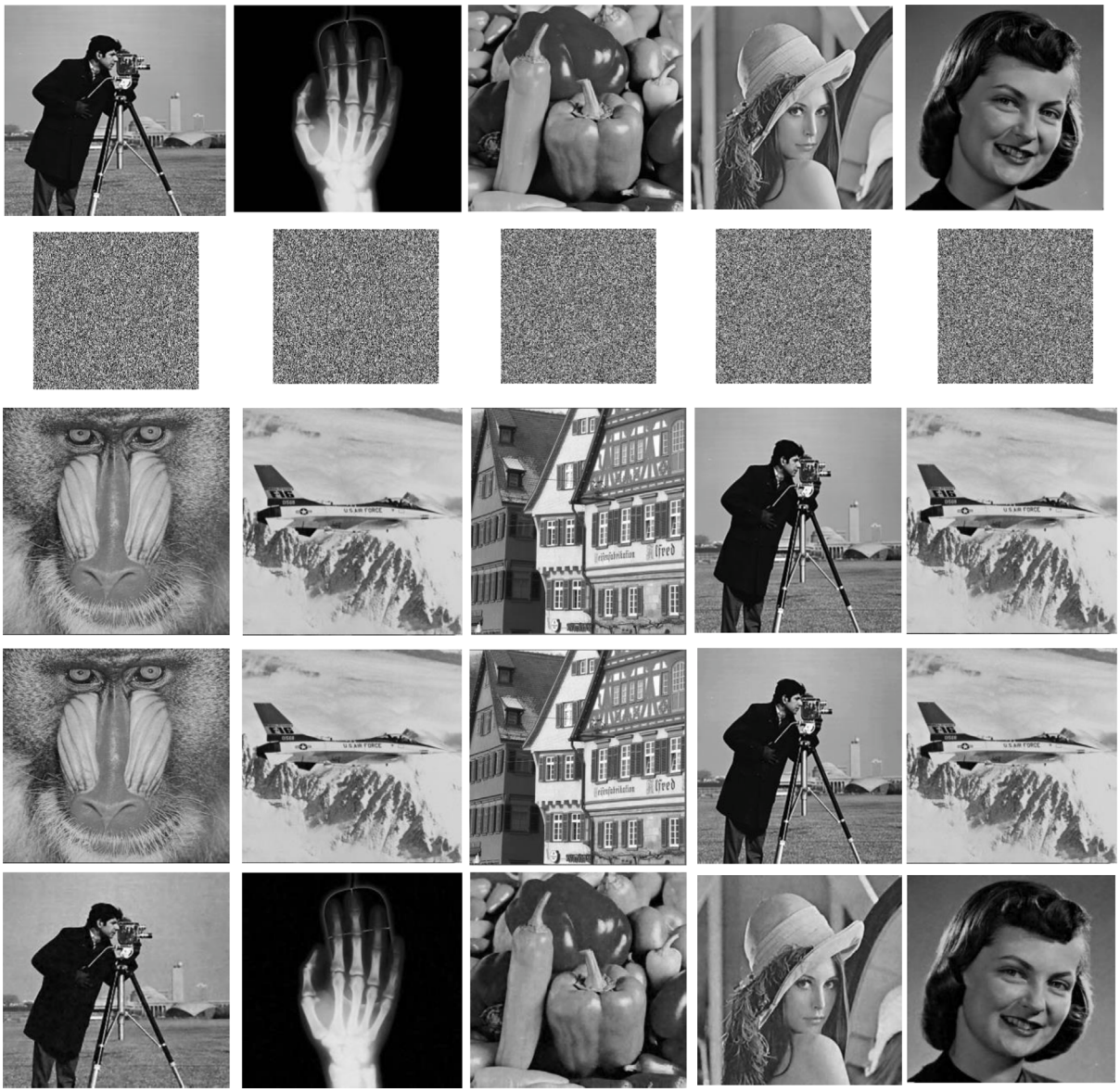


Fig. 8. The results of encryption and decryption of several plain images. The five rows represent plain images, pre-encrypted images, host images, corresponding steganographic images and decrypted images.

$$sum = \sum_{i=1}^{M}\sum_{j=1}^{N} PI(i,j) * T(i,j) \tag{23}$$

$$S_{mean} = \frac{sum}{M \times N} \tag{24}$$

$$su = \left\lfloor \mathrm{mod}(S_{mean} \times 10^{14}, cMN) \right\rfloor \tag{25}$$

$$su1 = S_{mean} - \lfloor S_{mean} \rfloor \tag{26}$$

Step 4.2.: Iterating Eq. (13) c^2MN times to obtain two random sequences $k3$, $k4$. Next, the following formulas are executed to obtain $T1$ and $T2$.

$$\begin{cases} T1 &= \left\lfloor \mathrm{mod}(k3 \times 10^{14}, 256) \right\rfloor \\ T2 &= \left\lfloor \mathrm{mod}(k4 \times 10^{14}, 256) \right\rfloor, \end{cases} \tag{27}$$

After that, two sequences Da and Db with lengths of $1 \times cM$ and $1 \times cN$ are generated by cutting from $T1$ and $T2$. Next, as shown in Eq. (28), Da and Db are used to scramble the compressed data to obtain $imgQD$.

$$\begin{array}{lcl} imgQ([1, Db(i)], :) &=& imgQ([Db(i), 1], :) \\ imgQ(:, [1, Da(\mathrm{j})]) &=& imgQ(:, [Da(\mathrm{j}), 1]) \\ imgQD &=& imgQ, \end{array} \tag{28}$$

Step 4.3. The pre-encrypted image Pr is obtained using the cipher feedback mode as shown in the following formula:

$$Pr(i,j) = \begin{cases} \mathrm{mod}(T1(i,j) * T2(i,j) \oplus 256) + \\ \quad (imgQD(i,j), 256) & i * j = 1 \\ \mathrm{mod}(imgQD(i,j) \oplus mod(T1(i,j) + T2(i,j) \\ \quad , 256) + 256, 256) \oplus C_{pre} & i * j \neq 1 \end{cases} \tag{29}$$

where C_{pre} is the previous encrypted value.

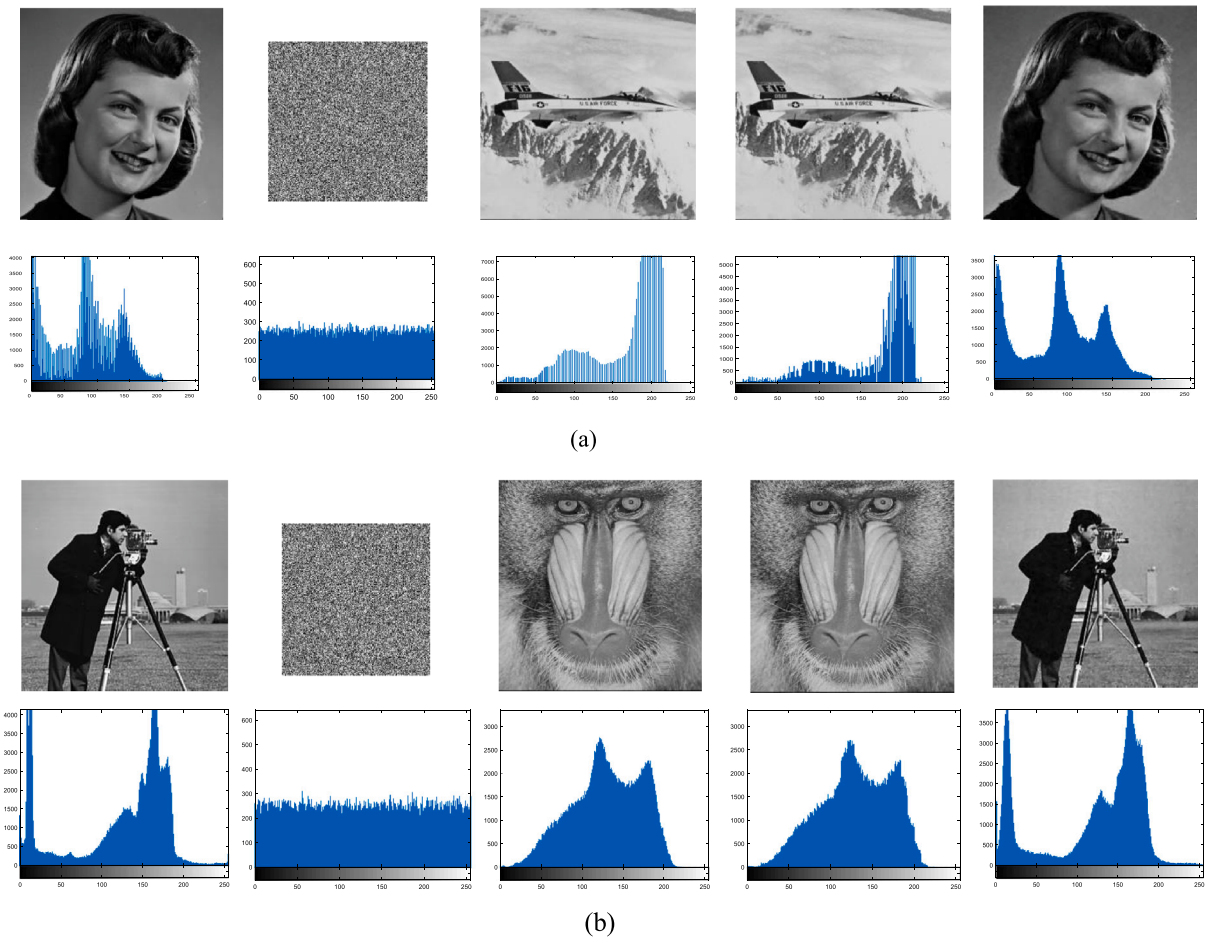


Fig. 9. The histograms of images of different stages in the encryption and decryption process.

4.1.2. The embedding stage

Step 1. Two sequences An and Bn derived from the 1-DICS map are obtained, as shown in the following equation.

$$\begin{cases} An = \{a_1, a_2, \ldots a_{cM}\} \\ Bn = \{b_1, b_2, \ldots b_{cN}\} \end{cases} \tag{30}$$

where the initial values of this 1-DICS map are set to the internal secret key, and the control parameters are all set to $su1$.

Step 2. The embedding position index sequences Asp and Bsp are generated by using the following formulas.

$$[\ , Asp] = \text{sort}(An) \tag{31}$$

$$[\ , Bsp] = \text{sort}(Bn) \tag{32}$$

Step 3. Algorithm 2 details the image embedding procedure. The input of this algorithm is a pre-encrypted image Pr, host image HI, and index sequences Asp, Bsp. After executing the algorithm, a visually meaningful steganographic image SI can be obtained.

4.2. Description of the decryption process

Fig. 7 describes the decryption process. In the extracting process, Pr can be extracted from steganographic image SI losslessly. Next, the measured image $imgQ$ is obtained by performing inverse diffusion and quantification on SI. Then, the 2DPG-ED algorithm is utilized to attain the reconstructed image. The following strategies can be implemented to decrypt the data:

Step 1. The pre-encrypted picture Pr can be extracted from the steganographic image SI using the inverse operation of matrix coding as well as the identical index matrix Asp and Bsp.

Step 2. The first encrypted pixel $imgQD(1,1)$ in the cipher image Pr can be calculated directly by Eq. (33). Additionally, the other pixel values are obtained by using the following formulas.

$$\begin{aligned} imgQD(1,1) = {} & mod(Pr(1,1) + 256 \\ & - mod(T1(1,1) * T2(1,1), 256), 256). \end{aligned} \tag{33}$$

$$imgQD(i,j) = \begin{cases} mod(Pr(1,j) \oplus Pr(1,j-1), 256) \oplus \\ mod(T1(1,j) + T2(1,j), 256) \quad i = 1, j \neq 1 \\ mod(Pr(i,1) \oplus Pr(i-1, M/2), 256) \oplus \\ mod(T1(i,1) + T2(i,1), 256) \quad i \neq 1, j = 1 \\ mod(Pr(i,j) \oplus Pr(i,j-1), 256) \oplus \\ mod(T1(i,j) + T2(i,j), 256) \quad i \neq 1, j \neq 1 \end{cases} \tag{34}$$

Step 3. Perform a reverse scrambling operation on $imgQD$ to obtain $imgQ$.

Step 4. Next, Eq. (35) is used to calculate the sampling data $imgC$ from the secret picture $imgQ$.

$$imgC = \frac{imgQ \times (imgQ_{\max} - imgQ_{\min})}{255} + imgQ_{\min} \tag{35}$$

Step 5. Eventually, the plain image PI is obtained from the secret image $imgC$ using the 2DPG-ED algorithm. The process can be illustrated as follows:

$$PI = 2DPGED(imgC) \tag{36}$$

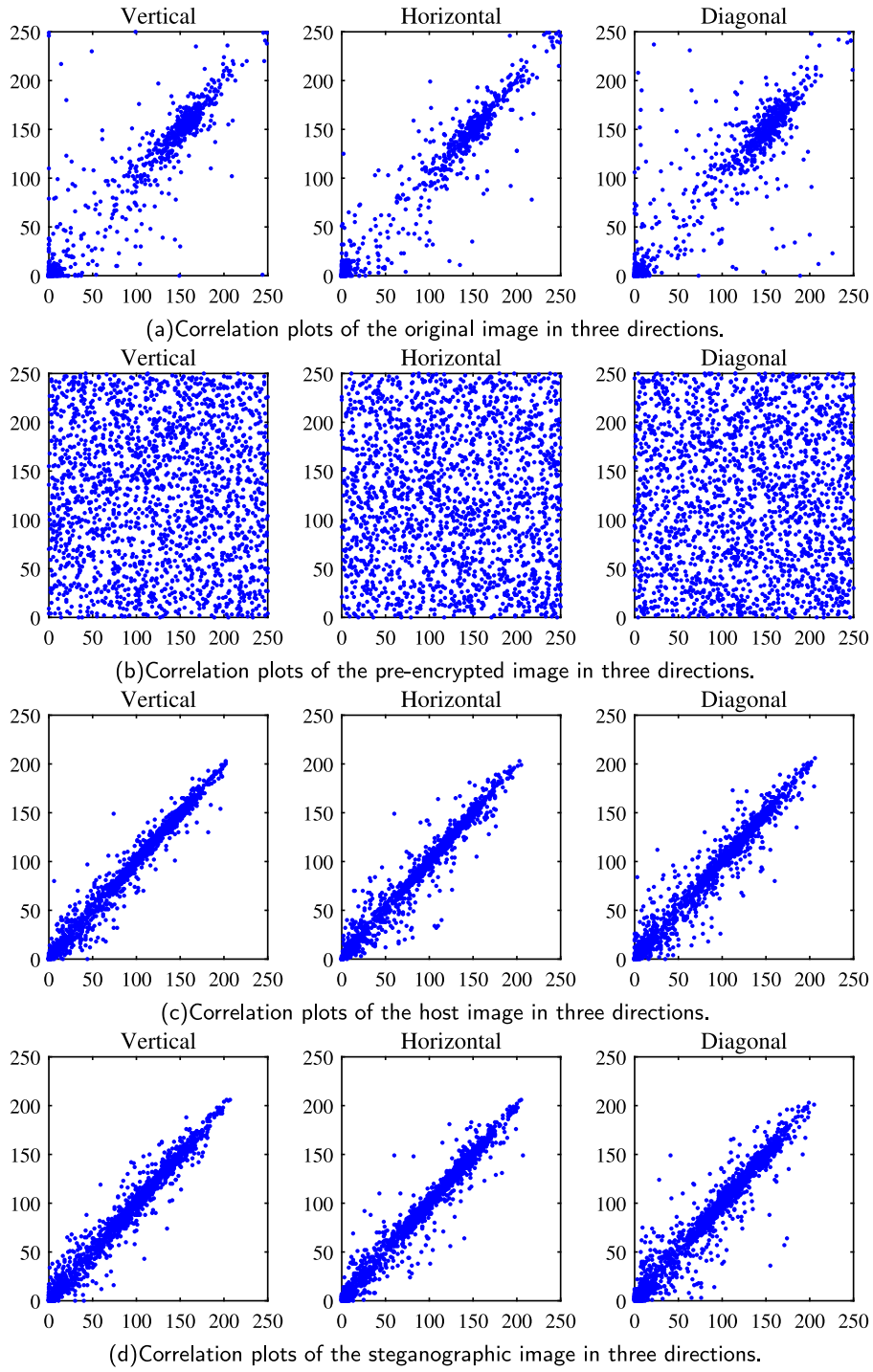


Fig. 10. Pixel correlation analysis.

5. Experimental results and analysis

To analyze the performances of the proposed cryptosystem, different tests were carried out in this section. MATLAB R2014b is used to run the tests on a desktop computer with a 2.90 GHz processor and 8 GB of RAM. In the experiments, with the aim of proving the general applicability of the algorithm, several common images, such as HeadCT, Cameraman, Finger, Peppers, Lena, Airplane, and GirlFace, are chosen at random. Incidentally, the compression rate $c = 0.5$. The following are the secret keys used in the proposed VMIE algorithm. A:[0.9734, 5], B:[0.9734, 0.34], C:[0.7, 0.9], $d = 5$, $N_0 = 100$.

5.1. Simulated results

The results of encryption and decryption of several plain images are shown in Fig. 8. As observed from the figures, after conducting 2DCS and diffusion operations on the original images, the compressed and encrypted images are reduced to a fourth of their original size. Moreover, the pre-encrypted images are embedded into the host image to generate steganographic images. In addition, the decrypted images are of excellent quality. Generally, the PSNR [38] and the mean structural similarity (MSSIM) [39] are used to evaluate the reconstruction quality of the encrypted images and the imperceptibility of steganographic images. The smaller the image distortion is, the higher the value, and

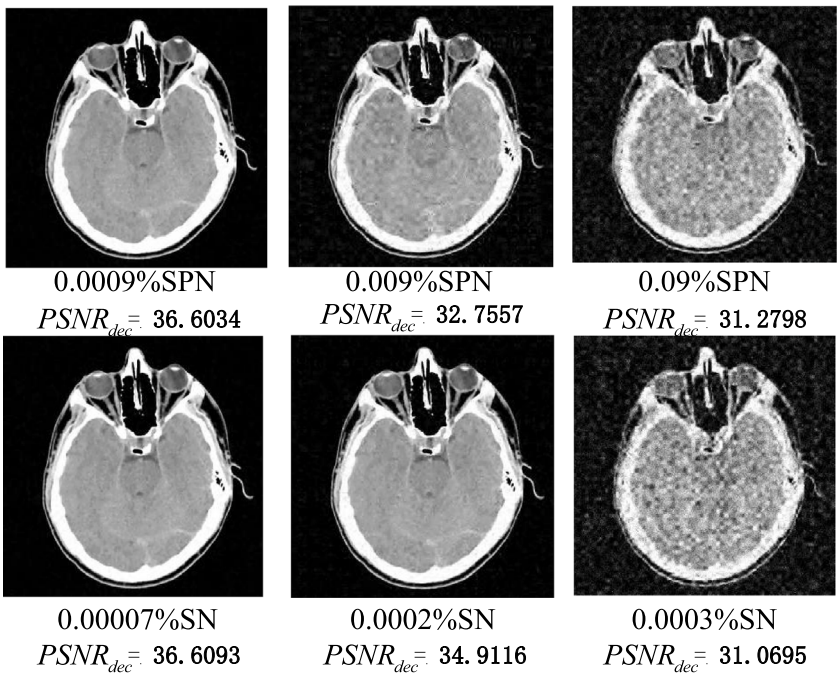


Fig. 11. Test results for noise attack (Unit: dB).

Table 2
Simulation results of PSNR and MSSIM values.

Plain image	Host image	$PSNR_{dec}$ (dB)	$MSSIM_{dec}$	$PSNR_{cip}$ (dB)	$MSSIM_{cip}$
Cameraman	Baboon	34.5663	0.9000	43.9113	0.9967
GirlFace	Airplane	36.7150	0.9301	43.5735	0.9900
Pepper	House	35.3741	0.9258	43.8305	0.9971
Lena	Cameraman	35.2031	0.9219	43.8732	0.9864

their mathematical representations are as follows:

$$PSNR = 10\lg \frac{255 \times 255}{\frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} (X(i,j) - Y(i,j))^2} \tag{37}$$

$$MSSIM(X,Y) = \frac{1}{M} \sum_{k=1}^{M} SSIM(x,y) \tag{38}$$

$$SSIM(x,y) = \frac{(2\mu_X \mu_Y + C_1)(2\sigma_{XY} + C_2)}{(\mu_X{}^2 + \mu_Y{}^2)(\sigma_X^2 + \sigma_Y^2 + C_2)} \tag{39}$$

where $L = 255$, $C_1 = (k_1 \times L)^2$, $C_2 = (k_2 \times L)^2$, $k_1 = 0.01$, $k_2 = 0.01$, and σ_X, σ_Y, μ_X, μ_Y, σ_{XY} denote the variances, mean and covariances of the plain image and decrypted image, respectively. According to the recommendation in [40], K is set to 64.

Table 2 lists the experimental data. For convenience, suffix cip means the values between host images and steganographic images, and suffix dec means the values between decrypted images and plain images. As shown in Table 2, the $PSNR_{cip}$ values are all above 43.5. The $MSSIM_{cip}$ values are greater than 0.98, which indicates that the steganographic images are more visually secure and have a high imperceptibility. Additionally, the $PSNR_{dec}$ values are all above 34.5, and the $MSSIM_{dec}$ values are greater than 0.9. Therefore, the decrypted image has less distortion.

5.2. Histogram analysis

For a general image, due to the difference in the distribution of pixel values in different regions of the image, the distribution of histograms is always asymmetrical. According to information theory, the least amount of information can be obtained when the pixels are distributed uniformly. Consequently, after being encrypted by a practical cryptosystem, the histogram distribution of the secret image should be uniform.

The histograms of images at various stages in the encryption and decryption process are shown in Fig. 9. The histograms of secret images obey a uniform distribution. Furthermore, the histograms between host images and their cipher images are pretty similar, showing that the attacker has difficulty gaining important information by analyzing the histogram of the steganographic image.

5.3. Correlation coefficient analysis

An effective encryption scheme should have good scrambling and diffusion effects and can be judged by computing the correlation between adjacent image pixels. In this experiment, we select 2000 pairs of adjacent pixels from the original image, pre-encrypted image, carrier image, and steganographic image. Then, the correlation coefficients are calculated in three directions according to

$$r_{xy} = \frac{\sum_{i=1}^{N} (x_i - \overline{x})(y_i - \overline{y})}{\sqrt{\sum_{i=1}^{N} (x_i - \overline{x})^2 \sum_{i=1}^{N} (y_i - \overline{y})^2}} \tag{40}$$

where x_i and y_i are the values of adjacent pixels and N denotes the number of selected pixel pairs. $\overline{x}$ and $\overline{y}$ are mean values. The results and correlation plots are shown in Table 3 and Fig. 10. It can be observed that there is a strong correlation between adjacent pixels of the original image. In contrast, the pre-encrypted image has a weak correlation. Furthermore, the correlation plot of the host picture differs significantly from that of the steganographic image, which indicates that the steganographic and host images are quite similar, implying that it is difficult for attackers to distinguish the private data using correlation analysis.

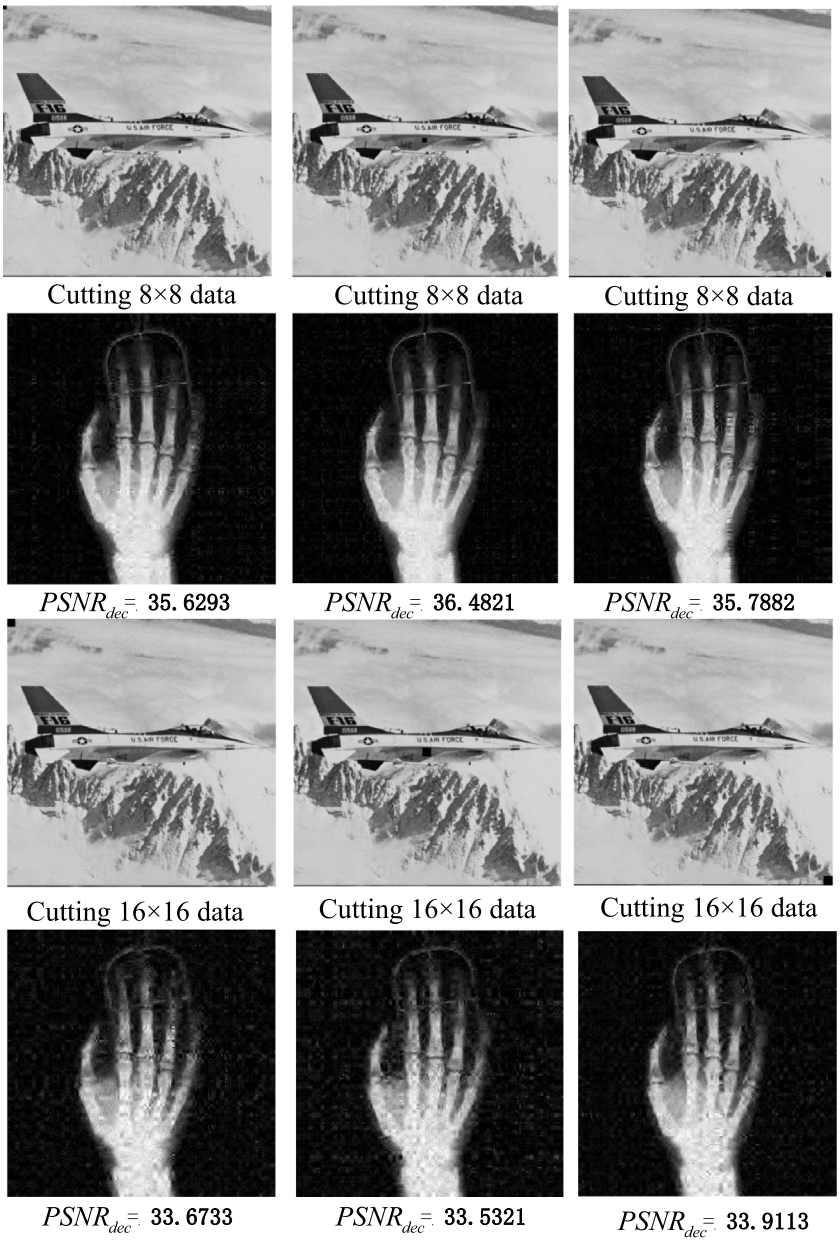


Fig. 12. Robustness test results against cropping attack (Unit: dB).

Table 3
Correlation analysis along three directions in the plain, pre-encrypted, host and steganographic images.

Image	Horizontal	Vertical	Diagonal
Plain image(HeadCT)	0.9809	0.9530	0.9402
Pre-encrypted image	0.0022	0.0054	−0.0069
Host image(GirlFace)	0.9845	0.9870	0.9792
Steganographic image	0.9826	0.9851	0.9772

5.4. Plaintext sensitivity analysis

In image cryptosystems, plaintext sensitivity is an important metric to evaluate immunity against chosen or known-plaintext attacks. In this subsection, we measure the plaintext sensitivity of the proposed algorithm through the number of pixels change rate (NPCR) and unified average changing intensity (UACI). For an ideal image cryptosystem, the ideal NPCR and UACI scores should be near 99.61% and 33.44%, respectively. The steganographic image created by using the proposed VMIE method is visually highly similar to the carrier images. As a result, we test the pre-encrypted images without considering the embedding procedure. Accordingly, four plain images with a size of 512 × 512 and the modified plain images that correspond to them are encrypted. The modified rule is to keep the total sum of pixels unchanged, add 1 to the pixel value at a random position of the plain image, and subtract one at the other position. The experimental data for calculating the NPCR and UACI are listed in Table 4.

$$NPCR = \frac{\sum_{i=1}^{cM}\sum_{j=1}^{cN} D(i,j)}{cM \times cN} \times 100\% \tag{41}$$

$$UACI = \frac{1}{cM \times cN}\left(\sum_{i=1}^{cM}\sum_{j=1}^{cN} \frac{\left|C_1(i,j) - C_2(i,j)\right|}{255}\right) \times 100\% \tag{42}$$

where $D(i,j) = \begin{cases} 0, & C_1(i,j) = C_2(i,j) \\ 1, & C_1(i,j) \neq C_2(i,j) \end{cases}$, C_1 and C_2 are two encrypted images with a size of $cM \times cN$.

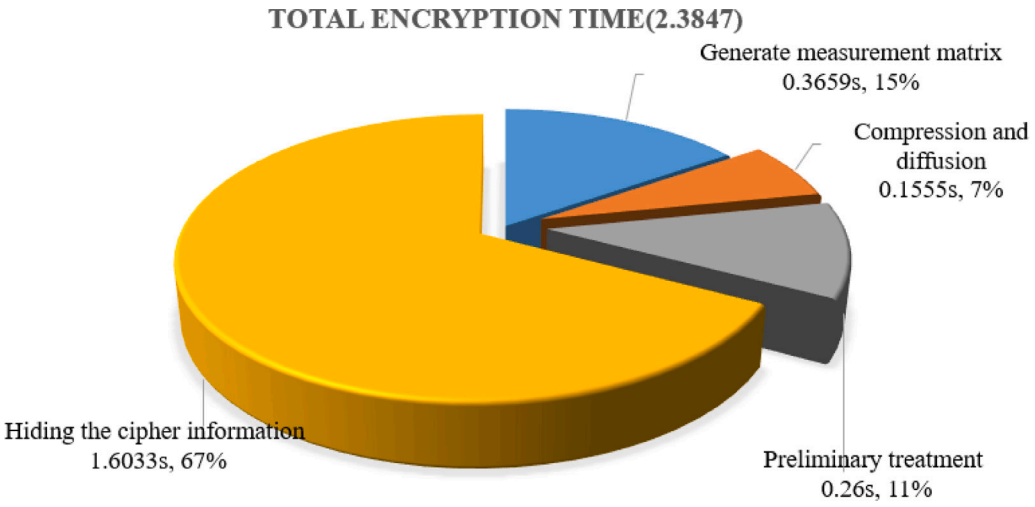


Fig. 13. The time consumed in each process for encrypting image HeadCT.

Table 4
The NPCR and UACI of different images.

Coordinate	Plain image	Host image	$NPCR$ (%)	$UACI$ (%)
$(10,115)^{+},(14,254)^{-}$	HeadCT	Airplane	99.6292	33.5088
$(100,215)^{+},(14,264)^{-}$	Girlface	Airplane	99.6094	33.4576
$(315,56)^{+},(199,237)^{-}$	Finger	Airplane	99.6170	33.4828
$(15,235)^{+},(145,264)^{-}$	Pepper	Airplane	99.6170	33.4565

Table 5
The keyspace of proposed algorithm and others.

Scheme	Proposed	[42]	[43]	[32]	[44]
key space	2^{305}	2^{307}	2^{249}	2^{256}	2^{197}

According to the results in Table 4, it is evident that the NPCR and UACI values are approximately equal to 99.61% and 33.44%, respectively. Furthermore, the proposed VMIE technique has a high plaintext sensitivity and can withstand a chosen/known plain attack.

5.5. Key space analysis

According to Ref. [41], the key pace of a cryptosystem that is not easily deciphered should not be less than 2^{100}. The following are the primary components of the secret keys of the proposed VMIE algorithm. (a) The secret keys d, N and $A : [x_1, u_1]$ used to generate the measurement matrix. (b) $B : [x_2, u_2]$ used to generate the chaotic matrix for obtaining a parameter associated with plaintext information. (c) The secret key $C : [x_3, x_4]$ adopted to generate the index matrix for controlling the embedding process. Based on Section 3.1, the computing accuracy of the initial value and control parameter is 10^{-16} and 10^{-14}, respectively. Then, the total key space is $> (10^{16})^4 \times (10^{14})^2 = 10^{92} \approx 2^{305} \gg 2^{100}$. Table 5 shows the key space of the proposed algorithm and others. It is concluded that the proposed cryptosystem has the advantages of security to withstand brute-force attacks.

5.6. Robustness analysis

Various noises or data loss will affect the steganographic picture during transmission, thereby lowering the quality of the decrypted image. A robust cryptosystem is one in which the decryption procedure can retrieve the majority of the details of the original image even if the secret image is blurred by noise or data is lost. This subsection measures the abilities to resist noise attacks and cropping attacks.

5.6.1. Noise attack

To evaluate the capacity of the proposed VMIE algorithm to withstand noise attacks statistically, different intensities of salt and pepper noise (SPN) and speckle noise (SN) are artificially added to the steganographic images. In this experiment, HeadCT and GirlFace with a size of 512×512 are selected as the plain image and host image, respectively. The corresponding decrypted images and PSNR values are displayed in Fig. 11. One can observe that the impact of SPN on the quality of the decrypted image is smaller than SN. When the steganographic image is affected by the 0.09% SPN, $PSNR_{dec}$ is greater than 30 dB. Additionally, the characteristic texture of the decrypted image is quite clear. As a result, the proposed VMIE scheme stands up to noise attacks well.

5.6.2. Cropping attack

In this subsection, the ability of the proposed system to withstand data loss is analyzed, and Finger is used as a plain image, while Airplane plays the role of a host image. Different data in different positions of the steganographic image are removed, and the corresponding decrypted images are shown in Fig. 12. From the figures, it can be known that even if the steganographic image suffers 16×16 data loss, the values $PSNR_{dec}$ all exceed 33 dB, and the details of the decrypted image can be seen. Therefore, the proposed VMIE algorithm is resistant to cropping attacks.

5.7. Time complexity analysis

Running time is an important indicator for evaluating the performance of the algorithm. In this subsection, the time complexity is analyzed. As can be seen, the encryption process (as shown in Fig. 6) includes pre-encryption and embedding. Assume that the sizes of the plain image and host image are $N \times N$, and the label c_i in the subsequent description represents a constant number. In the pre-encryption process, the time complexity of the generation of measurement matrices and the diffusion process is $O(c_1 N^2)$ and $O(c_2 N^2 log(N^2))$, respectively. Additionally, the time complexity for the embedding process is $O(c_3 N^2)$. It is noted that the time complexity of the decryption process largely depends on the reconstruction method.

In Table 6 and Table 7, it can be observed that for 512×512 images and 256×256 images, the encryption time is approximately 2.4 s and 0.6 s, respectively. Moreover, the entire encryption time of plain image Brain is shown in Fig. 13, along with the proportion of time required by each segment. The embedding process takes more than half of the total encryption time.

Algorithm 2 The image embedding procedure

input: The secret image $S \in \mathbb{R}^{M\times N}$,the host image Q with a size of $M_2 \times N_2$ ($M_2 \geq M, N_2 \geq N$), the index vectors X_n and Y_n.
output: The visually secure steganographic image C.

$imgHid \leftarrow \text{zeros}(1, M_2 \times N_2)$
$Q \leftarrow \text{reshape}(Q, 1, M_2 \times N_2)$
$a \leftarrow 0$
for $i \leftarrow 1 : M_2/2$ **do**
  for all $j \leftarrow 1 : N_2/2$ **do**
    $imgTmp \leftarrow \text{ENCODEMAT}(S(x(i), y(j)), Q(4a-3:4a))$
    $imgHid(4*a-3) \leftarrow imgTmp(1)$
    $imgHid(4*a-2) \leftarrow imgTmp(2)$
    $imgHid(4*a-1) \leftarrow imgTmp(3)$
    $imgHid(4*a) \leftarrow imgTmp(4)$
    $a \leftarrow a+1$
  end for
end for
$C \leftarrow \text{reshape}(imgHid, M_2, N_2)$
return C
function ENCODEMAT($imge, imgc$)
  $temp1 \leftarrow \text{bitand}(imge, 192)$
  $temp2 \leftarrow \text{bitand}(imge, 48)$
  $temp3 \leftarrow \text{bitand}(imge, 12)$
  $temp4 \leftarrow \text{bitand}(imge, 3)$
  $z(1) \leftarrow \text{bitshift}(temp1, -6)$
  $z(2) \leftarrow \text{bitshift}(temp2, -4)$
  $z(3) \leftarrow \text{bitshift}(temp3, -2)$
  $z(4) \leftarrow temp4$
  for $i \leftarrow 1 : 4$ **do**
    $a \leftarrow \text{bitget}(imgc(i), 1)$
    $b \leftarrow \text{bitget}(imgc(i), 2)$
    $c \leftarrow \text{bitget}(imgc(i), 3)$
    $summ \leftarrow \text{bitxor}(\text{bitxor}(c*1, b*2), a*3)$
    if $summ \neq z(i)$ **then**
      $s \leftarrow \text{bitxor}(summ, z(i))$
      if $\text{bitget}(imgc(i), 4-s) == 0$ **then**
        $v \leftarrow 1$
      else
        $v \leftarrow 0$
      end if
      $imgh(i) \leftarrow \text{bitset}(imgh(i), 4-s, v)$
    end if
  end for
  return $imgh$
end function

5.8. Comparison with other works

The comparison tests between the proposed method and other encryption schemes [32,42–44] are described in this subsection. Relative to the current VMIE algorithms, some typical images with sizes of 512×512 have been selected for experimentation. The results include the imperceptibility of the cipher image and the quality of the reconstructed image. It is worth noting that the outcomes of the competing systems are all explicitly cited from the source references to create a fair comparison.

From the point of the imperceptibility of the cipher image, Tables 8 and 9 show the comparison of the $PSNR_{cip}$ and $MSSIM_{cip}$ values. N/A indicates no mention of the value in the associated literature. Specifically, the PSNR values of the proposed scheme are greater than 43 dB, which are larger than others. Furthermore, the MSSIM values are closer to 1 than others.

In addition, the distortion of the reconstructed image is a significant metric in the VMIE algorithm. Table 10 lists the PSNR values of the reconstructed images in the different cryptosystems. The PSNR values of different reconstructed images generated by the proposed VMIE algorithm are greater than 35, which is much larger than most of the comparative literature. Based on the above content, it is shown that the proposed scheme can achieve VMIE without abating the quality of the reconstructed image. Therefore, the proposed algorithm has good visual security and decryption quality.

Table 6
The results of the encryption time (Unit: s).

Image (512 × 512)	Pre-encryption	Embedding	Total
Lena	0.83	1.65	2.48
GirlFace	0.77	1.64	2.41
Pepper	0.80	1.64	2.47
Baboon	0.77	1.67	2.45

Table 7
The results of the encryption time (Unit: s).

Image (256 × 256)	Pre-encryption	Embedding	Total
Lena	0.22	0.40	0.63
GirlFace	0.22	0.40	0.62
Pepper	0.22	0.40	0.63
Baboon	0.21	0.40	0.62

Table 8
Comparisons of the PSNR values in different encryption schemes.

Plain image	Host image	$PSNR_{cip}$ (dB)				
		[42]	[43]	[44]	[32]	Proposed
Lena	Peppers	18.5136	32.3513	31.7986	40.9115	43.8857
Airplane	Baboon	23.3967	37.8967	32.5976	40.9286	43.9490
Girl	Airplane	28.2318	36.1125	N/A	40.9335	43.5463
Barbara	Bridge	25.2321	35.5629	31.7397	40.9233	44.1320
Average		23.8436	35.4801	32.0453	40.9242	43.8783

Table 9
Comparisons of the MSSIM values in different encryption schemes.

Plain image	Host image	$MSSIM_{cip}$				
		[42]	[43]	[44]	[32]	Proposed
Lena	Peppers	0.6726	0.9257	0.9903	0.9917	0.9917
Jet	Baboon	0.6991	0.9833	0.9955	0.9967	0.9967
Girl	Airplane	0.7021	0.9666	N/A	0.9895	0.9901
Barbara	Bridge	0.7337	0.9783	0.9946	0.9973	0.9973
Average		0.7019	0.9635	0.9935	0.9938	0.9940

Table 10
The PSNR values of the reconstruction images in different algorithms (Unit: dB).

Image	[42]	[43]	[45]	Proposed
Lena	<35	28.4422	33.2108	35.3629
Peppers	<34	28.4422	33.2607	35.3795

6. Conclusion

This paper offered a novel 1-DICS chaotic map, which responds perfectly to cryptography requirements. Moreover, a secure and visual image cryptosystem based on 2DCS and a 1-DICS map was designed. The proposed image cryptosystem presented a compression–encryption–embedding structure. Noticeably, the index sequence is optimized using a simulated annealing algorithm to scramble the measurement matrices. In addition, the application of matrix encoding embedding makes the cipher image have an excellent visual effect, which can reduce the risk of being attacked. According to the comparative experiments and detailed analyses, the proposed VMIE algorithm can effectively resist various attacks, and its performance is significantly better in terms of the quality of the reconstructed image and the imperceptibility

of the steganographic image. In the future, the combination of deep learning and steganography will be investigated in terms of improving the efficiency of the proposed cryptosystem.

CRediT authorship contribution statement

Shufeng Huang: Conceptualization, Methodology, Investigation, Software, Writing – original draft, Writing – review & editing. **Donghua Jiang:** Methodology, Data curation, Writing – review & editing. **Qianxue Wang:** Methodology, Investigation, Writing – review & editing. **Mingwei Guo:** Visualization, Investigation. **Linqing Huang:** Software, Validation. **Weijun Li:** Supervision, Investigation. **Shuting Cai:** Project administration, Supervision, Funding acquisition, Writing – review & editing.

Declaration of competing interest

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

Data availability

Data will be made available on request.

References

[1] Huang Huawei, Guo Song, Liang Weifa, Wang Kun, Zomaya Albert Y. Green data-collection from geo-distributed IoT networks through low-earth-orbit satellites. IEEE Trans Green Commun Netw 2019;3:806–16.

[2] Liao Haijun, Zhou Zhenyu, Zhao Xiongwen, Zhang Lei, Mumtaz Shahid, Jolfaei Alireza, Ahmed Syed Hassan, Bashir Ali Kashif. Learning-based context-aware resource allocation for edge-computing-empowered industrial IoT. IEEE Internet Things J 2020;7:4260–77.

[3] Esposito Christian, Ficco Massimo, Gupta Brij Bhooshan. Blockchain-based authentication and authorization for smart city applications. Inf Process Manag 2021;58:102468.

[4] Kaur Manjit, Singh Dilbag, Kumar Vijay, Gupta BB, El-Latif Ahmed A Abd. Secure and energy efficient-based E-health care framework for green internet of things. IEEE Trans Green Commun Netw 2021;5:1223–31.

[5] Hamza Rafik, Yan Zheng, Muhammad Khandan, Bellavista Paolo, Titouna Faiza. A privacy-preserving cryptosystem for IoT E-healthcare. Inform Sci 2020;527:493–510.

[6] Liu Jinyuan, Wang Yong, Han Qi, Gao Jerry. A sensitive image encryption algorithm based on a higher-dimensional chaotic map and steganography. Int J Bifurc Chaos 2022;32(01).

[7] Gao Xinyu, Mou Jun, Xiong Li, Sha Yuwen, Yan Huizhen, Cao Yinghong. A fast and efficient multiple images encryption based on single-channel encryption and chaotic system. Nonlinear Dynam 2022;108(1):613–36.

[8] Nematzadeh Hossein, Enayatifar Rasul, Yadollahi Mehdi, Lee Malrey, Jeong Gisung. Binary search tree image encryption with DNA. Optik 2020;202:163505.

[9] Chen Lei, Li Chengqing, Li C. Security measurement of a medical communication scheme based on chaos and DNA coding. J Vis Commun Image Represent 2022;83:103424.

[10] Luo Yuling, Tang Shunbin, Liu Junxiu, Cao Lvchen, Qiu Senhui. Image encryption scheme by combining the hyper-chaotic system with quantum coding. Opt Lasers Eng 2020;124:105836.

[11] Dong Youheng, Zhao Geng, Ma Yingjie, Pan Zhou, Wu Rui. A novel image encryption scheme based on pseudo-random coupled map lattices with hybrid elementary cellular automata. Inform Sci 2022;593:121–54.

[12] Zeng Hongran, Xing Yan, Kim Seok-Tae, Li Xiaowei. Designing real-time 3D image security with CA-based random mode decomposition. Signal Process 2022;197.

[13] Wang Qianxue, Yu Simin, Guyeux Christophe, Wang Wei. Constructing higher-dimensional digital chaotic systems via loop-state contraction algorithm. IEEE Trans Circuits Syst I Regul Pap 2021;68:3794–807.

[14] Wang Qianxue, Yu Simin, Li Chengqing, Lu Jinhu, Fang Xiaole, Guyeux Christophe, Bahi Jacques M. Theoretical design and FPGA-based implementation of higher-dimensional digital chaotic systems. IEEE Trans Circuits Syst I Regul Pap 2016;63:401–12.

[15] Hua Zhongyun, Zhang Yinxing, Zhou Yicong. Two-dimensional modular chaotification system for improving chaos complexity. IEEE Trans Signal Process 2020;68:1937–49.

[16] Hua Zhongyun, Zhou Yicong, Huang Hejiao. Cosine-transform-based chaotic system for image encryption. Inform Sci 2019;480:403–19.

[17] Li Chengqing, Feng Bingbing, Li S, Kurths Juergen, Chen Guanrong. Dynamic analysis of digital chaotic maps via state-mapping networks. IEEE Trans Circuits Syst I Regul Pap 2019;66:2322–35.

[18] li Chai Xiu, Fu Xianglong, Gan Zhihua, Zhang Yushu, Lu Yang, Chen Yiran. An efficient chaos-based image compression and encryption scheme using block compressive sensing and elementary cellular automata. Neural Comput Appl 2018;32:4961–88.

[19] Zhou Nanrun, Li Haolin, Wang Dihua, Pan Shumin, Zhou Zhihong. Image compression and encryption scheme based on 2D compressive sensing and fractional Mellin transform. Opt Commun 2015;343:10–21.

[20] Huo Dongming, Zhu Zhilong, sheng Wei Li, Han Chao, Zhou Xin. A visually secure image encryption scheme based on 2D compressive sensing and integer wavelet transform embedding. Opt Commun 2021;492:126976.

[21] Gan Zhihua, Bi Jianqiang, Ding Wenke, li Chai Xiu. Exploiting 2D compressed sensing and information entropy for secure color image compression and encryption. Neural Comput Appl 2021;33:12845–67.

[22] Wang Zhongpeng, Hussein Zakarie Said, Wang Xiumin. Secure compressive sensing of images based on combined chaotic DWT sparse basis and chaotic DCT measurement matrix. Opt Lasers Eng 2020;134:106246.

[23] Jiang Donghua, Liu Lidong, Zhu Liya, Wang Xingyuan, Rong Xianwei, Chai Hongxiang. Adaptive embedding: A novel meaningful image encryption scheme based on parallel compressive sensing and slant transform. Signal Process 2021;188:108220.

[24] li Chai Xiu, Wu Haiyang, Gan Zhihua, Han Daojun, Zhang Yushu, Chen Yiran. An efficient approach for encrypting double color images into a visually meaningful cipher image using 2D compressive sensing. Inform Sci 2021;556:305–40.

[25] Wen Wenying, kui Hong Yu, Fang Yuming, Li Meng, Li Ming. A visually secure image encryption scheme based on semi-tensor product compressed sensing. Signal Process 2020;173:107580.

[26] Chai Xiuli, Wu Haiyang, Gan Zhihua, Zhang Yushu, Chen Yiran, Nixon Kent W. An efficient visually meaningful image compression and encryption scheme based on compressive sensing and dynamic LSB embedding. Opt Lasers Eng 2020;124:105837.

[27] Zhou Yan, Zeng Fanzhi. 2D compressive sensing and multi-feature fusion for effective 3D shape retrieval. Inform Sci 2017;409:101–20.

[28] Ghafari Aboozar, Babaie-Zadeh Massoud, Jutten Christian. Sparse decomposition of two dimensional signals. In: 2009 IEEE international conference on acoustics, speech and signal processing. 2009, p. 3157–60.

[29] Fang Yong, Wu Jiaji, Huang Bormin. 2D sparse signal recovery via 2D orthogonal matching pursuit. Sci China Inf Sci 2012;55:889–97.

[30] Chen Gao, Li Defang, Zhang Jiashu. Iterative gradient projection algorithm for two-dimensional compressive sensing sparse image reconstruction. Signal Process 2014;104:15–26.

[31] Zhang Bo, Xiao Di, Xiang Yong. Robust coding of encrypted images via 2D compressed sensing. IEEE Trans Multimed 2021;23:2656–71.

[32] Hua Zhongyun, Zhang Kuiyuan, Li Yuanman, Zhou Yicong. Visually secure image encryption using adaptive-thresholding sparsification and parallel compressive sensing. Signal Process 2021;183:107998.

[33] Butzer Paul, Jongmans François. P. L. Chebyshev (1821–1894): A guide to his life and work. J Approx Theory 1999;96(1):111–38.

[34] Midoun Mohamed Amine, yuan Wang Xing, Talhaoui Mohamed Zakariya. A sensitive dynamic mutual encryption system based on a new 1D chaotic map. Opt Lasers Eng 2021;139:106485.

[35] Talhaoui Mohamed Zakariya, yuan Wang Xing, Midoun Mohamed Amine. A new one-dimensional cosine polynomial chaotic map and its use in image encryption. Vis Comput 2020;37:541–51.

[36] Richman Joshua, Moorman J Randall. Physiological time-series analysis using approximate entropy and sample entropy. Am J Physiol Heart Circ Physiol 2000;278 6:H2039–49.

[37] Gottwald Georg A, Melbourne Ian. The 0-1 test for chaos: A review. 2016.

[38] Musanna Farhan, Dangwal Deepak, Kumar Sanjeev. A novel chaos-based approach in conjunction with MR-SVD and pairing function for generating visually meaningful cipher images. Multimedia Tools Appl 2020;1–28.

[39] Armijo-Correa JO, Murguía JS, Mejía-Carlos Marcela, Arce-Guevara Valdemar, Aboytes-González JA. An improved visually meaningful encrypted image scheme. Opt Laser Technol 2020;127:106165.

[40] Wang Zhou, Bovik Alan Conrad, Sheikh Hamid R, Simoncelli Eero P. Image quality assessment: from error visibility to structural similarity. IEEE Trans Image Process 2004;13:600–12.

[41] Álvarez Gonzalo, Li S. Some basic cryptographic requirements for chaos-based cryptosystems. Int J Bifurc Chaos 2006;16:2129–51.

[42] Chai Xiuli, Gan Zhihua, Chen Yiran, Zhang Yushu. A visually secure image encryption scheme based on compressive sensing. Signal Process 2017;134:35–51.
[43] Wang Hui, Xiao Di, Li Min, Xiang Yanping, Li Xinyan. A visually secure image encryption scheme based on parallel compressive sensing. Signal Process 2019;155:218–32.
[44] Zhu Liya, sheng Song Huan, Zhang Xi, Yan Maode, Zhang Tao, Wang Xiaoyan, Xu Juan. A robust meaningful image encryption scheme based on block compressive sensing and SVD embedding. Signal Process 2020;175:107629.
[45] Ping Ping, Yang Xiaohui, Zhang Xiaojuan, Mao Yingchi, Khalid Hakizimana. Generating visually secure encrypted images by partial block pairing-substitution and semi-tensor product compressed sensing. Digit Signal Process 2022;120:103263.