Optik - International Journal for Light and Electron Optics 262 (2022) 169375

Contents lists available at ScienceDirect

Optik

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

# Verifiable visually meaningful image encryption based on compressed sensing (CS) and improved game of life (IGOL)

Guoqiang Long [a], Lin Zhou [a,*], Zhihua Gan [b,c,**], Xiuli Chai [a,c], Zhifeng Fu [a], Yakun Ma [a]

[a] School of Artificial Intelligence, Henan Key Laboratory of Big Data Analysis and Processing, Henan University, Zhengzhou 450046, China
[b] School of Software, Intelligent Data Processing Engineering Research Center of Henan Province, Institute of Intelligent Network System, Henan University, Kaifeng 475004, China
[c] Henan Key Laboratory of Cyberspace Situation Awareness, Zhengzhou 450001, China

ARTICLE INFO

*Keywords:*
Image encryption
Secret image sharing (SIS)
Compressed sensing (CS)
Game of life (GOL)

ABSTRACT

Image encryption converts the plain image into a noise-like one to protect information security. However, the obtained cipher images are easy to attract the attention of third parties during transmission and storage, and it is vulnerable to information damage and tampering caused by hacking or noise pollution, which in turn makes the receiver unable to obtain the correct decrypted image even spending many resources. To address these issues, this paper proposed a verifiable visually meaningful image encryption based on compressed sensing (CS) and improved game of life (IGOL). Specifically, the plain image is preprocessed and compressed to obtain compressed image via CS, achieving the purpose of reducing the image size. Subsequently, to improve the encryption effect, dynamic cyclic shift confusion method (DCSCM) and diffusion method based on improved game of life (DMIGOL) are presented and performed on the compressed image to obtain the secret image. Next, multiple shadow images are obtained using the secret image sharing based on the Chinese remainder theorem (CRT-SIS) on the secret image, which improves the robustness of this scheme and achieves multi-party data transfer of image. Finally, the shadow images are embedded into the carrier images respectively to obtain visually meaningful cipher images, reducing the attacker's attention to the cipher images during transmission. Additionally, the Hamming distance authentication method relying on plain image and carrier image is applied, and users can perform identity authentication and integrity check on cipher image. Experimental results demonstrate the security and effectiveness of the proposed scheme.

## 1. Introduction

With the rapid development of internet and computer communication technology, a large amount of information is transmitted to all parts of the world through the Internet every day. Among them, digital images have become an important information transmission

* Corresponding author.
** Corresponding author at: School of Software, Intelligent Data Processing Engineering Research Center of Henan Province, Institute of Intelligent Network System, Henan University, Kaifeng 475004, China.
*E-mail addresses:* zhoulin@henu.edu.cn (L. Zhou), gzh@henu.edu.cn (Z. Gan).

https://doi.org/10.1016/j.ijleo.2022.169375
Received 26 April 2022; Received in revised form 23 May 2022; Accepted 23 May 2022
Available online 26 May 2022

medium for containing intuitive, convenient and rich information. However, there are security risks such as hacker attacks and information leakage in the process of transmission and storage of digital images [1], especially in the military, medical, and geographic fields [2,3]. Therefore, it is urgent to protect the security of digital image and prevent the leakage of image content.

To solve these problems, many image encryption algorithms have been proposed by combining chaotic systems, cellular automata (CA), Brownian motion, and other technologies to protect image security. For example, Kaur et al. [4] proposed an adaptive differential evolution-based Lorenz chaotic system for image encryption to improve the anti-attack ability. Besides, to prevent hackers from using existing chaotic systems to analyze and attack the image encryption scheme, Gao [5] designed a new two-dimensional chaotic system by combining two one-dimensional chaotic systems and linear function; and then, they proposed an image encryption scheme based on the new two-dimensional chaotic system to improve the security of the image. Then, Wang et al. [6] and Mansouri et al. [7] respectively presented image encryption schemes based on new chaotic systems. All these methods have the same feature, which is that the size of the cipher image generated by the above schemes is the same with that of the plain image.

In the big data era, a great many of big images are generated. To facilitate the transmission and storage of the encrypted image, Chai et al. [8] proposed an image compression and encryption scheme based on block compressive sensing (BCS) and elementary cellular automata (ECA) to reduce the size of the image and improve the encryption effect. In order to balance security and compression performance, Li et al. [9] provided an efficient plaintext-related chaotic image encryption scheme based on compressive sensing (CS). However, the confusion and diffusion parts in the above encryption schemes are independent of each other and are not closely related, which easily reduces the security of cipher images. Additionally, the above image encryption method encrypts the plain image to generate a noise-like and meaningless cipher image, and the cipher image information has been completely disrupted and cannot be distinguished. Such meaningless cipher image can be divided into two types according to the number of generated cipher image. The first is to encrypt a plain image to generate the single cipher image. This single cipher image is easily attracted to third-party attention and analysis when it is transmitted and stored together with other natural images. And the transmission process is susceptible to noise pollution leading to information loss and change, which causes decryption failure at the receiver. At the same time, this kind of cipher image is only suitable for two-party transmission and storage, and has no fault tolerance, so it does not meet the needs of multi-party transmission.

To cope with this issue, the second meaningless cipher image encryption method is proposed. That is, obtaining multiple shadow images through secret image sharing (SIS) for a plain image [10–13]. This image encryption method can generate multiple shadow images for transmission at one time. When a shadow image is damaged, other shadow images can be used to recover the plain image, which has strong fault tolerance. In 1979, Shamir [14] first proposed a secret sharing (SS) scheme using the ($k$, $n$) threshold, which divides the secret information into $n$ shares and distributes it to $n$ different receivers. When the data has $k$-1 shares or fewer shares, the secret information cannot be obtained, and the secret information can only be obtained with no less than $k$ pieces of data. Thien and Lin [10] applied SS technology to digital image protection for the first time and proposed image encryption technology based on SIS. Subsequently, Kanso et al. [11] proposed a polynomial-based SIS scheme based on Thien and Lin's scheme. The experimental analysis shows that this scheme has high robustness and effectiveness, however, it truncates the pixel value greater than 250, which leads to the loss of the generated shadow images and cannot perfectly restore the secret image. Therefore, Yan et al. [12] proposed SIS scheme based on the Chinese remainder theorem (CRT), which effectively solves the problem of the former lossy recovery and can achieve lossless recovery. But, the shadow image size generated by Yan's scheme is consistent with the secret image, which is not conducive to transmission and storage. To overcome this problem, Sardar et al. [13] presented a lossless SIS scheme based on polynomial ring, which can achieve lossless recovery while reducing the size of the shadow image. However, the shadow images generated by this SIS algorithm are also in the form of noise, which is easy to attract attention during transmission and storage. At the same time, these schemes do not have the authentication function, and when multiple shadow images are transmitted with information loss and corruption, the receiver cannot distinguish between lossy and lossless shadow image in the first place before decryption, which will bring uncertainty to the following decryption process and consume too much decryption resources and time.

To protect the security of image content and visual appearance, some researchers have proposed visually meaningful image encryption methods. This method first encrypts a plain image to generate the noise-like and meaningless secret image and then embeds it into the carrier image to generate the visually secure and meaningful cipher image [15–20]. This kind of image encryption method realizes the double protection of image information and visual appearance. In 2015, Bao and Zhou [15] first proposed a visually secure image encryption scheme to obtain the visually secure cipher image, but the size of the carrier image is four times that of the plain image, which brings great resource consumption to transmission and storage. To this end, Chai et al. [16] presented a visually secure image encryption scheme based on CS. The size of the generated visually secure cipher image is the same as that of the plain image, which effectively reduces resource consumption and transmission burden. Subsequently, to further improve the compression sampling efficiency and security performance, Wang et al. [17] proposed a visually secure image encryption based on parallel compressed sensing (PCS). To improve reconstruction quality, Hua et al. [18] also introduced visually secure image encryption using PCS and adaptive-thresholding sparsification. Meanwhile, to improve the visual quality and embedding ability of cipher image, Yang et al. [19] proposed a visually meaningful image encryption based on universal embedding model. To resist chosen-plaintext attack (CPA) and known-plaintext attack (KPA), Wang et al. [20] proposed optimized visually meaningful image embedding strategy based on CS and 2D DWT-SVD. Although the visually meaningful image encryption method realizes the visual security of the cipher image and effectively protects the plain image information, these schemes only obtain single cipher image; for the receiver, if the single cipher image is severely attacked, the decryption will fail. In this case, the cipher image needs to be sent again for decryption, which will cause the entire decryption process to take too much time and resources. In addition, transmitting the cipher image again will reduce its security and easily attract the attention of others.

In summary, the current image encryption methods have the following problems: (1) because the cipher image does not contain

authentication information, it cannot be checked to exclude the corrupted image in the first place when the image is corrupted; (2) the transmission of single cipher image is not fault-tolerant, which leads to decryption failure when the cipher image is corrupted in transit; (3) the transmission of meaningless cipher image easily attracts the attention of hacker; (4) there is less correlation between confusion and diffusion processes for plain image during encryption, which makes it easy to attack. To solve the above problems, this paper proposed a verifiable visually meaningful image encryption based on compressed sensing (CS) and improved game of life (IGOL). It consists of three main stages. In the first stage, to reduce the image size and encrypt the image information, the plain image is compressed, and then the secret image is obtained by performing the dynamic cyclic shift confusion method (DCSCM) and diffusion method based on improved game of life (DMIGOL) on it. In the second stage, shadow images are obtained by performing secret image sharing based on the Chinese remainder theorem (CRT-SIS) on the secret image under the transform domain. This allows the secret image to participate in multi-party transmission and can resist information loss during the transmission phase. In the third stage, considering the importance of visual appearance, the integer wavelet transform (IWT) is done on the carrier image to get the low-frequency and high-frequency components, and then the shadow image is embedded in the high-frequency component. In addition, the Hamming distance between the low-frequency component and the shadow image is calculated to get a 256-bit binary sequence as the authentication information, and it is embedded in the high-frequency component of the carrier image to improve the authentication capability of the scheme. Finally, the visually secure cipher image is generated by inverse conversion.

As shown in Fig. 1, the image provider can encrypt the plain image to generate multiple shadow images, and then, these shadow images and authentication information are distributed to different distributed servers for storage to improve security and fault tolerance. Among them, the distributed servers embed both shadow images and authentication information into the carrier images to secure the visual appearance of the distributed images. When users need to use the image, they can download the distributed images

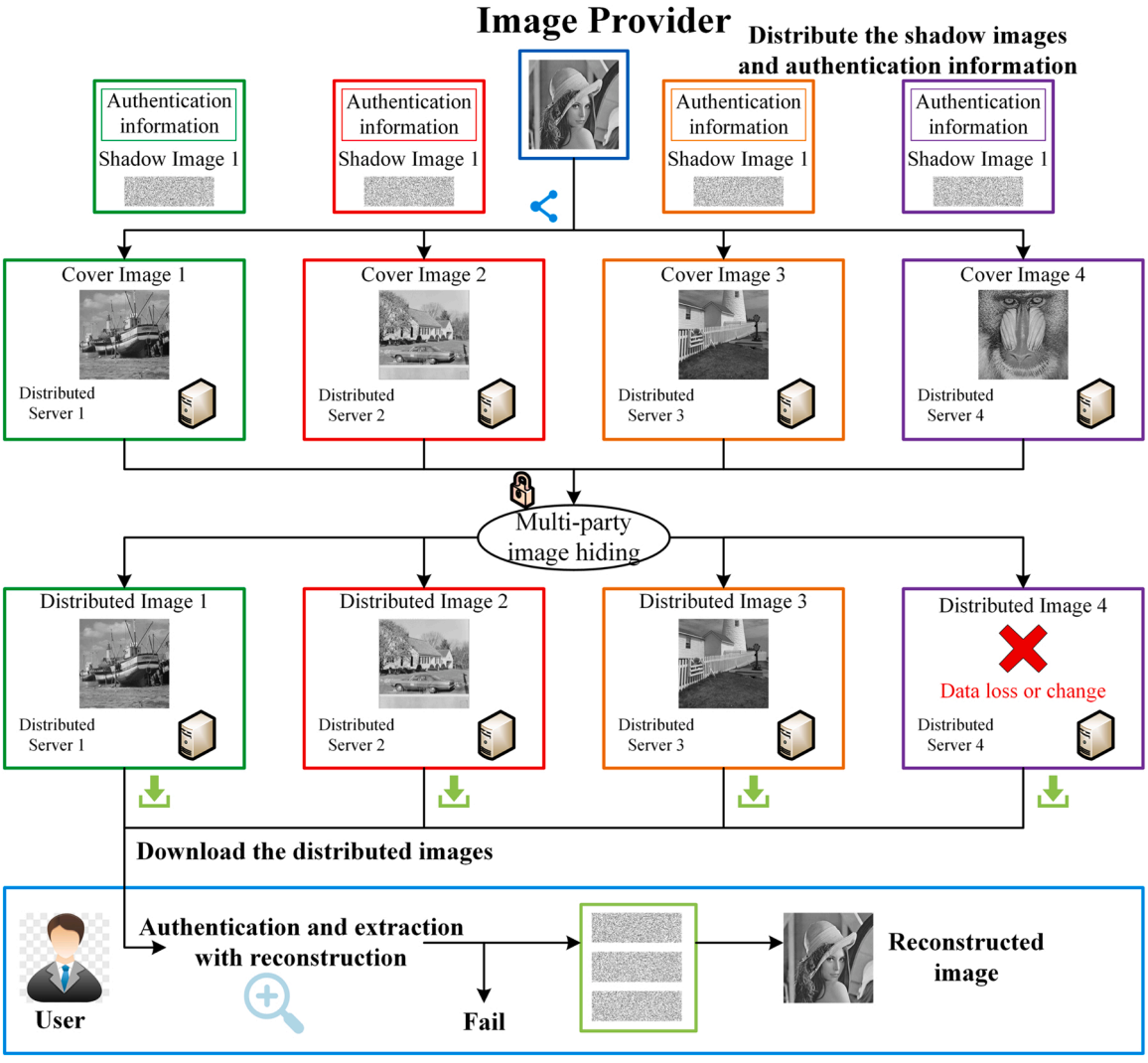


**Fig. 1.** Illustration of the proposed scheme.

from each distributed server for reconstruction to obtain the reconstructed images. When there is data loss or change in some of the downloaded distributed images, they can be authenticated and identified by the user side. Among them, when the number of damaged distributed images exceeds the reconstruction limit, the reconstruction procedure can be ended in advance to avoid the consumption of excessive resources. When the number of damaged images does not exceed the limit, the effect of damaged images can be eliminated in advance. Therefore, the authentication can screen the lossless distributed images in advance, and then they may be used to extract shadow images for reconstruction, and generate reconstructed images for users' use, achieving reasonable utilization of resources and time.

The contributions of our work are as follows:

(1) A dynamic cyclic shift confusion method (DCSCM) is proposed. First, two chaotic sequences are iteratively generated using the two-dimensional Logistic-ICMIC chaotic system (2D-LICMS), and then, each pixel of the plain image is dynamic cyclic shifted by the sequences to achieve effective elimination of the strong correlation between adjacent pixels of the plain image. At the same time, the key space of the encryption scheme is increased, and the ability to resist statistical attacks is improved.

(2) A diffusion method based on improved game of life (DMIGOL) is proposed. In the current GOL-based image encryption method, when there are less than 8 neighboring cells around the outermost cells of the matrix, but the evolution rule that satisfies 8 neighboring cells is still used, which will lead to a low degree of evolution of the outermost cells and the risk of being easily broken. Therefore, this paper considers the characteristic that the total number of neighboring cells is different in different regions of the matrix, improves the traditional GOL rules, designs corresponding evolution rules for different regions of cells, and evolves the initial cell matrix constructed by chaotic sequences to generate an evolution matrix for diffusion encryption of plain image. Both this method and DCSCM are controlled by 2D-LICMS, which can encrypt the image content to the largest extent and greatly improve the security of the encryption scheme.

(3) A secret image sharing based on the Chinese remainder theorem (CRT-SIS) and embedding method under integer wavelet transform (IWT) is proposed. Firstly, the IWT of the secret image is performed to obtain four components, and secondly, the CRT-SIS is done on them to obtain $n$ shadow data of the respective components. Then, 1 shadow is taken from every component and combined to obtain 1 shadow set. Every component has $n$ shadows, so $n$ shadow data sets can be obtained, and then $n$ shadow images are obtained by performing inverse IWT on them. Finally, the $n$ shadow images are embedded in the high-frequency components of each of the $n$ carrier images, and after performing the inverse IWT on them, $n$ visually meaningful cipher images are obtained.

(4) A Hamming distance authentication method relying on plain image and carrier image is proposed. The method uses 2D-LICMS to generate the random sequences. Then, the corresponding element values of the low-frequency components of the shadow image and the carrier image are selected by the sequences, and 256-bit binary authentication information is obtained by calculating the Hamming distance of the selected element values. This authentication information is highly correlated with the plain image and carrier image, with capabilities such as identity authentication and integrity check.

The rest of the paper is organized as follows. Preliminaries of the work are given in Section 2. In Section 3, the proposed image encryption and decryption schemes are presented. Simulation results and performance analyses are provided in Section 4. Section 5 discusses the security of this scheme and the necessity of some sub-operations. Finally, the conclusion is in Section 6.

## 2. Preliminaries

### 2.1. Chaotic system

#### 2.1.1. Two-dimensional Logistic ICMIC chaotic system (2D-LICMS)

2D-LICMS [21] consists of two one-dimensional chaotic systems: Logistic, iterative chaotic map with infinite collapse (ICMIC). This chaotic system has better ergodicity and stochasticity compared to the Logistic, ICMIC chaotic system, and also has more complex dynamics. This means that the system can generate more random chaotic sequences to participate in image encryption. The mathematical expressions are as follows:

$$\begin{cases} x_{n+1} = \sin(21/(\alpha \times (y_n + 3) \times \beta \times x_n \times (1 - \beta \times x_n))) \\ y_{n+1} = \sin(21/(\alpha \times (\beta \times x_{n+1} + 3) \times y_n \times (1 - y_n))) \end{cases} \tag{1}$$

where the system parameters $\alpha \in (0, \infty)$, $\beta \in (0, \infty)$.

#### 2.1.2. One-dimensional Logistic-Tent chaotic system (1D-LTS)

1D-LTS [22] is a new chaotic system obtained by use of two one-dimensional chaotic systems: Logistic and Tent. It has the features of short computation time, good chaotic performance, high security, and high sensitivity, which can be applied to image encryption to improve the performance of cryptosystem. It may be described as,

$$z_{n+1} = \begin{cases} (u \times z_n \times (1 - z_n) + (4 - u) \times z_n/2) mod 1, if z_n < 0.5 \\ (u \times z_n \times (1 - z_n) + (4 - u) \times (1 - z_n)/2) mod 1, if z_n \geq 0.5 \end{cases} \tag{2}$$

where the system parameter $u \in (0, 4)$, and the state variable $z_n \in (0, 1)$, $a \ mod \ b = c$ means that $a$ divided by $b$ has remainder of $c$.

#### 2.1.3. NIST test analysis

The chaotic sequences generated by chaotic systems are widely used in image encryption algorithms, and whether the sequences

are random and unpredictable is related to the encryption effect and security of images. In this section, the NIST SP800–22 test suite is used to test the randomness of the generated sequences. Then, under the condition that the confidence probability $P_\alpha$ is set to 0.01, the sequences generated by 2D-LICMS and 1D-LTS are tested, and the numerical results are shown in Tables 1 and 2. As can be seen from the data in the table, the P-values are all greater than the confidence probability, indicating that the generated sequences passed the test with good randomness. (In this part, chaotic sequences are generated for NIST test by iterating 2D-LICMS and 1D-LTS for 20 million times, respectively; and initial values are set as $x_0 = 0.5$, $y_0 = 0.5$, $\alpha = 0.6$, $\beta = 0.8$, $z_0 = 0.6$ and $u = 0.5502$).

### 2.2. Compressed sensing (CS)

CS was first proposed by Candes and Tao [23] in 2006. CS refers to the compressed sampling of the original signal to obtain fewer sample points, which is much lower than the number of samples determined by the Nyquist's sampling theorem. The original signal can be recovered more accurately by solving a convex optimization problem [24] when reconstructing the signal. Since this technique can change the signal value while compressing the signal, CS can be applied for image encryption. For a signal $x$ of dimension $N \times 1$, the measurement $y$ of $M\times 1$ can be obtained by compressing it using the measurement matrix $\Phi$ of $M\times N$ ($M<<N$), and the compression process is as follows,

$$y = \Phi \cdot x = \Phi \cdot \Psi \cdot s \tag{3}$$

where $\Psi$ is the orthogonal matrix, and $s$ is the sparse coefficient vector.

Signal reconstruction is an important part of the CS technique, where the original signal $x$ is reconstructed by some operation on the measurement $y$ and the measurement matrix $\Phi$ by solving the following convex optimization problem,

$$\min ||s||_1 s.t. y = \Phi \cdot \Psi \cdot s \tag{4}$$

where $||s||_1$ is the $l_1$ norm of the vector $s$ and the measurement matrix $\Phi$ has to satisfy restricted isometry property (RIP) [25]. The original signal $x$ can be effectively recovered by using the reconstruction methods such as matching pursuit (MP) [26], orthogonal matching pursuit (OMP) [27], and smoothed $l_0$ norm ($SL_0$)[28].

### 2.3. Secret image sharing based on the Chinese remainder theorem (CRT-SIS)

The CRT is essentially the problem of solving a set of linear congruent equations [29]. Randomly select $m$ positive integers $q_1, q_2, \ldots, q_m$ that are mutually prime, and for any integer $J_1, J_2, \ldots, J_m$, the following formula holds:

$$\begin{cases} K \equiv J_1 mod q1 \\ K \equiv J_2 mod q2 \\ \cdots \\ K \equiv J_m mod qm \end{cases} \tag{5}$$

Eq. (5) has unique integer solutions and they can be expressed as:

$$K \equiv (J_1 G_1 Q_1 + J_2 G_2 Q_2 + \cdots + J_m G_m Q_m) mod P \tag{6}$$

where $P = \prod_{i=1}^{m} qi$, $G_i = P / qi$, $G_i Q_i \equiv 1\ (mod\ qi)$, $i = 1, 2, \ldots, m$; $K \equiv J_1\ mod\ q1$ means that the integers $K$ and $J_1$ have the same remainder

**Table 1**
Test results of the sequences generated by 2D-LICMS with NIST SP800–22 suite.

| Test Items | P-value ($x_n$) | Results | P-value ($y_n$) | Results |
|---|---|---|---|---|
| Frequency test | 0.304126 | Pass | 0.616305 | Pass |
| Block Frequency test | 0.759756 | Pass | 0.798139 | Pass |
| Cusum-forward test | 0.401199 | Pass | 0.851383 | Pass |
| Cusum-reverse test | 0.534146 | Pass | 0.202268 | Pass |
| Runs test | 0.935716 | Pass | 0.275709 | Pass |
| Longest run test | 0.129620 | Pass | 0.383827 | Pass |
| Rank test | 0.987896 | Pass | 0.350485 | Pass |
| FFT test | 0.289667 | Pass | 0.759756 | Pass |
| Non-Overlapping template test | 0.983453 | Pass | 0.935716 | Pass |
| Overlapping template test | 0.595549 | Pass | 0.978072 | Pass |
| Universal test | 0.383827 | Pass | 0.897763 | Pass |
| Approximate entropy test | 0.657933 | Pass | 0.759756 | Pass |
| Random-excursions test | 0.951882 | Pass | 0.974555 | Pass |
| Random-excursions variant test | 0.808725 | Pass | 0.808725 | Pass |
| Serial1 test | 0.834308 | Pass | 0.678686 | Pass |
| Serial2 test | 0.637119 | Pass | 0.115387 | Pass |
| Linear complexity test | 0.759756 | Pass | 0.249284 | Pass |

**Table 2**
Test results of the sequences generated by 1D-LTS with NIST SP800–22 suite.

| Test Items | P-value | Results |
|---|---|---|
| Frequency test | 0.236810 | Pass |
| Block Frequency test | 0.983453 | Pass |
| Cusum-forward test | 0.534146 | Pass |
| Cusum-reverse test | 0.401199 | Pass |
| Runs test | 0.202268 | Pass |
| Longest run test | 0.739918 | Pass |
| Rank test | 0.699313 | Pass |
| FFT test | 0.023545 | Pass |
| Non-Overlapping template test | 0.998821 | Pass |
| Overlapping template test | 0.115387 | Pass |
| Universal test | 0.085587 | Pass |
| Approximate entropy test | 0.202268 | Pass |
| Random-excursions test | 0.949602 | Pass |
| Random-excursions variant test | 0.985035 | Pass |
| Serial1 test | 0.437274 | Pass |
| Serial2 test | 0.798139 | Pass |
| Linear complexity test | 0.798139 | Pass |

for $q1$.

To show the sharing process, a 2 × 2 matrix is used for CRT-SIS. The secret sharing process is shown in Fig. 2. Assuming $q_1 = 9$, $q_2 = 10$, $q_3 = 11$, $q_4 = 13$. According to Eq. (5), the elements in the matrix are respectively operated to obtain four groups of 2 × 2 shared data.

### 2.4. Dynamic cyclic shift confusion method (DCSCM)

To improve the security and encryption effect of our scheme, the DCSCM is proposed. Algorithm 1 gives the pseudo-code of the proposed confusion method. The confusion process is as follows: firstly, convert the 1 × $mn$ sequences $X1$ and $Y1$ into $m$× $n$ matrices $X_1$, $Y_1$; and then, use the elements in the matrices $X_1$ and $Y_1$ to perform cyclic shift on the elements in the $m$× $n$ plain image $P$ to generate confused image $P1$. Among them, the $X_1$ element is an integer in [1,4], which is used to determine the shift direction of the elements in $P$; the $Y_1$ element is an integer in [1, $m$], which is used to determine the number of shift bits of the elements in $P$.

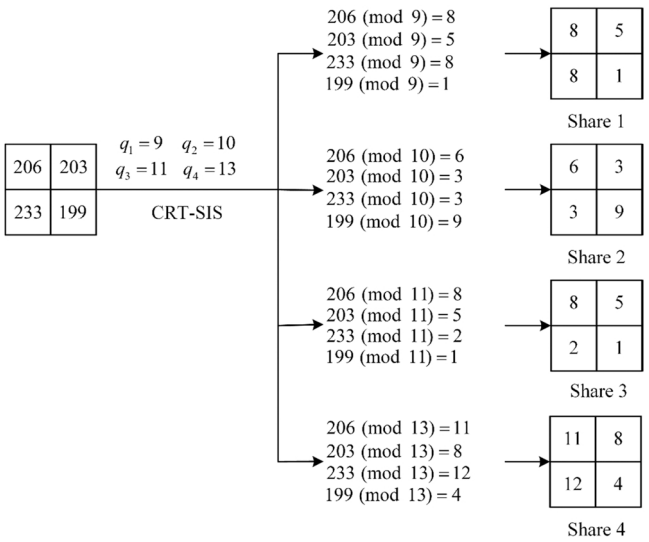


**Fig. 2.** Illustration of CRT-SIS.

**Algorithm 1.** DCSCM.

```
X1 = reshape(X1, m, n); Y1 = reshape(Y1, m, n);
for i = 1 : m do
    for j = 1 : n do
        switch (X1(i, j)) do
            case 1   P(i, :) = circshift(P(i, :), [0, Y1(i, j)]);
            case 2   P(:, j) = circshift(P(:, j), [Y1(i, j)], 0);
            case 3   P(i, :) = circshift(P(i, :), [0, −Y1(i, j)]);
            case 4   P(:, j) = circshift(P(:, j), [−Y1(i, j)], 0);
        end switch
    end for
end for
P1 = P;
```

where, *circshift*() is the circular shift function.

Fig. 3 gives one example of DCSCM. Given the matrix $P$ sized of $3 \times 3$ and matrices $X_1$, $Y_1$, the matrix $P$ is confused by using the matrices $X_1$, $Y_1$ to obtain the confused matrix $P1$. First, cyclically shift the row or column where $P(1, 1)$ is located, since $X_1(1, 1) = 2$, $Y_1(1, 1) = 1$, it can be seen that according to Algorithm 1, the first column of matrix $P$ is circularly shifted by 1 bit from top to bottom. Then, cyclically move the row or column where $P(1, 2)$ is located. It can be seen $X_1(1, 2) = 3$, $Y_1(1, 2) = 2$. Then according to Algorithm

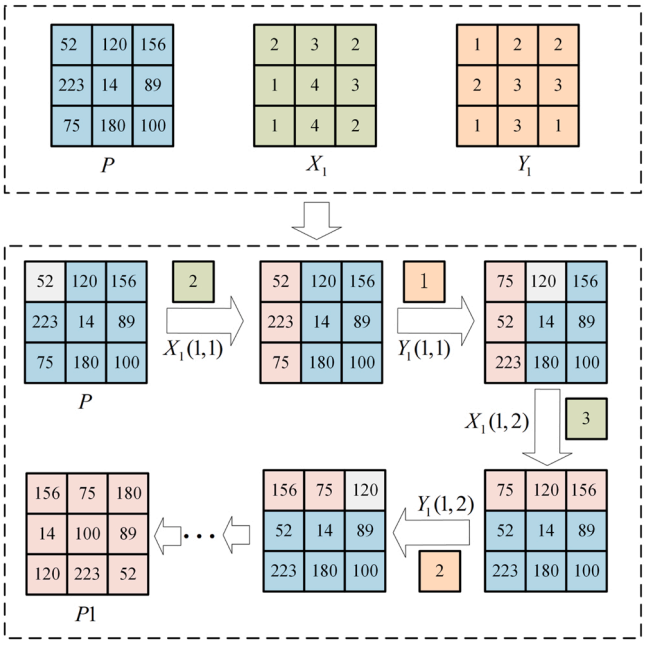


**Fig. 3.** An example of DCSCM.

1, the first row of the matrix $P$ is rotated 2 bits from right to left. Next, through Algorithm 1, the row or column where each element of the matrix $P$ is located is cyclically shifted, and finally, the confused matrix $P1$ is obtained.

### 2.5. Diffusion method based on improved game of life (DMIGOL)

GOL is composed of a two-dimensional cell matrix, and the state of every cell can only be alive or dead. The evolution result of each cell is determined by the state of the adjacent 8 cells around it. Both Gan et al.[30] and Wang et al.[31] introduced GOL into the image encryption scheme to improve the encryption effect and security. However, the GOL used in the current study is not suitable for the evolution of all cells of the matrix. There are less than 8 adjacent cells around the outermost cell, but the evolution rule that satisfies 8 adjacent cells is still adopted, which will lead to the outermost cell having low degree of evolution and risk in danger of being easily cracked. Therefore, this paper considers the different total numbers of adjacent cells in different regions of the matrix, improves the traditional GOL model, designs corresponding evolution rules for cells in different regions, and conducts the initial cell matrix constructed by the chaotic sequence.

#### 2.5.1. Traditional GOL evolution rules

1.Life status of the cell: 1 is alive, and 0 is dead.

2. Evolutionary rules: the evolution of each cell is determined by the state of its adjacent 8 cells, which are cells located in adjacent horizontal, vertical and diagonal directions.

(1) When the current cell is 1, the sum of the surrounding 8 cells is 2 or 3, and it evolves to 1.
(2) When the current cell is 1, the sum of the surrounding 8 cells is greater than 3, and it evolves to 0.
(3) When the current cell is 1, the sum of the surrounding 8 cells is less than 2, and the evolution is 0.
(4) When the current cell is 0, the sum of the surrounding 8 cells is equal to 3, and it evolves to 1.

#### 2.5.2. IGOL evolution rules

1. Life status of the cell: 1 is alive, and 0 is dead.
2. Internal cell evolution rules:
(1) When the current cell is 1, the sum of the surrounding 8 cells is less than 2, and the evolution is 0.
(2) When the current cell is 1, the sum of the surrounding 8 cells is 2 or 3, and it evolves to 1.
(3) When the current cell is 1, the sum of the surrounding 8 cells is greater than 3, and it evolves to 0.
(4) When the current cell is 0, the sum of the surrounding 8 cells is 3, and the evolution is 1, otherwise it is 0.
3. Outermost cell evolution rules (excluding the 4 vertex cells):
(1) When the current cell is 1, the sum of the surrounding 5 cells is 0, and the evolution is 0.
(2) When the current cell is 1, the sum of the surrounding 5 cells is 1 or 2, and it evolves to 1.
(3) When the current cell is 1, the sum of the surrounding 5 cells is greater than 2, and it evolves to 0.
(4) When the current cell is 0, the sum of the surrounding 5 cells is 2, and the evolution is 1, otherwise it is 0.
4. The evolution rules of the outermost 4 vertex cells.
(1) When the current cell is 1, the sum of the surrounding 3 cells is 0, and the evolution is 0.
(2) When the current cell is 1, the sum of the surrounding 3 cells is 1, and it evolves to 1.
(3) When the current cell is 1, the sum of the surrounding 3 cells is greater than 1, and it evolves to 0.
(4) When the current cell is 0, the sum of the surrounding 3 cells is 1, and the evolution is 1, otherwise it is 0.

#### 2.5.3. The manipulation of DMIGOL

Based on the IGOL, we present a DMIGOL, and it uses the IGOL to generate an evolution matrix, which is used to perform the XOR operation with a plain image. Algorithm 2 gives the pseudo-code of this method. The diffusion process is as follows: from lines 1–2 of Algorithm 2, the $1 \times mn$ sequences $X1$ and $Y1$ are converted into $m\times n$ matrices $X_1$, $Y_1$, and the xor operation is performed on them to obtain a $m\times n$ cell matrix $Z$. From lines 3–9 of Algorithm 2, the cell matrix $Z$ is binarily decomposed to generate eight $m\times n$ binary cell matrices $Z_i$, $i = 1, 2, \ldots, 8$; Next, $Z_i$ are evolved $g$ times respectively. Then, the total number of cells $C_j^{sum}(p, q)$ around every cell and the total number of alive cells $C_j^{live}(p, q)$ are calculated during each evolution, $p = 1, 2, \ldots, m$; $q = 1, 2, \ldots, n$; $j = 1, 2, \ldots, g$; then use $C_j^{sum}(p, q)$, $C_j^{live}(p, q)$, and $Z_i$ to evolve according to the rules of the IGOL in Section 2.5, thus obtain the binary evolution matrix $E_i$; then combine the 8 binary evolution matrices $E_i$ to get a $m\times n$ decimal evolution matrix $E$. From lines 10–15 of Algorithm 2, the $m\times n$ evolution matrix $E$ and plain image $P$ are converted into $1 \times mn$ sequences $E1$ and $P1$, and they are xored to obtain the sequence $P2$, finally, $P2$ is converted into the $m\times n$ diffused image $P3$.

**Algorithm 2.** DMIGOL.

$X_1 = reshape(X1, m, n)$; $Y_1 = reshape(Y1, m, n)$;
$Z = X_1 \oplus Y_1$;
for $i = 1 : 8$ do
$Z_i = \left\lfloor \frac{Z \bmod 2^{9-i}}{2^{8-i}} \right\rfloor$;
for $j = 1 : g$ do
The total number of cells $C_j^{sum}(p, q)$ around every cell and the total number of alive cells $C_j^{live}(p, q)$ are calculated during each evolution, $p = 1, 2, \ldots, m$; $q = 1, 2, \ldots, n$; $j = 1, 2, \ldots, g$. According to Section 2.5.2, using the IGOL and $C_j^{sum}(p, q)$, $C_j^{live}(p, q)$ to get the corresponding binary evolution matrix $E_i$.
end for
$E = \sum_{i=1}^{8} E_i \times 2^{i-1}$;
end for
$E1 = reshape(E, 1, mn)$; $P1 = reshape(P, 1, mn)$;
$P2(1) = P1(1) \oplus E1(1) \oplus Y1(1)$;
for $i = 2 : mn$ do
$P2(i) = P1(i) \oplus E1(i) \oplus P2(i\text{-}1)$;
end do
$P3 = reshape(P2, m, n)$;

where, $\oplus$ means xor operation, *reshape*() is a function to adjust the dimension of the matrix, $\lfloor Z \rfloor$ means to take the largest integer not greater than $Z$.

#### 2.5.4. Example of evolution matrix generation

As shown in Fig. 4, given the initial cell matrix $Z$ of $4 \times 4$, the evolution matrix is obtained by using the IGOL evolution. First, decompose the cell matrix of $4 \times 4$ to obtain 8 binary matrices $Z_i$, then use the IGOL rules to evolve each binary matrix $Z_i$ to generate binary evolution matrices $E_i$, and finally, merge the 8 binary evolution matrices $E_i$ to obtain the decimal matrix $E$, which is the evolution matrix, $i = 1, 2, \ldots, 8$.

## 3. The proposed image encryption and decryption scheme

In this section, a verifiable visually meaningful image encryption based on CS and IGOL will be introduced in detail. In the encryption scheme, the plain image is first compressed and encrypted into the secret image, then a set of shadow images is generated by performing CRT-SIS on the secret image. Next, the authentication information is calculated by using the carrier image and the shadow image, and it is embedded in the carrier image. Finally, the cipher image is obtained after embedding the authentication information and shadow images into the carrier image. In the decryption scheme, the authentication information and cipher data are extracted from the cipher image. Then, the cipher data is recovered to get the secret image. Finally, the secret image is decrypted and reconstructed to find the reconstructed image. The detailed encryption and decryption steps are as follows.

### 3.1. Encryption scheme

The encryption scheme proposed in this paper consists of three stages. In the first stage, the plain image is compressed and encrypted into the secret image by CS, confusion, and diffusion methods. In the second one, the IWT is done on the secret image to get one low-frequency and three high-frequency components, and then CRT-SIS is performed on each component to get the corresponding shadow data, and then, the shadow images are obtained by taking the inverse IWT on the shadow data of different components. In the third part, perform IWT on the carrier image to obtain one low frequency and three high frequency components, calculate the Hamming distance of its low-frequency component and the shadow image to get 256-bit binary data as authentication information;

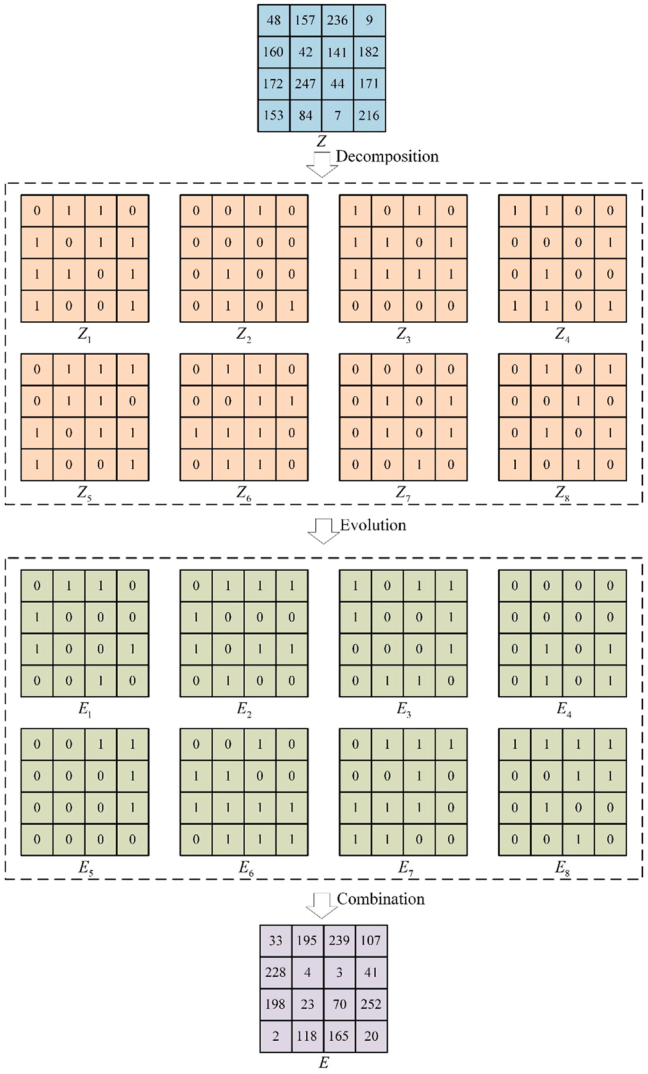


**Fig. 4.** An example of evolution matrix generation.

next, embed the authentication information and the shadow image into the high-frequency components of the carrier image. Finally, perform inverse IWT on the obtained image to get a visually secure cipher image. The detailed image encryption process is shown in Fig. 5.

### *3.1.1. Compression-confusion-diffusion of plain image*

Read in the plain image, and then perform the compression-confusion-diffusion operation on it. The specific steps are as follows.

**Step 1:** Read the plain image $P$ of size $n \times n$, and set the compression ratio CR= 0.25. Manipulate DWT on plain image $P$ to obtain a sparse matrix $P_1$ of the same size. Next, perform zigzag scrambling on the matrix $P_1$ according to Eq. (7) to obtain the $n \times n$ scrambling matrix $P_2$.

$$P_2 = zigzag\left(P_1, A_{zigzag}, B_{ziazag}\right) \tag{7}$$

where $A_{zigzag}$ and $B_{zigzag}$ represent the coordinates of the starting point of zigzag scrambling, respectively; *zigzag*() means *zigzag* scrambling function.

**Step 2:** Set the initial values $x_0$, $y_0$, $a_0$, $b_0$ and bring them into the 2D-LICMS to iterate $m_1 + m \times n$ times, where $m_1 \geq 1000$, $m = ceil$ (CR$\times$ $n$). In order to avoid the influence of transient effects, the first $m_1$ values are discarded, and two chaotic sequences $X$ and $Y$ of $1 \times mn$ are obtained. Then, perform quantization operation on the sequences $X$ and $Y$ according to Eqs. (8) and (9) to obtain $1 \times mn$ sequences $X1$, $Y1$, and $1 \times (n/8)$ index sequences $X2$, $Y2$.

$$\begin{cases} X1(i) = ceil\left(abs\left(X(i) \times 10^{14}\right) mod 4\right) \\ Y1(i) = ceil\left(abs\left(Y(i) \times 10^{14}\right) mod m\right) \end{cases} \tag{8}$$

$$\begin{cases} X2(j) = ceil\left(abs\left(X(j) \times 10^{14}\right) mod \left(n/2\right)\right) \\ Y2(j) = ceil\left(abs\left(Y(j) \times 10^{14}\right) mod \left(n/2\right)\right) \end{cases} \tag{9}$$

where $i$ is an integer in [1, $mn$], $j$ is an integer in [1, ($n$/8)], *ceil*() is the round-up function, the *mod* is the remainder function, and *abs*() is the absolute value function. The sequences $X1$ and $Y1$ are used in the confusion and diffusion operations, and the sequences $X2$ and $Y2$ are utilized in the authentication information generation stage.

**Step 3:** The given initial values $z_0$ and $u_0$ are brought into the 1D-LTS chaotic system to iterate $m_2 + mn$ times, where $m_2 \geq 1000$. In order to avoid the influence of transient effects, the first $m_2$ values are discarded, and the chaotic sequence $Z$ of $1 \times mn$ is obtained. According to Eqs. (10) and (11), the sequence $Z$ is processed to obtain a new sequence $Z_1$, and then the size of $Z_1$ is adjusted to obtain the measurement matrix $\Phi$ of $m \times n$.

$$Z_1 = Z - 0.5 \tag{10}$$

$$\Phi = reshape(Z_1, m, n) \tag{11}$$

where *reshape*() is a function to resize the matrix.

**Step 4:** According to Eqs. (12) and (13), use the $m \times n$ measurement matrix $\Phi$ to measure the $n \times n$ scrambled matrix $P_2$ and obtain the $m \times n$ measurement value matrix $P_3$. Normalize the matrix $P_3$ to the range of [0255] row by row to obtain the $m \times n$ quantization matrix $P_4$.

$$P_3 = \Phi \cdot P_2 \tag{12}$$

$$P_4 = round(mapminmax(P_3, 0, 1) \times 255) \tag{13}$$

where *round*() is the rounding function, *mapminmax*($a$, $b$) is to quantize the elements in the matrix in [$a$, $b$] row by row.

**Step 5:** As described in Section 2.4, take the $1 \times mn$ sequences $X1$, $Y1$, and $m \times n$ quantization matrix $P_4$ as the input of Algorithm 1, perform the DCSCM on the quantization matrix $P_4$, and output the $m \times n$ confused image $P_5$.

**Step 6:** As described in Section 2.5, set the number of evolution $g$, and use the sequences $X1$, $Y1$ of $1 \times mn$, the confused image $P_5$ of $m \times n$, and the number of evolution $g$ as the input of Algorithm 2. The DMIGOL is performed on the confused image $P_5$, and the $m \times n$ secret image $P_6$ is output.

### 3.1.2. Secret image sharing of the secret image

Perform CRT-SIS on the secret image to get the shadow images. The specific steps are as follows.

**Step 1:** According to Eq. (14), perform IWT on the $m \times n$ secret image $P_6$ to obtain components $R_A$, $R_H$, $R_V$, and $R_D$, and all of them have dimensions ($m$/2)× ($n$/2).

$$[R_A, R_H, R_V, R_D] = iwt(P_6, wname) \tag{14}$$

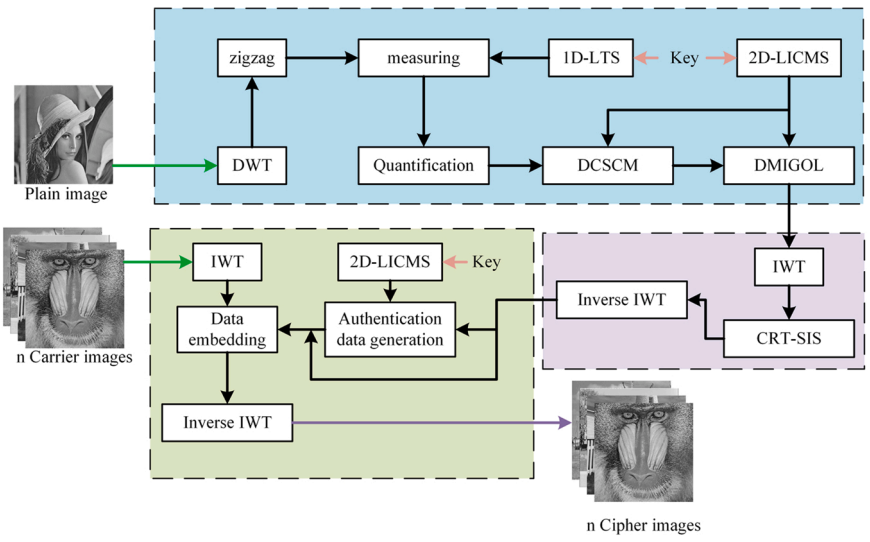


**Fig. 5.** The framework of the proposed image encryption scheme.

where *iwt*() represents the IWT, and *wname* represents the wavelet type.

**Step 2:** According to Eqs. (15) and (16), obtain the minimum values $Min_{RH}$, $Min_{RV}$ and $Min_{RD}$ of the components $R_H$, $R_V$ and $R_D$, and operate these minimum values with the corresponding components to eliminate negative elements to obtain $(m/2)\times(n/2)$ components $R_H^{'}$, $R_V^{'}$ and $R_D^{'}$.

$$[Min_{RH}, Min_{RV}, Min_{RD}] = min(R_H, R_V, R_D) \tag{15}$$

$$\begin{cases} R_H^{'} = R_H - Min_{RH} + 1 \\ R_V^{'} = R_V - Min_{RV} + 1 \\ R_D^{'} = R_D - Min_{RD} + 1 \end{cases} \tag{16}$$

where *min*() is the function to obtain the minimum value.

**Step 3:** Determine the $(t, k)$ threshold secret sharing scheme, where $k$ is the total number of shadow images generated by secret sharing, and $t$ is the threshold value. Any shadow images not less than $t$ can be used to obtain the secret image. Select $k$ pairs of mutually prime numbers $q_i$ as the private key to participate in the SIS, as shown in Eq. (17), perform the CRT-SIS on the four $(m/2)\times(n/2)$ components $R_A$, $R_H$, $R_V^{'}$ and $R_D^{'}$, respectively; to obtain the corresponding shadow data $S_{Ai}$, $S_{Hi}$, $S_{Vi}$ and $S_{Di}$ generated by each component. $i = 1, 2, \ldots, k$, and the size of each component is $(m/2)\times(n/2)$.

$$\left[S_{Ai}, S_{Hi}, S_{Vi}, S_{Di}\right] = crt\left(R_A, R_H^{'}, R_V^{'}, R_D^{'}, qi\right) \tag{17}$$

where *crt*() represents CRT-SIS.

**Step 4:** As shown in Eqs. (18) and (19), carry out IWT to the shadow data $S_{Ai}$, $S_{Hi}$, $S_{Vi}$ and $S_{Di}$ of $(m/2)\times(n/2)$ to obtain $k$ $m\times n$ matrices $S_i^{'}$, $i = 1, 2, \ldots, k$. At the same time, get the minimum value $MinS_i^{'}$ of the matrices $S_i^{'}$.

$$S_i^{'} = Iiwt\left(S_{Ai}, S_{Hi}, S_{Vi}, S_{Di}, wname\right) \tag{18}$$

$$MinS_i^{'} = min\left(S_i^{'}\right) \tag{19}$$

where *Iiwt*() is the inverse IWT.

**Step 5:** According to Eqs. (20) and (21), subtract $k$ $m\times n$ matrices $S_i^{'}$ and their corresponding minimum values $MinS_i^{'}$ to obtain the matrices $S_i^{''}$, and then adjust the size of the matrices $S_i^{''}$ to obtain $(2m)\times(n/2)$ shadow images $C_i$, $i = 1, 2, \ldots, k$.

$$S_i^{''} = S_i^{'} - MinS_i^{'} + 1 \tag{20}$$

$$C_i = reshape\left(S_i^{''}, 2m, n/2\right) \tag{21}$$

### 3.1.3. Generation and embedding of authentication information

**Step 1:** Perform IWT on $k$ carrier images $F_i$ of size $n \times n$ to obtain four $(n/2)\times(n/2)$ components $cA_i$, $cH_i$, $cV_i$ and $cD_i$ for each carrier image, $i = 1, 2, \ldots, k$.

**Step 2:** The Hamming distance is the number of different characters in the corresponding positions of two strings of the same length. This scheme calculates the Hamming distance of two matrices of the same size and converts it into a binary sequence as authentication information. As shown in Eq. (22), calculate the Hamming distance of the low-frequency components $cA_i$ of $(n/2)\times(n/2)$ and the shadow images $C_i$ of $(2m)\times(n/2)$, and get $1\times(n/2)$ binary data as authentication information $A_{Ui}$, $i = 1, 2, \ldots, k$; $j = 1, 2, \ldots, n/8$.

$$A_{Ui} = Hamd(C_i(X2(j), Y2(j)), cA_i(Y2(j), X2(j))) \tag{22}$$

where *Hamd*() is to calculate the Hamming distance. Define CR = 0.25, so $2m = (n/2)$.

**Step 3:** According to Eq. (23), embed the authentication information $A_{Ui}$ of $1\times(n/2)$ into the lowest bit of the first column element of the low-frequency component $cV_i$ of $(n/2)\times(n/2)$ to obtain $cV_i^{'}$, $i = 1, 2, \ldots, k$, $j = 1, 2, \ldots, n/2$.

$$cV_i^{'}\left(j, 1\right) = \left\lfloor \frac{cV_i(j, 1)}{2} \right\rfloor \times 2 + A_{Ui}(j) \tag{23}$$

where $\lfloor\cdot\rfloor$ means round down.

**Step 4:** As shown in Eq. (24), use the shadow images $C_i$ of $(2m)\times(n/2)$ to replace the high-frequency components $cD_i$, and perform inverse IWT on the components $cV_i^{'}$, $cA_i$, $cH_i$, and $C_i$ of $(n/2)\times(n/2)$, and obtain the $n \times n$ visually secure cipher image $V_i$, $i = 1, 2, \ldots, k$.

$$V_i = Iiwt\left(cA_i, cH_i, cV_i^{'}, C_i, wname\right) \tag{24}$$

where $2m = (n/2)$.

### 3.2. Decryption scheme

The decryption scheme is the inverse of the image encryption scheme. It consists of three stages: cipher image and authentication information extraction and authentication, secret image recovery, and reconstructed image generation. Before decryption, parameter keys such as chaotic system parameters $x_0$, $y_0$, $a_0$, $b_0$, $z_0$ and $u_0$, CR, wavelet transform type *wname*, SIS private key *qi*, matrix minimum values $Min_{RH}$, $Min_{RV}$, $Min_{RD}$, $MinS_i^{'}$ and other parameters need to be passed to the receiver for decryption operation, $i = 1, 2, \ldots, k$. The decryption process is shown in Fig. 6.

#### 3.2.1. Extraction and authentication of the cipher image and authentication information

Suppose that any $f$ images are selected from $k$ visually secure cipher images $V_i$ of size $n \times n$ to extract cipher image and authentication information, and then, authentication operation is performed on them to find lossless cipher images, $i = 1, 2, \ldots, k$, $t \le f \le k$. Specific steps are as follows:

**Step 1:** According to Eqs. (25) and (26), perform IWT on the $f$ visually secure cipher images to obtain the components $eA_j$, $eH_j$, $eV_j$ and $eS_j$ of $(n/2)\times (n/2)$, Then, the authentication information $eA_{Uj}$ of $1 \times (n/2)$ is extracted from the lowest bit of the element in the first column of components $eV_j$. Among them, the component $eS_j$ is the cipher information extracted from each visually secure cipher image, $i = 1, 2, \ldots, n / 2$, and $j = 1, 2, \ldots, f$.

$$\left[eA_j, eH_j, eV_j, eS_j\right] = iwt\left(V_j, wname\right) \tag{25}$$

$$eA_{Uj}(i) = eV_j\left(i, 1\right) mod 2 \tag{26}$$

**Step 2:** According to Step 2 of Section 3.1.1 of the encryption scheme, iterate the 2D-LICMS to obtain $1 \times (n/8)$ index sequences $X2_A$, $Y2A$, respectively.

**Step 3:** According to Step 2 of Section 3.1.3 of the encryption scheme, use index sequences $X2_A$ and $Y2A$, low-frequency components $eA_j$ and cipher data $eS_j$ to generate the binary verification information $eA_{Gj}$ sized of $1 \times (n/2)$, $j = 1, 2, \ldots, f$.

**Step 4:** Compare the authentication information $eA_{Uj}$ and verification information $eA_{Gj}$ of $1 \times (n/2)$. If they have the same data, the authentication is considered successful, otherwise, it fails. If no less than $t$ pieces of authentication information pass the authentication, it means that the corresponding cipher data is correct, and the next step of the decryption operation can be continued; otherwise, the number of cipher information that has passed the authentication does not meet the minimum decryption requirements, and the program stops and exits here, $j = 1, 2, \ldots, f$.

#### 3.2.2. Recovery of the secret image

**Step 1:** As shown in Eq. (27), adjust the size of $g$ cipher information $eS_i$ that has passed the authentication to obtain matrices $S_i$ of $m\times n$, $t \le g \le f$, $i = 1, 2, \ldots, g$.

$$S_i = reshape(eS_i, m, n) \tag{27}$$

**Step 2:** According to Eqs. (28) and (29), add the $m\times n$ matrices $S_i$ and the minimum values $MinS_i^{'}$ to obtain the matrices $D_i$, and then perform the IWT on the $m\times n$ matrices $D_i$ to obtain $(m/2)\times (n/2)$ components $dA_i$, $dH_i$, $dV_i$ and $dD_i$, $i = 1, 2, \ldots, g$.

$$D_i = eS_i + MinS_i^{'} - 1 \tag{28}$$

$$[dA_i, dH_i, dV_i, dD_i] = iwt(D_i, wname) \tag{29}$$

**Step 3:** According to Eqs. (30) and (31), using the components $dA_i$, $dH_i$, $dV_i$ and $dD_i$ of $(m/2)\times (n/2)$, the private key $q_i$ is calculated according to the solution process of the congruence equation set in Section 2.3, and $(m/2)\times (n/2)$ matrices $dA$, $dH$, $dV$ and $dD$ are

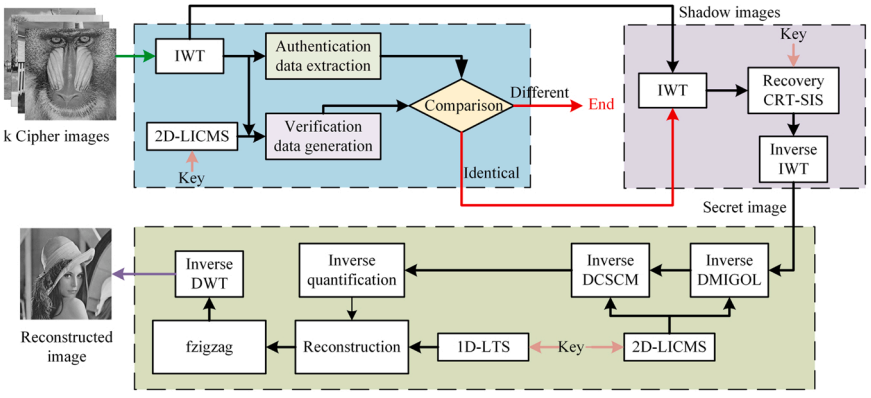


**Fig. 6.** The framework of the proposed decryption scheme.

obtained. And then, add $dH$, $dV$, $dD$, and the minimum values $Min_{RH}$, $Min_{RV}$ and $Min_{RD}$ to obtain $(m/2)\times(n/2)$ matrices $dH^{'}$, $dV^{'}$ and $dD^{'}$, respectively. $i = 1, 2, \ldots, g$.

$$[dA, dH, dV, dD] = Rcrt(dA_i, dH_i, dV_i, dD_i, qi) \tag{30}$$

$$\begin{cases} dH^{'} = dH + Min_{RH} - 1 \\ dV^{'} = dV + Min_{RV} - 1 \\ dD^{'} = dD + Min_{RD} - 1 \end{cases} \tag{31}$$

where $Rcrt()$ is the secret image recovery function.

**Step 4:** As shown in Eq. (32), perform inverse IWT on the $(m/2)\times(n/2)$ matrices $dA$, $dH^{'}$, $dV^{'}$ and $dD^{'}$ to obtain the $m\times n$ secret image $S$.

$$S = Iiwt(dA, dH^{'}, dV^{'}, dD^{'}, wname) \tag{32}$$

### 3.2.3. Generation of the reconstructed image

**Step 1:** According to Step 2 of Section 3.1.1 of the encryption scheme, iterate the 2D-LICMS to obtain the sequences $X1_A$, $Y1_A$ sized of $1\times mn$.

**Step 2:** According to Step 6 of Section 3.1.1 of the encryption scheme and Algorithm 2, the $m\times n$ matrix $S_1$ is obtained by manipulate inverse DMIGOL on the $m\times n$ secret image $S$ using the sequences $X1_A$, $Y1_A$ of $1\times mn$, and the evolution times $g$.

**Step 3:** According to Step 5 of Section 3.1.1 of the encryption scheme and Algorithm 1, use the $1\times mn$ sequences $X1_A$ and $Y1_A$ to perform inverse DCSCM on the $m\times n$ matrix $S_1$ to obtain $m\times n$ matrix $S_2$.

**Step 4:** According to Step 3 of Section 3.1.1 of the encryption scheme, iterate the 1D-LTS to generate $m\times n$ measurement matrix $\Phi 1$.

**Step 5:** According to Eqs. (33)-(36), the inverse quantization process is performed on the $m\times n$ matrix $S_2$ to obtain the matrix $S_3$, and then, $m\times n$ measurement matrix $\Phi 1$ is used to reconstruct the matrix $S_3$ using the $ONSL_0$ method to obtain matrix $S_4$ of $n\times n$. Next, use inverse zigzag scrambling on the matrix $S_4$ of $n\times n$ to find the matrix $S_5$. Finally, perform the inverse DWT on the matrix $S_5$ to obtain the reconstructed image $C$ of $n\times n$.

$$S_3 = mapminmax(reverse, (S_2/255)) \tag{33}$$

$$S_4 = ONSL_0(S_3, \Phi 1) \tag{34}$$

$$S_5 = fzigzag\left(S_4, A_{zigzag}, B_{zigzag}\right) \tag{35}$$

$$C = Idwt(S_5, wname) \tag{36}$$

where $mapminmax(reverse, A)$ is the inverse quantization operation of matrix $A$, $ONSL_0$ is the image reconstruction method, $fzigzag()$ is the inverse zigzag scramble, and $Idwt$ is inverse DWT.

## 4. Simulation results and performance analyses

In this section, the proposed image encryption scheme is experimentally assessed in terms of encryption and decryption effect, sensitivity, security, and operation efficiency. At the same time, it is compared with some of the state-of-the-art schemes. In the experiments, the 64-bit Windows computer with an i7–2.80 GHz CPU and 16 G memory is used, and the software is Matlab2017b.

### 4.1. Analysis of simulation results

The 512 × 512 plain image "Lena" is encrypted and decrypted using the proposed algorithm, and the 512 × 512 "Boat", "House", "Lighthouse" and "Baboon" are used as carrier images. In this case, the CR= 0.25, the secret sharing scheme (3, 4), and the reconstruction method is $ONSL_0$. As can be seen from Fig. 7, the plain image "Lena" in Fig. 7(a) is compressed and encrypted to obtain the secret image shown in Fig. 7(c), which is easy to attract attention in the transmission and storage process due to its noise-like appearance. The secret image is shared and then embedded in different carrier images shown in Fig. 7(d)-(g) to obtain visually secure cipher images shown in Fig. 7(h)-(k). It can be seen that the obtained cipher images are visually indistinguishable from the original carrier images and do not easily attract attention, reflecting the strong concealment of cipher information of the proposed algorithm. The reconstructed image in Fig. 7(l) has a good visual effect and can meet practical human needs, reflecting the good effect of our image reconstruction.

### 4.2. Visual quality analysis

The 512 × 512 plain image "Lena" is encrypted and embedded in the same carrier images and different carrier images of the same size, and the peak signal-to-noise ratio (PSNR) and structural similarity index measurement (SSIM) are used to evaluate the visual quality of the obtained image. Among them, PSNR is one of the most commonly used objective evaluation indicators of image quality

[32]. It is often used to judge the quality of the decrypted image. Here, it is used to evaluate the visually quality of the visual security cipher image. The larger the PSNR value, the more similar the visual security of cipher image is to that of the original carrier image, the better the cipher data is hidden, and the less likely it is to be discovered. SSIM is an index to measure the similarity of two images. The larger the SSIM value, the more similar the two images; on the contrary, the two images are not related. PSNR and SSIM are calculated according to Eqs. (37)-(39) [33]:

$$MSE = \frac{1}{m \times n}\sum_{i=1}^{m}\sum_{j=1}^{n}[X(i,j) - Y(i,j)]^2 \tag{37}$$

$$PSNR = 10 \times \log_{10}\frac{255 \times 255}{\sqrt{MSE}} \tag{38}$$

$$\begin{cases} L\left(X,Y\right) = \dfrac{2\mu_X\mu_Y + c_1}{\mu_X^2 + \mu_Y^2 + c_1} \\ C\left(X,Y\right) = \dfrac{2\sigma_X\sigma_Y + c_2}{\sigma_X^2 + \sigma_Y^2 + c_2} \\ S\left(X,Y\right) = \dfrac{\sigma_{XY} + c_3}{\sigma_X\sigma_Y + c_3} \\ SSIM(X,Y) = L(X,Y) \times C(X,Y) \times S(X,Y) \end{cases} \tag{39}$$

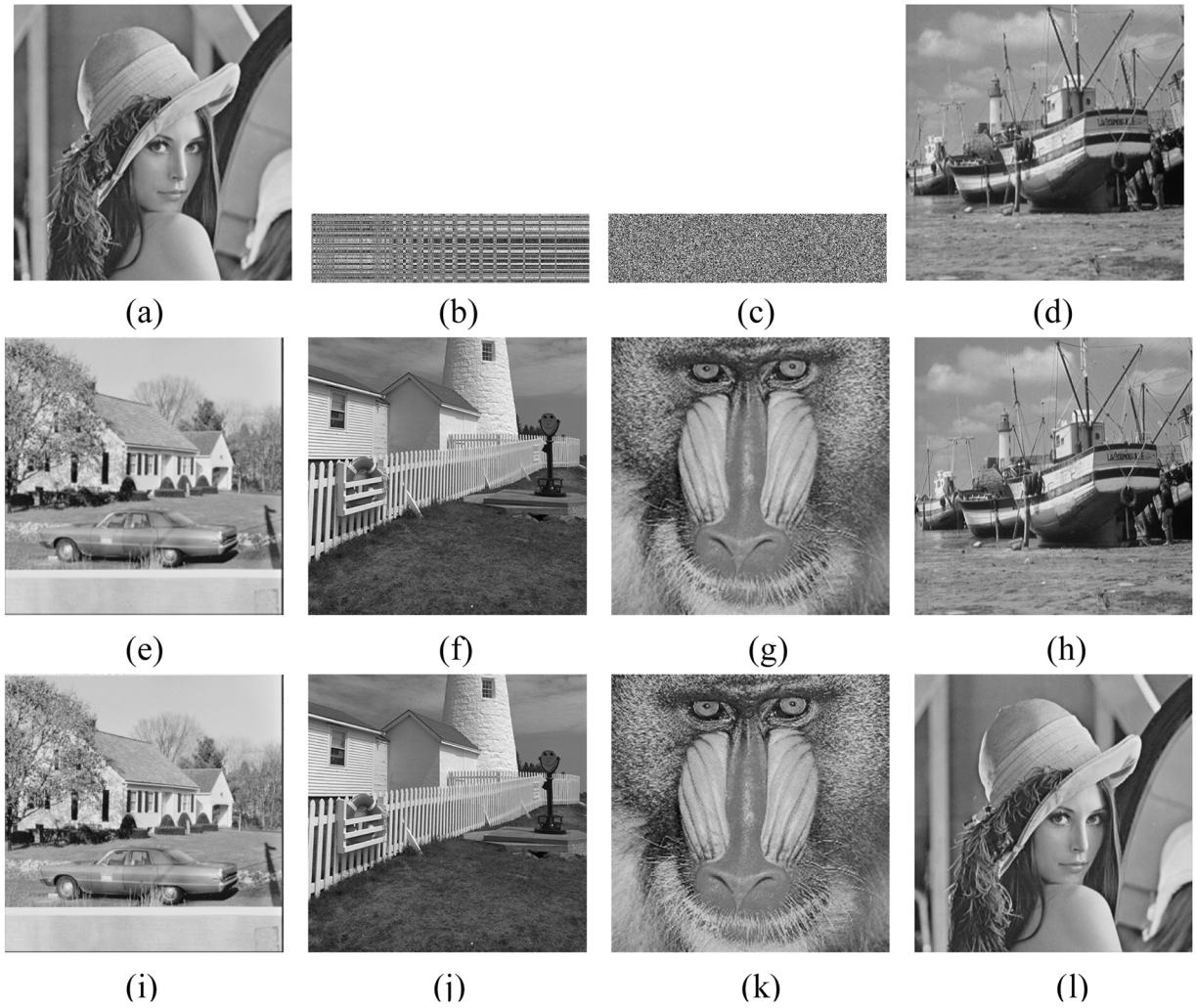


**Fig. 7.** Different carrier images encryption effect. (a) plain image, (b) compressed image, (c) secret image, (d)-(g) carrier images "Boat", "House", "Lighthouse" and "Baboon", (h)-(k) cipher images, (l) reconstructed image.

where $m$ and $n$ denote the size of image, $X(i, j)$, $Y(i, j)$ represent two different images, respectively.$\mu_X$and$\mu_Y$are the mean values of $X$ and $Y$, respectively.$\sigma_X$and$\sigma_Y$are the variances of $X$ and $Y$, respectively.$\sigma_{XY}$is the covariance of $X$ and $Y$, and$c_1$,$c_2$,$c_3$are constants.

Here, seven different plain images of 512 × 512 are encrypted separately and then embedded into different carrier images to generate cipher images with PSNR and SSIM as shown in Table 3. As seen in Table 3, the PSNR and SSIM values of visually secure cipher images obtained by encrypting the same plain image with different carrier images are generally similar, with the PSNR value above 41 dB and the SSIM value above 0.9990. Among them, the PSNR of visually secure cipher image 4 with plain image "Jetplane" is the largest, with the value of 43.3154 dB, and the PSNR of visually secure cipher image 3 with plain image "Jetplane" is the smallest, with the value of 40.3154 dB. This shows that the visual quality of visually secure cipher image is high, the plain image is well hidden, and the proposed scheme can flexibly select different images as carrier image to embed cipher information.

### 4.3. Reconstruction quality analysis

Seven different plain images of 512 × 512 are encrypted and decrypted, and PSNR and SSIM are used to evaluate the visual quality of the reconstructed images, as shown in Table 4 below. At the same time, the relationship between different reconstructed images and different CR is analyzed, as shown in Fig. 8. In Table 4, the PSNR value of the reconstructed image is above 31 dB, and the SSIM value is above 0.9890. Among them, the reconstructed image using the "Woman" plain image has the highest PSNR and SSIM values, which are 39.3040 dB and 0.9990, respectively. As can be seen from Fig. 8, as the CR continues to increase, the PSNR and SSIM values of the reconstructed image also continue to improve. Fig. 8(a) shows that when the CR is 0.1, the maximum value of the reconstructed image is about 35 dB and the minimum value is about 28 dB. As the CR increases to 0.9, the maximum value is about 52 dB and the minimum value is about 42 dB. Among them, the growth curve of the "Woman" reconstruction image is the fastest in the early stage, and the growth curve of the "Cameraman" reconstruction image is the fastest in the last stage. Fig. 8(b) shows that as the CR continues to increase, the SSIM curve of the reconstructed image continues to increase, but the growth rate gradually decreases. When the CR is 0.9, the SSIM value approaches 1. The above results show that the visual quality of the reconstructed images gotten by our algorithm is high, which can well meet the needs of real life.

### 4.4. Analysis of CRT-SIS results

Encrypt the plain image "Lena" of 512 × 512 and share the secret image to obtain the corresponding shadow images, and then select different numbers of shadow images to restore and reconstruct the secret image to obtain the reconstructed image. The experimental results are shown in Fig. 9 and Fig. 10. Wherein, in Figs. 10, (2, 3) threshold SIS scheme is constructed, and the private keys are set as $q_1 = 29$, $q_2 = 35$ and $q_3 = 37$, respectively; in Figs. 11, (3, 4) threshold SIS scheme is constructed, and the private keys are set as $q_1 = 9$, $q_2 = 10$, $q_3 = 11$ and $q_4 = 13$, respectively. The results in Fig. 9 and Fig. 10 show that the correct reconstructed image cannot be obtained when less than $t$ shadow images participate in the restoration and reconstruction of the secret image, and the correct reconstructed image can be obtained when no less than $t$ shadow images are used for reconstruction, and the visual quality of the reconstructed image is almost not affected by the number of shadow images. This shows that the $(t, n)$ threshold sharing scheme has strong flexibility and fault tolerance when participating in multi-party transmission activities.

### 4.5. Key sensitivity analysis

Key sensitivity is one of the important indicators to evaluate the security of an image encryption algorithm. Here we use the 512 × 512 plain image "Lena" as the test image, the carrier images are "Boat", "House", "Lighthouse" and "Baboon", and the encrypted image is shown in Fig. 7. If the calculation accuracy of the computer is $10^{-14}$, each time one of the initial values of the chaotic system $x_0$, $y_0$, $z_0$ is changed, and the other two remain unchanged. The decryption results are shown in Fig. 11.

**Table 3**
Visually quality analysis results of cipher images using PSNR and SSIM.

| Plain images | Item | Cipher 1 (Boat) | Cipher 2 (House) | Cipher 3 (Lighthouse) | Cipher 4 (Baboon) |
|---|---|---|---|---|---|
| Lena | PSNR(dB) | 42.1187 | 42.7851 | 41.0523 | 43.1310 |
| | SSIM | 0.9991 | 0.9993 | 0.9991 | 0.9990 |
| Cameraman | PSNR(dB) | 42.1140 | 42.7760 | 41.0399 | 43.1138 |
| | SSIM | 0.9991 | 0.9993 | 0.9991 | 0.9990 |
| Peppers | PSNR(dB) | 42.1088 | 42.7927 | 41.0490 | 43.1299 |
| | SSIM | 0.9991 | 0.9993 | 0.9991 | 0.9990 |
| Pirate | PSNR(dB) | 42.1243 | 42.7923 | 41.0354 | 43.1451 |
| | SSIM | 0.9991 | 0.9993 | 0.9991 | 0.9990 |
| Woman | PSNR(dB) | 42.1207 | 42.7785 | 41.0377 | 43.1328 |
| | SSIM | 0.9991 | 0.9993 | 0.9991 | 0.9990 |
| Jetplane | PSNR(dB) | 42.1197 | 42.7939 | 40.9851 | 43.3154 |
| | SSIM | 0.9991 | 0.9993 | 0.9991 | 0.9991 |
| Milk | PSNR(dB) | 42.1139 | 42.7796 | 41.0468 | 43.1152 |
| | SSIM | 0.9991 | 0.9993 | 0.9991 | 0.9990 |

**Table 4**
Reconstruction quality analyses of reconstructed images using PSNR (dB) and SSIM.

| Reconstructed images | PSNR (dB) | SSIM |
|---|---|---|
| Lena | 34.3230 | 0.9948 |
| Cameraman | 35.8263 | 0.9978 |
| Peppers | 31.4843 | 0.9921 |
| Pirate | 31.6475 | 0.9902 |
| Woman | 39.3040 | 0.9990 |
| Jetplane | 31.3989 | 0.9891 |
| Milk | 35.0919 | 0.9962 |

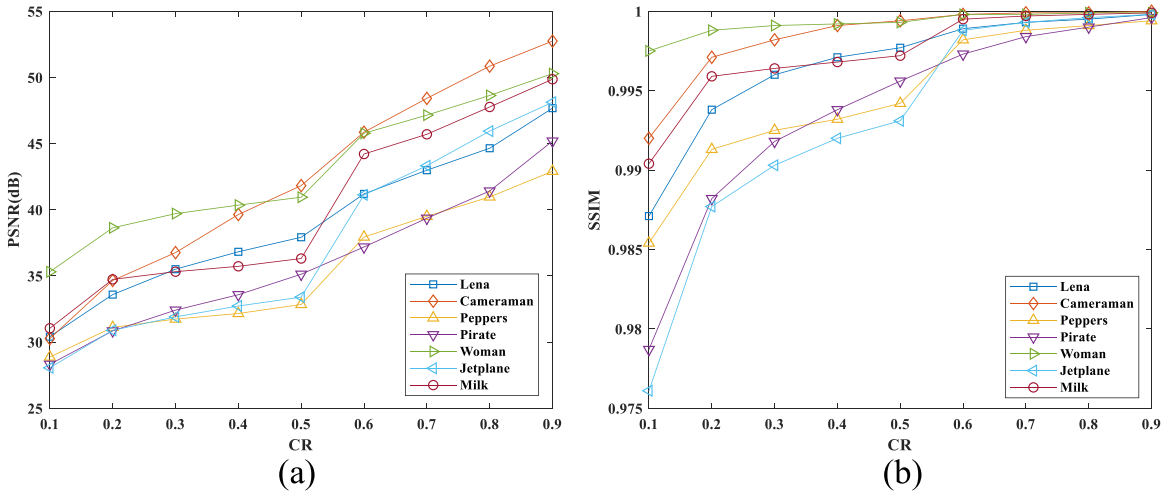


**Fig. 8.** PSNR and SSIM of different reconstructed images at different CR. (a) PSNR vs CR for different reconstructed images; (b) SSIM vs CR for different reconstructed images.

It can be seen from Fig. 11 that when the key changes slightly, it cannot be decrypted correctly, and the decrypted image is a texture-like and meaningless image. It shows that the key sensitivity of the proposed scheme is strong, and the information security of the image can be effectively protected. Besides, the number of pixel change rate (NPCR) and the unified average changing intensity (UACI) are used to evaluate the difference between the reconstructed images before and after the key is changed. The test results are shown in Table 5 below. NPCR and UACI are calculated according to Eqs. (40) and (41) [27]:

$$NPCR = \frac{\sum_{i=1}^{m}\sum_{j=1}^{n} D(i,j)}{m \times n} \times 100\% \tag{40}$$

$$UACI = \frac{1}{m \times n}\left[\sum_{i=1}^{m}\sum_{j=1}^{n} \frac{|D_1(i,j) - D_2(i,j)|}{255}\right] \times 100\% \tag{41}$$

where $m$ and $n$ are the dimensions of the image, $D_1(i, j)$ is the pixel value of the original image at.

$(i, j)$, $D_2(i, j)$ represents the pixel of the cipher image at $(i, j)$ gotten by the changed key; if $D_1(i, j) = D_2(i, j)$, then $D(i, j) = 0$, otherwise, $D(i, j) = 1$.

It can be seen from Table 5 that when the key changes slightly, 99% of the pixels of the cipher image change, and the UACI is above 33%, which is close to the ideal value. It shows that the proposed scheme has the satisfactory ability to resist differential attacks.

### 4.6. Histogram analysis

The histogram reflects the distribution of image pixel values[19]. The distribution of the histogram of the plain image is not uniform and has remarkable characteristics. The histogram distribution of the traditional noise-like encrypted image is uniform and flat; the histogram of visually secure images is similar to that of the original carrier image. Here, the plain images "Lena", "Cameraman", and "Peppers" of 512 × 512 are encrypted and decrypted, respectively, and the corresponding histograms of the plain images, secret images, and reconstructed images are shown in Fig. 12.

It can be seen from Fig. 12 that the histogram distribution of the secret image is uniform and flat, and the histogram distribution of the plain image and the reconstructed image are nearly the same. This shows that the image encryption effect of our method is good, and the reconstruction effect can meet some practical applications.

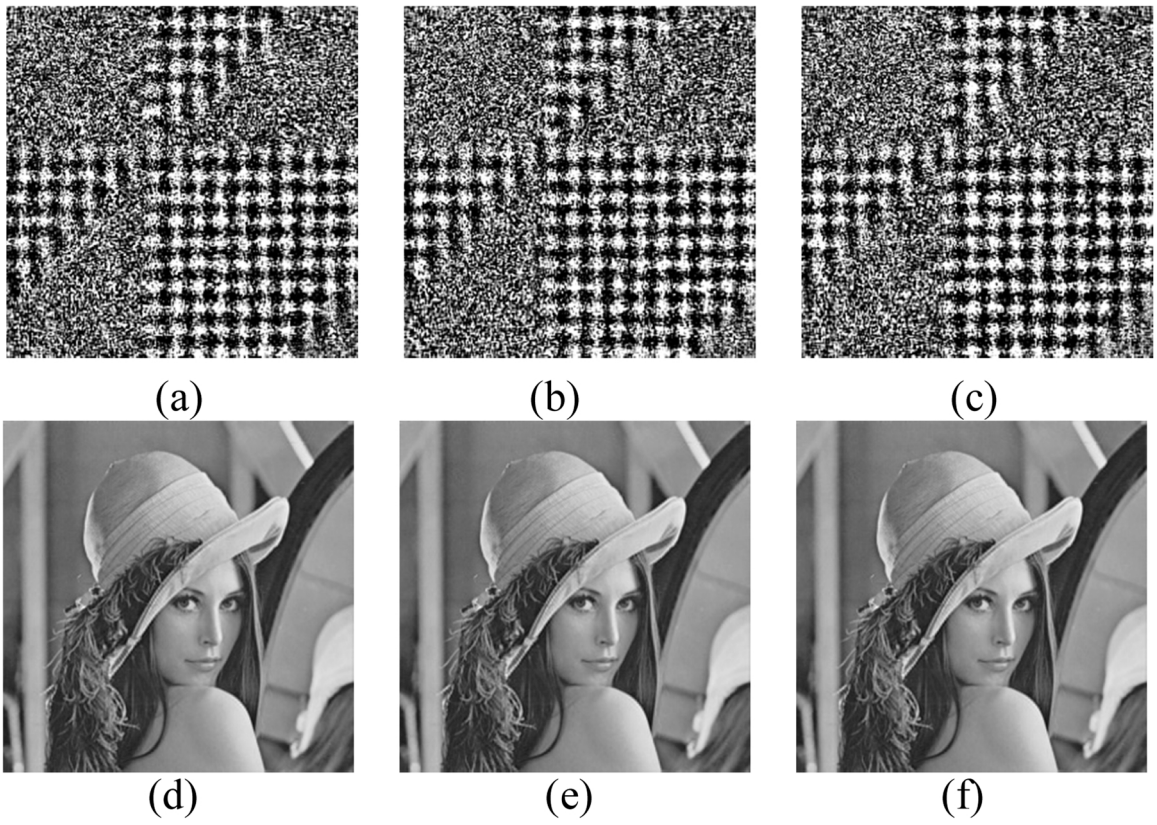


**Fig. 9.** Reconstructed images in (2,3) threshold. (a) reconstructed image using shadow image 1; (b) reconstructed image using shadow image 2; (c) reconstructed image using shadow image 3; (d) reconstructed image using shadow images 1 and 2; (e) reconstructed image using shadow images 1 and 3; (f) reconstructed image using shadow images 1,2 and 3.

### 4.7. Correlation analysis of adjacent pixels

The 512 × 512 plain image "Lena" is encrypted and decrypted, and its plain image, secret image, and reconstructed image are tested for the distribution of adjacent pixel pairs in the horizontal, vertical, and diagonal directions, as shown in Fig. 13. It can be found that the pixel distribution of the plain image and the reconstructed image is similar, and the pixel distribution of the secret image is uniform, which shows that our scheme effectively reduces the correlation between the adjacent pixels of the secret image.

According to Eq. (42)[34], calculate the correlation coefficients of plain images of 512 × 512 and their corresponding secret images and reconstructed images in the horizontal, vertical and diagonal directions, as shown in Table 6,

$$\rho_{x,y} = \frac{\sum_{i=1}^{N}(x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\sum_{i=1}^{N}(x_i - \bar{x})^2} \times \sqrt{\sum_{i=1}^{N}(y_i - \bar{y})^2}} \tag{42}$$

where $N$ is the number of image pixels, $x_i$ and $y_i$ are the pixel values of adjacent pixels in the image, $\bar{x}$and$\bar{y}$are the mean of two adjacent pixels.

As shown in Table 6, it is found that the correlation coefficient between the plain images and their corresponding reconstructed images is close, and the value is close to the theoretical value of 1. The correlation coefficient value of the secret images is close to 0, indicating that the correlation coefficient of the adjacent pixels of the secret images is weak, indicating that this scheme can effectively resist statistical analysis.

### 4.8. Information entropy

Information entropy is used to measure the uncertainty of information. For a grayscale image with 256 gray levels, the ideal information entropy is 8. The image information entropy is calculated according to Eq. (43)[35],

$$H(s) = -\sum_{i=0}^{2^{k-1}} \nu(s_i)\log_2\nu(s_i) \tag{43}$$

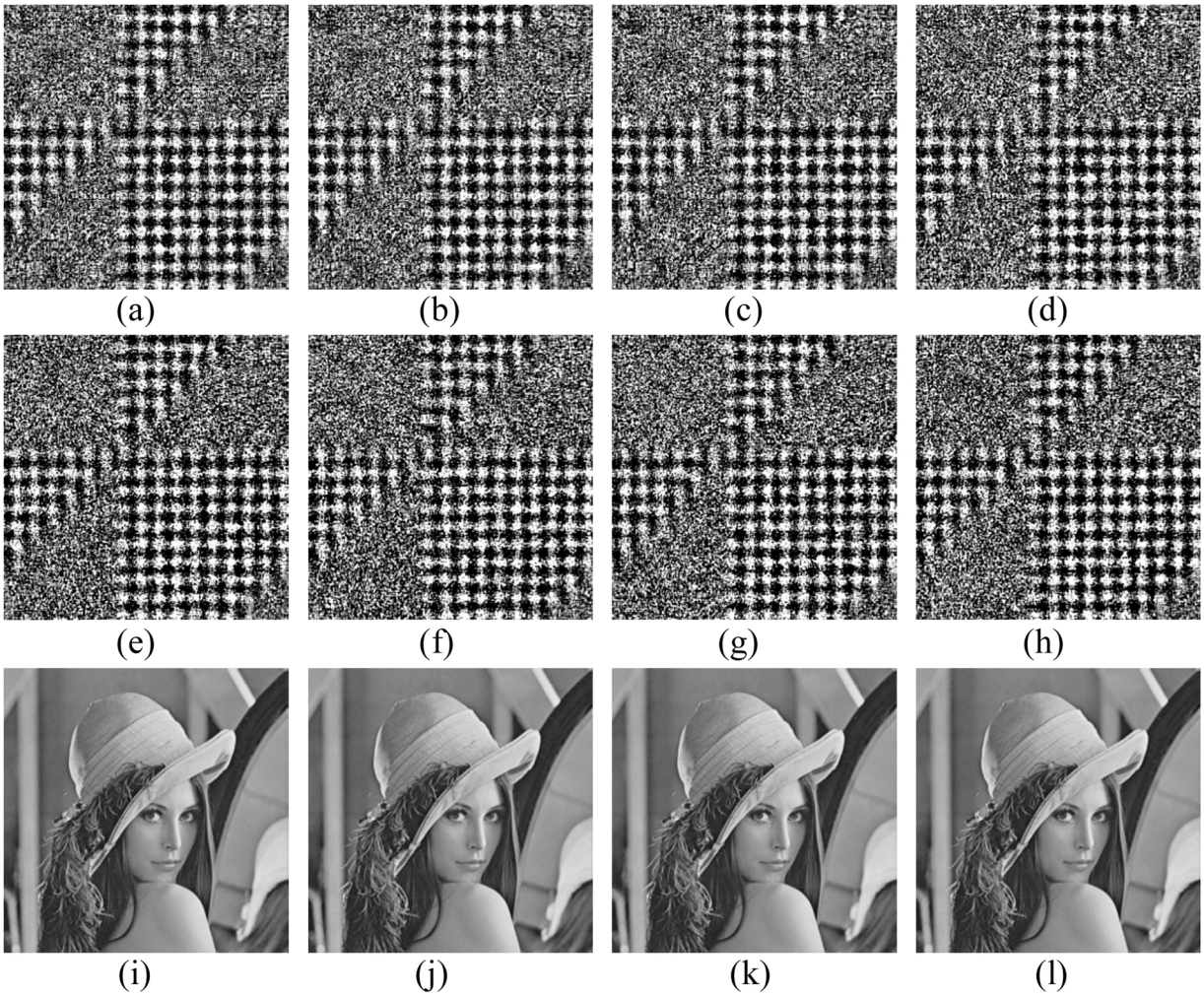


**Fig. 10.** Reconstructed images in (3,4) threshold. (a) reconstructed using shadow image 1; (b) reconstructed result using shadow image 2; (c) reconstructed result using shadow image 3; (d) reconstructed result using shadow image 4; (e) reconstructed result using shadow images 1 and 2; (f) reconstructed result using shadow images 1 and 3; (g) reconstructed result using shadow images 2 and 3; (h) reconstructed result using shadow images 3 and 4; (i) reconstructed result using shadow image 1, 2 and 3; (j) reconstructed result using shadow images 1, 2 and 4; (k) reconstructed result using shadow images 2, 3 and 4 (l) reconstructed result using shadow image 1, 2, 3 and 4.

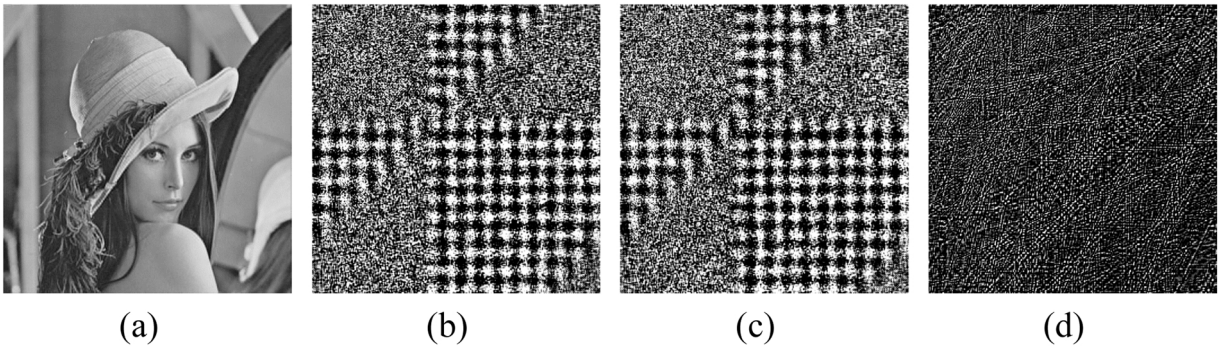


**Fig. 11.** Key sensitivity analyses in decryption process: (a) correct Key; (b) $x_0 + 10^{-14}$; (c) $y_0 + 10^{-14}$; (d) $z_0 + 10^{-14}$.

**Table 5**
NPCR and UACI after minor key change.

| Key | NPCR | UACI |
|---|---|---|
| $x_0 + 10^{-14}$ | 99.6078% | 33.4825% |
| $y_0 + 10^{-14}$ | 99.6292% | 33.6702% |
| $z_0 + 10^{-14}$ | 99.6063% | 33.5270% |

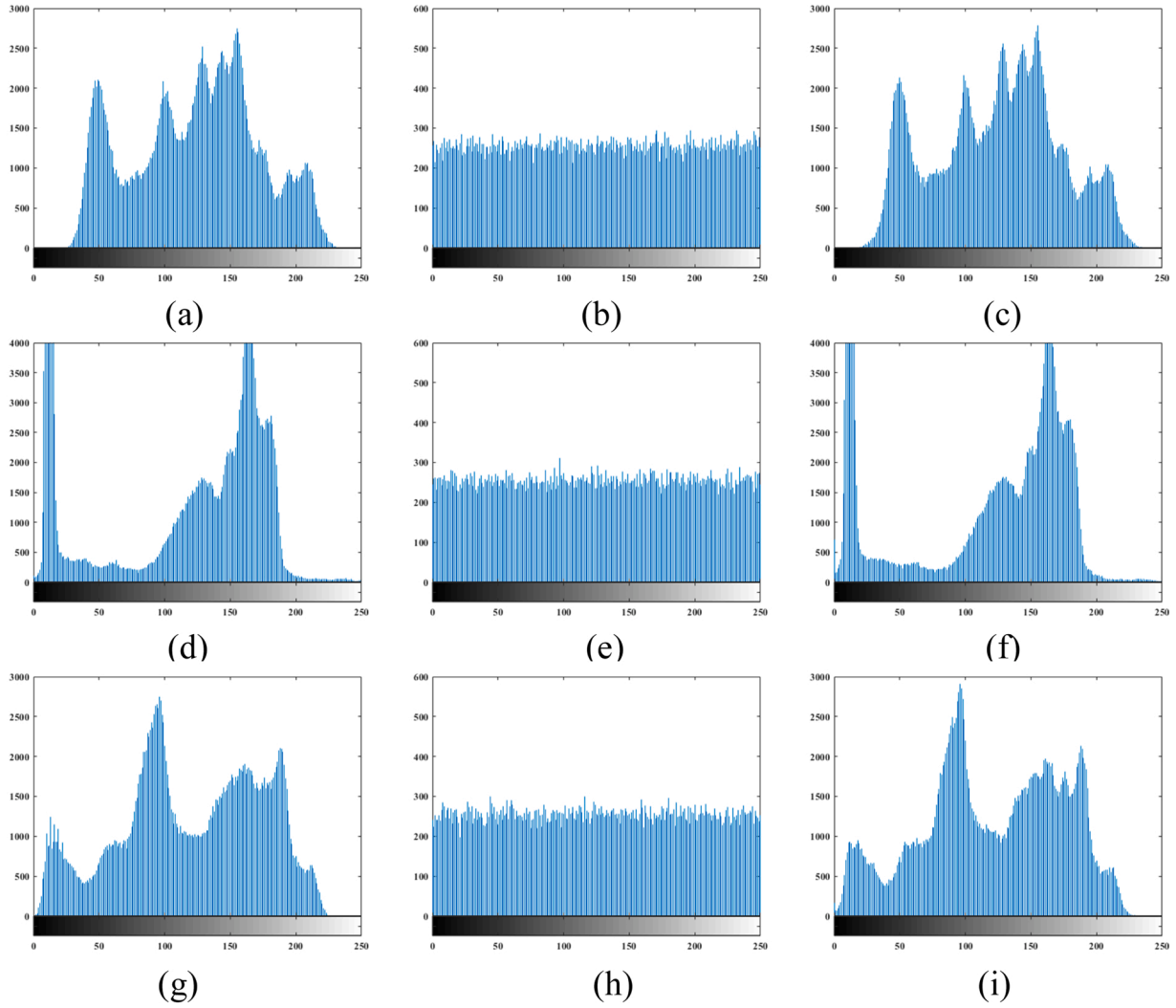


**Fig. 12.** Histogram analyses results: (a) the histogram of the plain image "Lena"; (b) the histogram of the secret image "Lena"; (c) the histogram of the reconstructed image "Lena"; (d) the histogram of the plain image "Cameraman"; (e) the histogram of the secret image "Cameraman"; (f) the histogram of the reconstructed image "Cameraman"; (g) the histogram of the plain image "Peppers"; (h) the histogram of the secret image "Peppers"; (i) the histogram of the reconstructed image "Peppers".

where $\nu(s_i)$ represents the probability of occurrence of $s_i$, and $k$ is the total number of bits of $s_i$.

Different plain images sized of $512 \times 512$ are encrypted and decrypted by our scheme, and the information entropy of the plain images, secret images, and reconstructed images are calculated and listed in Table 7. It can be seen that the information entropy of the plain images and the reconstructed images are very close, and the information entropy of the secret image is above 7.99, which is close to the ideal value. It shows that this scheme has better security.

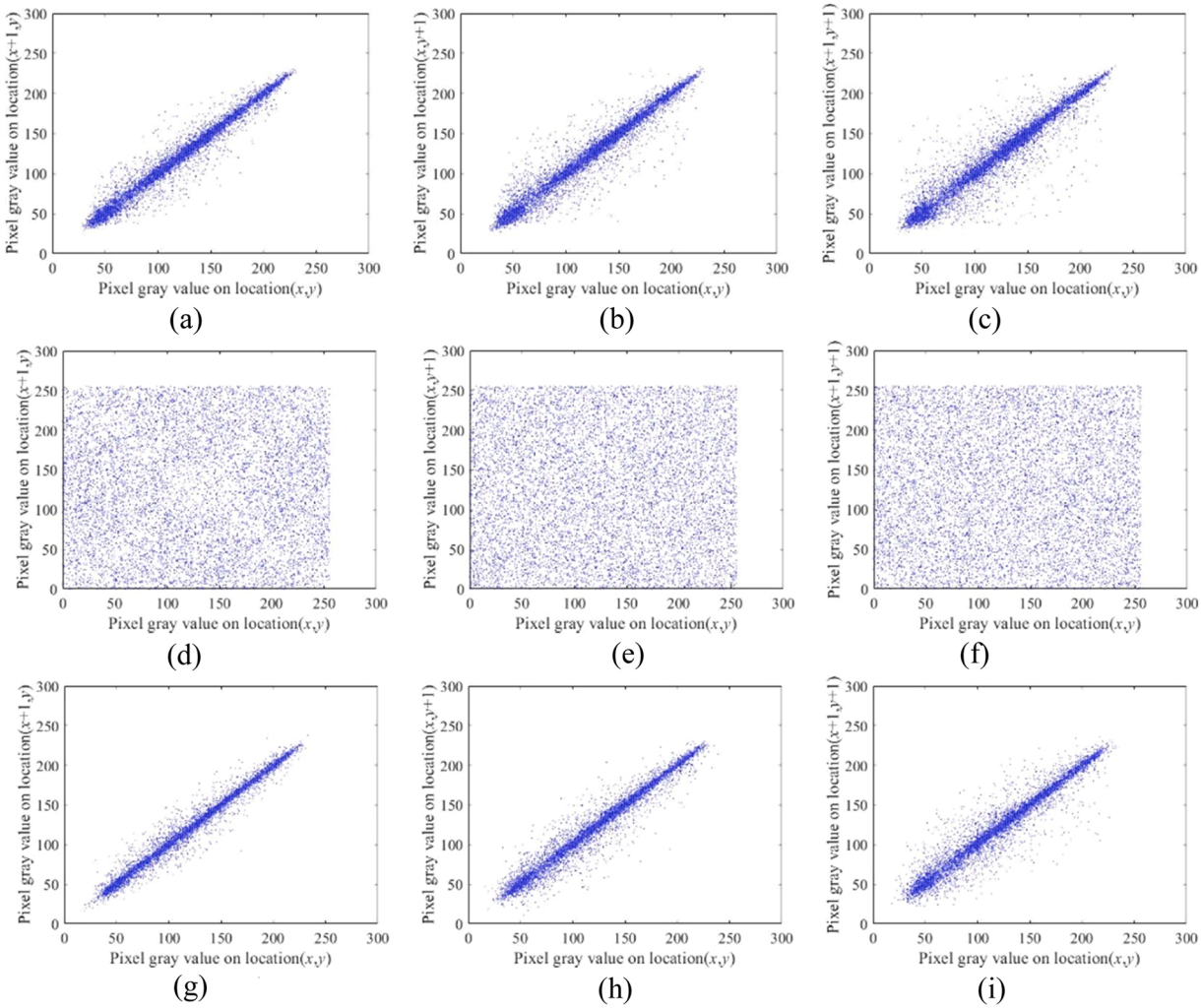


**Fig. 13.** Pixels correlation distribution analyses: (a)-(c) plain image "Lena" in horizontal, vertical, and diagonal directions; (d)-(f) secret image "Lena" in horizontal, vertical, and diagonal directions; (g)-(i) reconstructed image "Lena" in horizontal, vertical, and diagonal directions.

### *4.9. Authentication effect analysis*

Authentication refers to a function used in image transmission and storage to detect whether image information has been tampered with or not. By adding an authentication function to the image encryption scheme, no tampered and tampered images can be effectively detected and identified in the decryption scheme, avoiding decryption failures and excessive resource consumption due to information changes. The proposed scheme obtains 256-bit authentication information by solving the Hamming distance between the shadow image and the carrier image; and then, embeds it and the shadow image into the high-frequency component of the carrier image at the same time. When the visually secure cipher image needs to be received or decrypted, authentication information can be extracted from it, and then verification information can be generated using the shadow image and the low-frequency component of the carrier image. If the content of the authentication information and verification information is the same, the authentication is passed, and users can continue to perform the next step. Otherwise, the program will stop running. In short, by using the authentication function, incorrect decryption operations can be avoided, and the influence of the tampered image can be eliminated. With the ($t$, $n$) threshold scheme, the scheme can have certain fault tolerance and strong robustness.

### *4.10. Running efficiency analysis*

Running efficiency is an important index to evaluate the performance of the image encryption scheme. Calculate the encryption time and decryption time of different plain images of 512 × 512, as shown in Table 8. At the same time, according to the average encryption and decryption time in Table 8, the time distribution diagram of this scheme in different stages is drawn in Fig. 14.

It can be seen from Table 8 that the average encryption time of this scheme is 1.4487 *s*, the average decryption time is 4.1230 *s*, and

**Table 6**
Correlation coefficients of adjacent pixels.

| Images | Item | Horizontal | Vertical | Diagonal |
|---|---|---|---|---|
| Lena | Plain image | 0.9846 | 0.9736 | 0.9613 |
| | Secret image | 0.0140 | 0.0062 | -0.0257 |
| | Reconstructed image | 0.9901 | 0.9797 | 0.9675 |
| Cameraman | Plain image | 0.9899 | 0.9834 | 0.9726 |
| | Secret image | 0.0169 | 0.0119 | 0.0085 |
| | Reconstructed image | 0.9901 | 0.9847 | 0.9746 |
| Peppers | Plain image | 0.9772 | 0.9777 | 0.9628 |
| | Secret image | 0.0268 | -0.0109 | -0.0006 |
| | Reconstructed image | 0.9899 | 0.9874 | 0.9769 |
| Pirate | Plain image | 0.9702 | 0.9622 | 0.9451 |
| | Secret image | 0.0070 | -0.0103 | -0.0040 |
| | Reconstructed image | 0.9824 | 0.9764 | 0.9599 |
| Woman | Plain image | 0.9968 | 0.9964 | 0.9947 |
| | Secret image | 0.0135 | -0.0087 | -0.0021 |
| | Reconstructed image | 0.9973 | 0.9971 | 0.9949 |
| Jetplane | Plain image | 0.9650 | 0.9699 | 0.9405 |
| | Secret image | -0.0254 | -0.0039 | 0.0110 |
| | Reconstructed image | 0.9747 | 0.9774 | 0.9541 |
| Milk | Plain image | 0.9919 | 0.9855 | 0.9791 |
| | Secret image | -0.0451 | -0.0057 | -0.0098 |
| | Reconstructed image | 0.9939 | 0.9893 | 0.9841 |

**Table 7**
The information entropy of different images.

| Images | Plain image | Secret image | Reconstructed image |
|---|---|---|---|
| Lena | 7.4451 | 7.9973 | 7.4551 |
| Cameraman | 7.0480 | 7.9975 | 7.0848 |
| Peppers | 7.5937 | 7.9971 | 7.5976 |
| Pirate | 7.2367 | 7.9970 | 7.3431 |
| Woman | 7.2767 | 7.9969 | 7.2878 |
| Jetplane | 6.7025 | 7.9978 | 6.7815 |
| Milk | 7.2533 | 7.9974 | 7.2715 |

the time consumed by different images is not much different, which shows that the running time is less affected by the image size. Besides, it can be seen from Fig. 14(a) that among the time consumption of different encryption stages, 55% is for confusion and diffusion, 19% for data embedding, and 11% for chaotic sequences generation. The confusion and diffusion processes consume the largest proportion of time because each pixel needs to be processed, making the process consume too much time. In Fig. 14(b), for the decryption stage time proportion, 66% is for reconstruction, 20% for inverse confusion and inverse diffusion, and 6% for secret image recovery. The long decryption time is mainly due to the need for reconstruction. From the practical application point of view, this scheme can be applied for some real-time communications.

### *4.11. Comparison with other schemes*

In order to demonstrate the advantages of this scheme, it is compared with some state-of-the-art schemes. The visual quality of the reconstructed image under different CR, the visual quality of the visually secure cipher image, and the advantages and disadvantages of the SIS function are compared. To provide a relatively fair comparison environment, the comparison data is obtained from the relevant comparison scheme.

In Table 9, different plain images of $512 \times 512$ are encrypted and decrypted. It can be seen that under different CR, the reconstructed image quality of this scheme is better than[36], and with the continuous increase of the CR, the PSNR value of the reconstructed image continues to increase. At the same time, the visual quality of the cipher image of this scheme and other schemes is compared. In Table 10, the visual quality of the cipher image gotten by our scheme is better than that of[36–39], and its PSNR value is above 42 dB. In addition, this paper also compares the differences between this scheme and related SIS schemes, and the comparison results are listed in Table 11. It can be seen that the proposed scheme has many merits, such as visually meaningful cipher image, lossless recovery of secret image, and authentication capability. But compared with[37,40], it cannot losslessly recover carrier image, which is an area that needs to be improved in the future. The above results show that this scheme has the advantages of the better visual quality of reconstructed image and cipher image, and the secret image sharing function basically satisfies the user's needs.

**Table 8**
The encryption and decryption time(s) for different plain images.

| Images | Encryption time (s) | Decryption time (s) | Total (s) |
|---|---|---|---|
| Lena | 1.5174 | 4.1233 | 5.6407 |
| Cameraman | 1.4386 | 4.0644 | 5.5030 |
| Peppers | 1.5095 | 4.2093 | 5.7188 |
| Pirate | 1.4934 | 4.2033 | 5.6967 |
| Woman | 1.3399 | 3.9254 | 5.2653 |
| Jetplane | 1.4181 | 4.2684 | 5.6865 |
| Milk | 1.4242 | 4.0669 | 5.4911 |
| Average | 1.4487 | 4.1230 | 5.5717 |

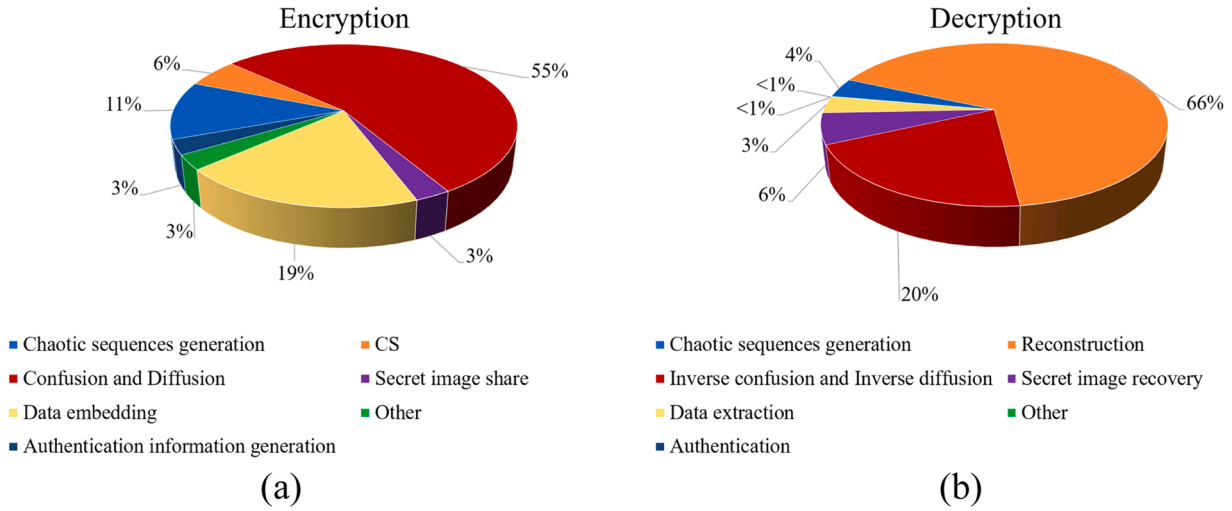


**Fig. 14.** Running times of different phases for the proposed scheme: (a) Encryption; (b) Decryption.

## 5. Discussion

In this section, we will analyze the performance of the proposed image encryption, including the reason why our scheme uses some sub-operations (e.g. CS, DCSCM, and etc.) and why not more loops.

First, to illustrate the importance of these sub-operations, we remove CS and DMIGOL for encryption and decryption operations, respectively. The running time and secret image histograms are shown in Fig. 15 and Fig. 16 below. We can see that the use of CS effectively improves the encryption and decryption time, especially when operating on large image sizes. In addition, the secret image histogram generated by the scheme without DMIGOL has a significant feature distribution, which will reduce the security of the algorithm and bring security risks to the image. This shows that CS can effectively reduce the size of images, reduce the time and space consumption of ciphertext images in transmission and storage, and satisfy users' needs for security and efficiency. DCSCM and DMIGOL, as the scrambling and diffusion parts of this scheme, are controlled by 2D-LICMS, which can scramble the pixel location of the image to the largest extent and change the pixel value, so as to improve the encryption effect of the image effectively. In addition, many researchers use confusion-diffusion in their encryption schemes to improve security. For example, R. Enayatifar et al.[42] used cellular automata permutation and DNA diffusion techniques to improve algorithm security. Subsequently, Wang et al.[43] introduced

**Table 9**
PSNR (dB) comparison of reconstruction images of various schemes.

| Images | CR | Ref.[36] | Ours |
|---|---|---|---|
| Lena | 0.25 | 25 | 34.3230 |
| | 0.5 | 32 | 37.9184 |
| | 0.75 | 36 | 43.9179 |
| Cameraman | 0.25 | 24 | 35.8263 |
| | 0.5 | 28 | 41.8211 |
| | 0.75 | 34 | 49.7526 |
| Peppers | 0.25 | 25 | 31.4843 |
| | 0.5 | 31 | 32.8397 |
| | 0.75 | 35 | 40.1195 |

**Table 10**
PSNR (dB) comparison of shadow images of various schemes.

| Scheme | Baboon | Lena | Peppers |
|---|---|---|---|
| Ref.[36] | 40.0880 | 39.7284 | 39.8211 |
| Ref.[37] | 40.33 | 40.32 | 40.32 |
| Ref.[38] | 41.42 | 41.21 | 40.10 |
| Ref.[39] | 41 | 41 | 41.07 |
| Ours | 44.1911 | 44.3136 | 42.3680 |

**Table 11**
Comparisons with some secret image sharing methods.

| Item | Ref.[29] | Ref.[36] | Ref.[37] | Ref.[38] | Ref.[40] | Ref.[41] | Ours |
|---|---|---|---|---|---|---|---|
| $(t, n)$ threshold | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| Meaningful shadow image | No | Yes | Yes | Yes | Yes | No | Yes |
| Lossless recovery of secret image | Yes | No | Yes | Yes | Yes | Yes | Yes |
| Lossless recovery of carrier image | No | No | Yes | No | Yes | No | No |
| Authentication ability | No | No | No | Yes | No | Yes | Yes |

chaotic systems and Boolean networks to achieve image scrambling and diffusion, thereby ensuring secure image communication. Chai et al.[24] proposed cross-component confusion and diffusion algorithm based on chaotic system control, which improves the encryption effectiveness and security of images. These show that the confusion-diffusion method is an important part of image encryption.

Secondly, the proposed confusion and diffusion methods may achieve high security. On the one hand, DCSCM and DMIGOL are directly applied for every pixel point of the image when they are used, making them participate in encryption activities as independent individuals and effectively enhancing the image encryption effect. On the other hand, this scheme can be divided into two major parts, CS-confusion-diffusion and SIS-embedding. The first one is aimed at generating secret image to effectively protect image information security; the second one secretly shares secret image and then embeds them into carrier image to generate cipher image, and achieve the visual appearance protection. To sum up, this scheme realizes the double protection of image information and appearance, which makes the cipher image have high security.

Finally, in terms of security and effectiveness, we increase the number of cycles for the DCSCM and DMIGOL stages, respectively. The information entropy of the secret image and the running time of the encryption scheme under different loop times are obtained, as shown in Fig. 17 and Fig. 18. From these figures, it can be seen that the information entropy does not change significantly as the number of loops is increased, and at the same time, the encryption time and decryption time of this scheme are gradually improved. It shows that single confusion and diffusion can encrypt image information to the maximum extent, indicating that this scheme has high security and effectiveness. Looping for some sub-operations does not bring significant safety performance improvement, and the operation efficiency gradually decreases and does not meet the practical application requirements.

Overall, our scheme has high security, effectiveness and robustness, and some sub-operations are necessary.

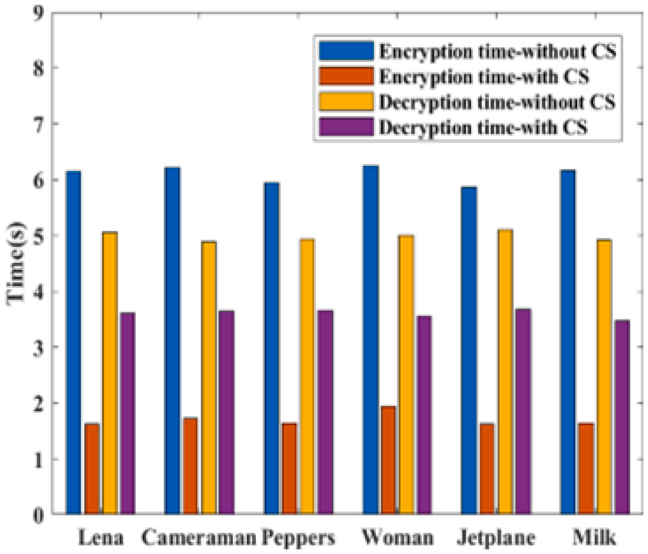


**Fig. 15.** Running times comparison with CS and without CS scheme.

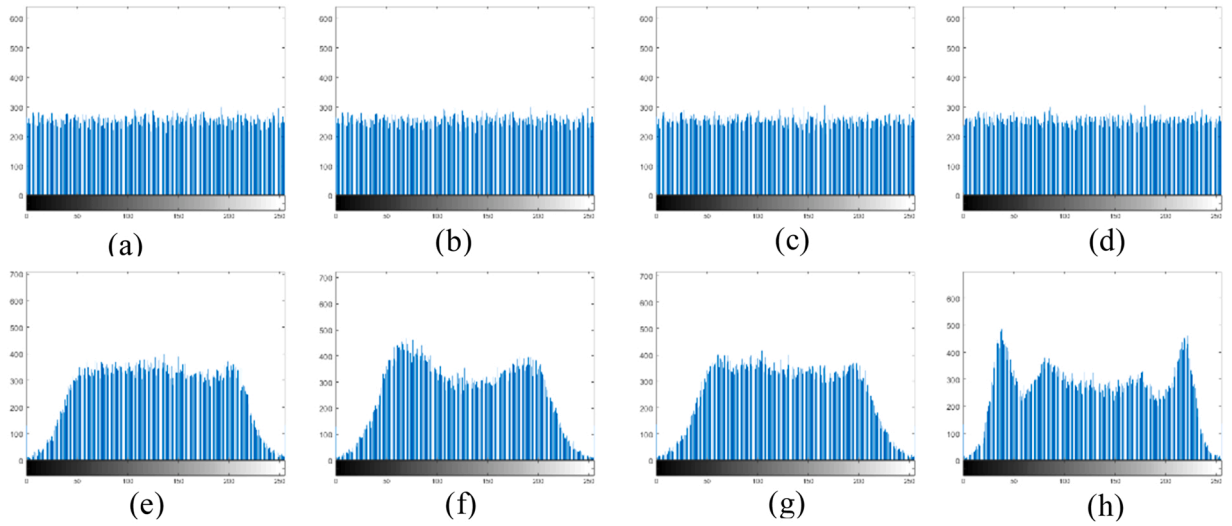


**Fig. 16.** Histogram comparison with and without DMIGOL scheme: (a)-(d) are the histograms of the secret images Lena, Cameraman, Peppers, and Woman under the proposed scheme, respectively; (e)-(h are the histograms of the secret images Lena, Cameraman, Peppers, and Woman without the DMIGOL scheme, respectively.

## 6. Conclusion

In this paper, we propose a verifiable visually meaningful image encryption based on CS and IGOL. In our work, CS is used to compress and encrypt the plain image, thus reducing the size of the image and improving the transmission efficiency. In addition, the introduction of DCSCM solves the problem of no correlation between row cyclic shift and column cyclic shift, which makes the confusing process dynamic and flexible and improves the effect of image encryption. Meanwhile, IGOL is designed and DMIGOL is used to diffuse the permutated image, thus increasing the security of the cipher image. In addition, in order to satisfy the demand for multi-party collaborative transmission and to reduce the risk of losing the cipher image and making it difficult to recover the corresponding reconstructed image, CRT-SIS is used to share the secret image to obtain multiple shadow images, which makes the proposed scheme more robust and fault-tolerant. In the decryption, the shadow images are embedded into the carrier images to obtain multiple visually secure cipher images to reduce the attention of hackers. Finally, in order to avoid illegal users from using and maliciously tampering with the cipher image, an authentication scheme is added to ensure the correct and secure use of the cipher image. The experimental results and comparative analysis show that the proposed scheme has high security, robustness, and transmission efficiency. Therefore, the proposed scheme can be applied in medical, military, and commercial fields to enable multi-user image data transmission. Such as the transmission of medical image for inter-hospital medical consultation, protection of sensitive military image, and multi-party encrypted transmission of commercially important image. However, this scheme has some problems, such as carrier image cannot

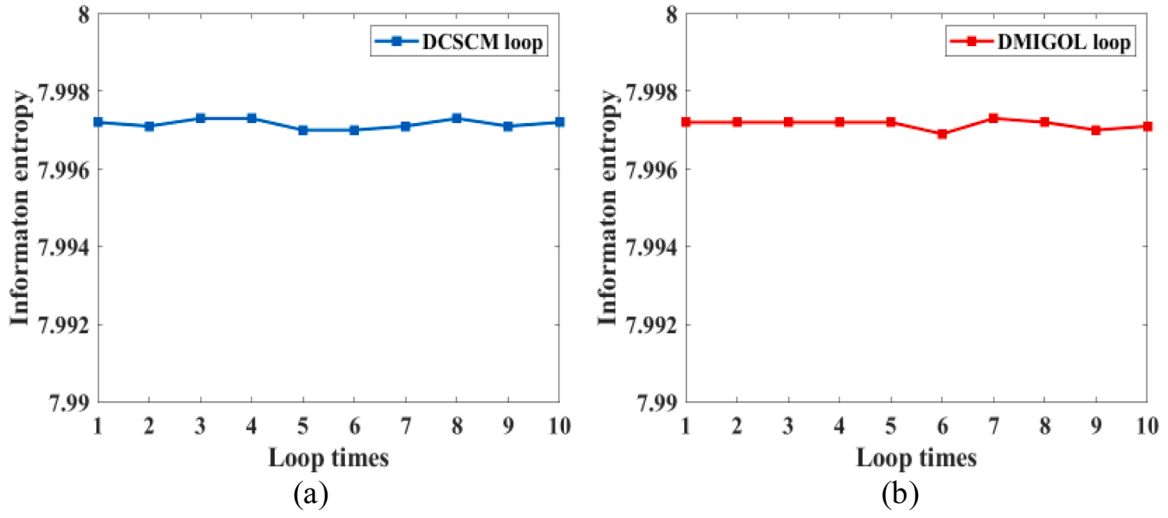


**Fig. 17.** Information entropy of secret image under different loop times: (a) DCSCM loop; (b) DMIGOL loop.

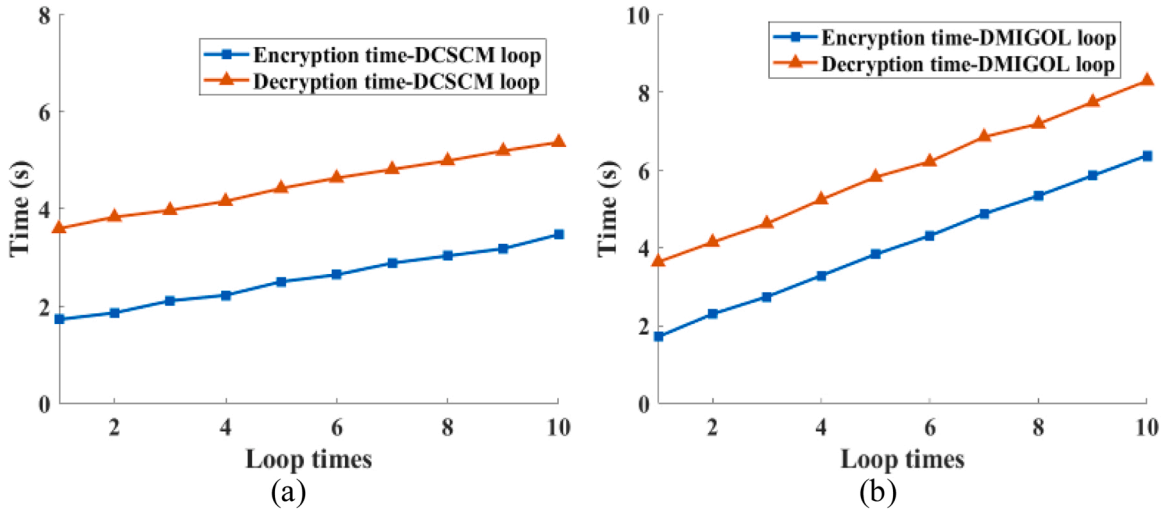


**Fig. 18.** Encryption and Decryption times under different loop times: (a) DCSCM loop; (b) DMIGOL loop.

be recovered and the running time is a bit long. In the future work, we will consider carrier image recovery, use parallel computing to improve the running speed and efficiency, and introduce techniques such as quantum computing to improve the security of the encryption scheme and effectively resist the threat of quantum computing cracking.

## 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.

## Acknowledgments

All the authors are deeply grateful to the editors for smooth and fast handling of the manuscript. The authors would also like to thank the anonymous referees for their valuable suggestions to improve the quality of this paper. This work is supported by the National Natural Science Foundation of China (Grant Nos. 61802111, 61872125, 62171114), and Open Foundation of Henan Key Laboratory of Cyberspace Situation Awareness (No. HNTS2022019).

## References

[1] X. Chai, Y. Wang, X. Chen, Z. Gan, Y. Zhang, TPE-GAN: thumbnail preserving encryption based on GAN with key, IEEE Signal Process. Lett. 29 (2022) 972–976.
[2] J.Y. Fu, Z.H. Gan, X.L. Chai, Y. Lu, Cloud-decryption-assisted image compression and encryption based on compressed sensing, Multimed. Tools Appl. 81 (2022) 17401–17436.
[3] J.W. Cheng, X.H. Yan, L.T. Liu, Y. Jiang, X. Wang, Meaningful secret image sharing with saliency detection, Entropy 24 (2022) 340.
[4] M. Kaur, V. Kumar, Adaptive differential evolution-based lorenz chaotic system for image encryption, Arab. J. Sci. Eng. 43 (2018) 8127–8144.
[5] X.H. Gao, Image encryption algorithm based on 2D hyperchaotic map, Opt. Laser Technol. 142 (2021), 107252.
[6] X. Wang, M. Zhang, An image encryption algorithm based on new chaos and diffusion values of a truth table, Inf. Sci. 579 (2021) 128–149.
[7] A. Mansouri, X.Y. Wang, A novel block-based image encryption scheme using a new Sine powered chaotic map generator, Multimed. Tools Appl. 80 (2021) 21955–21978.
[8] X.L. Chai, X.L. Fu, Z.H. Gan, Y.S. Zhang, Y. Lu, Y.R. Chen, An efficient chaos-based image compression and encryption scheme using block compressive sensing and elementary cellular automata, Neural Comput. Appl. 32 (2020) 4961–4988.
[9] Z. Li, C.G. Peng, W.J. Tan, L.R. Li, An efficient plaintext-related chaotic image encryption scheme based on compressive sensing, Sensors 21 (2021) 758.
[10] C.-C. Thien, J.-C. Lin, Secret image sharing, Comput. Graph. 26 (2002) 765–770.
[11] A. Kanso, M. Ghebleh, An efficient (t,n)-threshold secret image sharing scheme, Multimed. Tools Appl. 76 (2017) 16369–16388.
[12] X.H. Yan, Y.L. Lu, L.T. Liu, S. Wan, W.M. Ding, H.L. Liu, Chinese remainder theorem-based secret image sharing for (k, n) Threshold, Cloud Comput. Secur 10603 (2017) 433–440.
[13] M.K. Sardar, A. Adhikari, A. New Lossless Secret Image Sharing Scheme for Grayscale Images with Small Shadow Size, in: Proc. Int. Conf. Front. Comput. Syst. (2021) 701–709.
[14] A. Shamir, How to share a secret, Commun. ACM 22 (1979) 612–613.
[15] L. Bao, Y.C. Zhou, Image encryption: generating visually meaningful encrypted images, Inf. Sci. 324 (2015) 197–207.
[16] X.L. Chai, Z.H. Gan, Y.R. Chen, Y.S. Zhang, A visually secure image encryption scheme based on compressive sensing, Signal Process 134 (2017) 35–51.
[17] H. Wang, D. Xiao, M. Li, Y.P. Xiang, X.Y. Li, A visually secure image encryption scheme based on parallel compressive sensing, Signal Process 155 (2019) 218–232.
[18] Z.Y. Hua, K.Y. Zhang, Y.M. Li, Y.C. Zhou, Visually secure image encryption using adaptive-thresholding sparsification and parallel compressive sensing, Signal Process 183 (2021), 107998.
[19] Y.G. Yang, B.P. Wang, Y.L. Yang, Y.H. Zhou, W.M. Shi, X. Liao, Visually meaningful image encryption based on universal embedding model, Inf. Sci. 562 (2021) 304–324.

[20] K.S. Wang, M.Q. Liu, Z.H. Zhang, T.G. Gao, Optimized visually meaningful image embedding strategy based on compressive sensing and 2D DWT-SVD, Multimed. Tools Appl. (2022), https://doi.org/10.1007/s11042-022-12305-4.
[21] C. Cao, K.H. Sun, W.H. Liu, A novel bit-level image encryption algorithm based on 2D-LICM hyperchaotic map, Signal Process 143 (2018) 122–133.
[22] M. Gupta, K.K. Gupta, M.R. Khosravi, P.K. Shukla, S. Kautish, A. Shankar, An intelligent session key-based hybrid lightweight image encryption algorithm using logistic-tent map and crossover operator for internet of multimedia things, Wirel. Pers. Commun. 121 (2021) 1857–1878.
[23] E.J. Candes, J. Romberg, T. Tao, Robust uncertainty principles: exact signal reconstruction from highly incomplete frequency information, IEEE Trans. Inf. Theory 52 (2006) 489–509.
[24] X.L. Chai, J.Y. Fu, Z.H. Gan, Y. Lu, Y.S. Zhang, An image encryption scheme based on multi-objective optimization and block compressed sensing, Nonlinear Dyn. 108 (2022) 2671–2704.
[25] D.M. Huo, Z.L. Zhu, L.S. Wei, C. Han, X. Zhou, A visually secure image encryption scheme based on 2D compressive sensing and integer wavelet transform embedding, Opt. Commun. 492 (2021), 126976.
[26] Z.Y. Hua, Z.H. Zhu, S. Yi, Z. Zhang, H.J.A. Huang, Cross-plane colour image encryption using a two-dimensional logistic tent modular map, Inf. Sci. 546 (2021) 1063–1083.
[27] L.Y. Zhu, H.S. Song, X. Zhang, M.D. Yan, T. Zhang, X.Y. Wang, J. Xu, A robust meaningful image encryption scheme based on block compressive sensing and SVD embedding, Signal Process 175 (2020), 107629.
[28] D.H. Jiang, L.D. Liu, L.Y. Zhu, X.Y. Wang, X.W. Rong, H.X. Chai, Adaptive embedding: a novel meaningful image encryption scheme based on parallel compressive sensing and slant transform, Signal Process 188 (2021), 108220.
[29] X.H. Yan, Y.L. Lu, L.T. Liu, J.J. Liu, G.Z. Yang, Chinese remainder theorem-based two-in-one image secret sharing with three decoding options, Digit. Signal Process. 82 (2018) 80–90.
[30] Z.H. Gan, X.L. Chai, J.T. Zhang, Y.S. Zhang, Y.R. Chen, An effective image compression-encryption scheme based on compressive sensing (CS) and game of life (GOL), Neural Comput. Appl. 32 (2020) 14113–14141.
[31] X.Y. Wang, Q. Ren, D.H. Jiang, An adjustable visual image cryptosystem based on 6D hyperchaotic system and compressive sensing, Nonlinear Dyn. 104 (2021) 4543–4567.
[32] X.Y. Chen, M.L. Zou, B. Yang, Z.L. Wang, N.N. Wu, L.L. Qi, A visually secure image encryption method based on integer wavelet transform and rhombus prediction, Math. Biosci. Eng. 18 (2021) 1722–1739.
[33] L.D. Liu, D.H. Jiang, X.Y. Wang, X.W. Rong, R.X. Zhang, 2D Logistic-Adjusted-Chebyshev map for visual color image encryption, J. Inf. Secur. Appl. 60 (2021), 102854.
[34] P.K. Naskar, S. Bhattacharyya, D. Nandy, A. Chaudhuri, A robust image encryption scheme using chaotic tent map and cellular automata, Nonlinear Dyn. 100 (2020) 2877–2898.
[35] K. Jain, A. Aji, P. Krishnan, Medical image encryption scheme using multiple chaotic maps, Pattern Recognit. Lett. 152 (2021) 356–364.
[36] B. Wu, D. Xie, F.L. Chen, X.L. Wang, Y.Y. Zeng, A multi-party secure encryption-sharing hybrid scheme for image data base on compressed sensing, Digit. Signal Process. 123 (2022), 103391.
[37] P.Y. Lin, C.S. Chan, Invertible secret image sharing with steganography, Pattern Recognit. Lett. 31 (2010) 1887–1893.
[38] L.Z. Xiong, X.W. Zhong, C.N. Yang, DWT-SISA: a secure and effective discrete wavelet transform-based secret image sharing with authentication, Signal Process 173 (2020), 107571.
[39] L.Z. Xiong, X.W. Zhong, C.N. Yang, X. Han, Transform domain-based invertible and lossless secret image sharing with authentication, IEEE Trans. Inf. Forensics Secur. 16 (2021) 2912–2925.
[40] K.J. Meng, F.Y. Miao, Y. Xiong, C.C. Chang, A reversible extended secret image sharing scheme based on Chinese remainder theorem, Signal Process. Commun. 95 (2021), 116221.
[41] X.H. Yan, Y.L. Lu, C.N. Yang, X.P. Zhang, S.D. Wang, A common method of share authentication in image secret sharing, IEEE Trans. Circuits Syst. Video Technol. 31 (2021) 2896–2908.
[42] R. Enayatifar, F.G. Guimaraes, P. Siarry, Index-based permutation-diffusion in multiple-image encryption using DNA sequence, Opt. Lasers Eng. 115 (2019) 131–140.
[43] X.Y. Wang, S. Gao, Image encryption algorithm for synchronously updating Boolean networks based on matrix semi-tensor product theory, Inf. Sci. 507 (2020) 16–36.