Signal Processing 155 (2019) 218–232

Contents lists available at ScienceDirect

Signal Processing

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

A visually secure image encryption scheme based on parallel compressive sensing

Hui Wang[a], Di Xiao[a,*], Min Li[a], Yanping Xiang[a], Xinyan Li[b]

[a] Key Laboratory of Dependable Service Computing in Cyber Physical Society of Ministry of Education, College of Computer Science, Chongqing University, Chongqing 400044, China

[b] School of Mathematics and Statistics, Yangtze Normal University, Chongqing 408100, China

ARTICLE INFO

Article history:
Received 14 February 2018
Revised 22 September 2018
Accepted 1 October 2018
Available online 2 October 2018

Keywords:
Image encryption
Parallel compressive sensing
Visually secure cipher image
Discrete wavelet transform
Integer discrete wavelet transform

ABSTRACT

It is generally recognized that encrypting an original image into meaningless cipher image is an ideal method to protect image information. However, during transmission, the meaningless cipher image would draw attention and thus attract attacks. Recently, compressive sensing (CS) and carrier images have been utilized by Chai et al. to construct a novel image encryption scheme with visual security. However, in this scheme, some extra transmission is required for possible decryption besides the encrypted image. Moreover, the imperceptibility of the cipher image can be further improved and the recovered image quality would be severely degraded if unsuitable carrier images are selected. In this paper, we design a visually secure encryption scheme by using the parallel compressive sensing (PCS) counter mode and embedding technique. In order to achieve higher security level, Logistic-Tent system and 3-D Cat map are introduced to construct the measurement matrices and to disturb the order of the embedded information, respectively. Furthermore, experimental results demonstrate that the cipher image exhibits superior imperceptibility and the recovered image possesses more satisfactory quality, which is independent of the carrier image.

1. Introduction

Image is widely utilized for communications. However, transmission channels are not secure enough [1]. Normally, to ensure image security, users usually encrypt the original images into meaningless cipher images before transmission. However, it is noteworthy that the meaningless cipher image in the transmission channels would draw more attention of attackers and attract further cryptanalytic attacks on the intercepted cipher image. Therefore, it is necessary to design image encryption schemes to ensure both image security and visual security.

As there exist some intrinsic characteristics such as strong redundancy and high pixel correlation, traditional encryption algorithms are not suitable for images [2]. Therefore multiple image encryption schemes are designed based on other cryptographic features, such as chaos theory [3–10], quantum transformations [11,12], DNA coding [13–15] and optical techniques [16,17]. Fridrich [3] presented a general classic architecture to generate cipher image based on chaos. Specifically, the architecture includes the permutation stage and diffusion stage, in which permutation is achieved by shuffling the pixel locations while diffusion is accomplished by modifying the pixel values sequentially. After that, various effective image encryption schemes referred as the variants for the general architecture were presented [7,9]. A fast image encryption scheme based on total plain image characteristics and chaotic map was presented in [7]. In [9], a robust and fast fingerprint image encryption scheme based on a hyperchaotic map was designed. Furthermore, if the encrypted image can be further compressed before transmission, it can improve the transmission efficiency and be more suitable for the transmission channels with limited bandwidth. However, although the aforementioned algorithms can achieve security performance, they cannot further compress the encrypted image.

Fortunately, the emergence of compressed sensing (CS) makes it possible to perform compression and encryption simultaneously. In addition, CS indicates that a sparse signal can be reconstructed with high probability from only a small set of measurements [18]. From the perspective of cryptography, the CS framework can be considered as a variant of symmetric cryptosystem [19], where the original signal, the measurement matrix and the measurement obtained by linear projection are treated as the plain image, the secret key and the cipher image, respectively. Moreover, the

* Corresponding author.
E-mail address: xiaodi_cqu@hotmail.com (D. Xiao).

https://doi.org/10.1016/j.sigpro.2018.10.001
0165-1684/

security can be achieved by symmetric cryptography based on CS framework, which has been studied in [20–22]. For instance, [20] indicates that the cryptosystem based on CS can resist cipher only attack and brute force attack to achieve computational secrecy. As a result, multiple cryptosystems were presented based on CS. In [23], the permutation matrix is combined with CS to scramble the measurements. In addition, the scrambling is performed directly on the measurements [24]. Another type of scrambling is done before encoding the signal [25,26]. Similar results are shown in [27] where the compound cryptosystem is generated by incorporating the double-random phase encoding technique with CS. However, as pointed in [28], the above methods cannot resist chosen plain attack (CPA) under the measurement matrix reuse circumstances. In order to ensure security even if the measurement matrix is reused many times, [29] introduced parallel compressive sensing (PCS) which is immune to CPA. In [30], PCS is proved to be capable of resisting CPA under certain conditions, and a novel image encryption scheme is presented. A novel encryption scheme based on PCS and the parameterized reality-preserving discrete fractional cosine transform matrix was presented in [31]. However, the cipher images generated by the aforementioned algorithms [23–27,29–31] are meaningless, and the generated cipher images cannot reduce the attacker's suspicion during transmission.

The visually secure cryptosystem is discussed recently. A visually secure cryptosystem was designed in [32] by embedding the secret image generated via any an existing image encryption algorithm into the selected carrier image to obtain the visually secure cipher image. Similar result was shown in [33]. However, the size of the final cipher image is twice that of the plain image, which will result in additional storage space or transmission burden. Different from the above works, Chai et al. exploited CS and secure SHA 256 hash function for designing a visually secure image algorithm which ensures that the size of cipher image is the same as the plain image [34]. However, the hash value of the plain image has to be transmitted to the receiver, which still results in extra transmission burden. Besides, the quality of recovery image depends on the selected carrier image. If the carrier image is selected inappropriately, the quality of the recovery image will severely degrade. Therefore, the flexibility of selecting carrier image is poor.

In this paper, we present an efficient visually secure image encryption scheme based on PCS and the embedding technique. First, the plain image is subjected to PCS and zigzag confusion to obtain the resulting image referred to as secret image. In our work, the discrete wavelet transform (DWT) is employed to transform the plain image, and the obtained coefficient matrix is then sampled in a column-wise manner via PCS counter mode by utilizing the measurement matrices constructed based on chaotic map. Second, the secret image is embedded into the carrier image to get the cipher image. Particularly, the integer discrete wavelet transform (IWT) [35] is introduced to decompose the carrier image to obtain coefficient matrix. Moreover, the order of secret image element insertion is controlled via chaotic sequences. Our contributions can be listed as follows.

(1) The proposed algorithm is immune to CPA with the assistance from PCS counter mode rather than the hash value of the plain image, and thus no extra burden is required to be transmitted.
(2) The chaotic map is employed for embedding to increase the security level of the proposed algorithm.
(3) The proposed algorithm can achieve higher visual security of cipher image with superior secure performance in terms of imperceptibility.
(4) The quality of reconstructed image exhibits no degeneration under the condition that the carrier image is introduced. Since the quality of reconstructed image is independent of carrier image, we can choose the carrier image flexibly.

The rest of this paper is organized as follows. After establishing the necessary preliminaries in Section 2, Chai's scheme is described in Section 3. The proposed encryption scheme is presented and explained in Section 4. Our simulation and security analyses are discussed in Section 5. Comparison with related schemes is presented in Section 6. The last section draws a conclusion.

2. Preliminaries

In this section, we introduce some necessary preliminaries for the proposed scheme, including chaotic maps, PCS, PCS counter mode based encryption, zigzag confusion and reversibility discussion for DWT and IWT.

2.1. Chaotic maps

Since the direct storage of measurement matrix requires large space, how to generate measurement matrix using the initial state values and control parameters of chaotic maps has been studied in [30,34,36]. In this paper, Logistic-Tent system is introduced to construct the measurement matrix, and the 3-D cat map is employed for image permutation as three chaotic sequences can be generated simultaneously.

2.1.1. Logistic-Tent system

In the proposed encryption scheme, Logistic-Tent system is employed to construct the measurement matrix. Logistic-Tent system is the combination of two classical one-dimensional chaotic maps, that is, Logistic map and Skew Tent map. Logistic map is defined as

$$z_{n+1} = \mu z_n(1 - z_n), \tag{1}$$

and Skew Tent map is defined as

$$z_{n+1} = \begin{cases} \frac{z_n}{r} & 0 < z_n < r \\ \frac{1-z_n}{1-r} & r \le z_n < 1, \end{cases} \tag{2}$$

where the initial state value $z_0 \in (0, 1)$, and the control parameter $\mu \in [3.57, 4]$ and $r \in (0, 1)$.

Logistic-Tent system is introduced to generate chaotic sequence with superior performance than Logistic map and Skew Tent map, and it is described by

$$t_{n+1} = \begin{cases} (rt_n(1 - t_n) + 0.5 \times (4 - r)t_n) \bmod 1 & t_n < 0.5 \\ (rt_n(1 - t_n) + 0.5 \times (4 - r)(1 - t_n)) \bmod 1 & t_n \ge 0.5, \end{cases} \tag{3}$$

where, the system initial value $t_0 \in (0, 1)$ and the control parameter $r \in (0, 4]$ [30].

2.1.2. The 3-D cat map

In this paper, the 3-D cat map [36] is introduced for image permutation. The 3-D cat map can be viewed as the extension of two-dimensional Arnold cat map, and it possesses superior randomness for chaotic sequences compared with two-dimensional chaotic maps. The 3-D cat map can be defined as

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \\ z_{n+1} \end{bmatrix} = A \begin{bmatrix} x_n \\ y_n \\ z_n \end{bmatrix} (\mathrm{mod} 1), \tag{4}$$

here

$$A = \begin{bmatrix} 1 + a_x a_z b_y & a_z \\ b_z + a_x b_y + a_x a_z b_y b_z & a_z b_z + 1 \\ a_x b_x b_y + b_y & b_x \end{bmatrix}$$

$$\begin{matrix} a_y + a_x a_z + a_x a_y a_z b_y \\ a_y a_z + a_x a_y a_z b_y b_z + a_x a_z b_z + a_x a_y b_y + a_x \\ a_x a_y b_x b_y + a_x b_x + a_y b_y + 1 \end{matrix} \Bigg], \quad (5)$$

and a_x, a_y, a_z, b_x, b_y, b_z are positive integers. By letting $a_x = a_y = a_z = b_x = b_y = b_z$=1, the specific 3-D cat map can be obtained as follows [36]:

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \\ z_{n+1} \end{bmatrix} = \begin{bmatrix} 2 & 1 & 3 \\ 3 & 2 & 5 \\ 2 & 1 & 4 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \\ z_n \end{bmatrix} (\mathrm{mod}1). \quad (6)$$

Three chaotic sequences are generated by iterating the above defined 3-D cat map, and they will play an important role in the phase of embedding.

2.2. Parallel compressive sensing

2.2.1. Background: Parallel compressive sensing

Traditional CS directly operates on a one-dimensional signal. The size of the required measurement matrix becomes significantly large when the multidimensional signal to be sampled is reshaped to one-dimensional signal. Since the measurement matrix is too large, it increases the computational complexity and the storage space. It is necessary to propose a CS based cryptosystem framework with low computational complexity for both the encoder and decoder. To this end, the PCS is suggested in [37]. For a one-dimensional signal, it is rearranged into a 2D matrix firstly, and then sampled in a column-wise manner via CS by utilizing the same measurement matrix.

For an image X of size $N \times N$, let x_i of size $N \times 1$ denote the $i-th$ column of the image X. Then, the measurement process of PCS can be denoted as

$$y_i = \Phi x_i, \quad (7)$$

where $i = 1, 2, \ldots, N$, and Φ is a sensing matrix of size $M \times N$. Consequently, we can obtain the measurement value matrix $y = [y_1, y_2, \ldots, y_N]$ with the size of $M \times N$.

Similarly, the recovering process from measurement value matrix to the original image is performed column by column. For a single column, CS reconstruction theory indicates that x_i can be faithfully reconstructed with high probability from y_i under the condition that Φ satisfies the restricted isometry property (RIP) and x_i is sparse. Normally, however, the natural signal is sparse in some transform domain, such as DCT, DWT. x_i is said to be k-sparse if $x_i = \Psi S_i$, where S_i is an N-dimensional signal with $\|S_i\|_0 = k$ and Ψ is an $N \times N$ orthogonal matrix. In this case, the measurement process of PCS can be rewritten as

$$y_i = \Phi x_i = \Phi \Psi S_i = \Theta S_i. \quad (8)$$

Consequently, if Φ satisfies RIP and is incoherent with sparse representation basis Ψ, S_i can be recovered with overwhelming probability based on CS reconstruction theory. Then the detailed recovering process of PCS by solving the convex optimization problem can be formalized as:

$$\min \| S_i\|_1 \quad s.t. \quad y = \Theta S_i, \quad (9)$$

here, $i = 1, 2, \ldots, N$. We can obtain $S = [S_1, S_2, \ldots, S_N]$, and hence further reconstruct $X = \Psi S$. Some greedy pursuit algorithms such as orthogonal matching pursuit (OMP) [38], matching pursuit (MP), and convex optimization method can be employed to solve the above equation.

It's remarkable that the sample process and recovering process of PCS are operated in a column-wise manner, while that of the traditional CS is performed on the whole image. Obviously, the parallel PCS can exhibit superior performance in terms of the computational complexity. On the other side, in the aspect of the key composition, traditional CS normally regards the entire sensing matrix as the key; while PCS considers the initial state value and control parameters of the chaotic map as the secret key, and the entries of measurement matrix are constructed by Logistic-Tent system. Thus, PCS shows superior performance under the condition of limited transmission space. All in all, from the point view of computational complexity or the space of secret key storage, PCS is more suitable for practical applications compared with traditional CS.

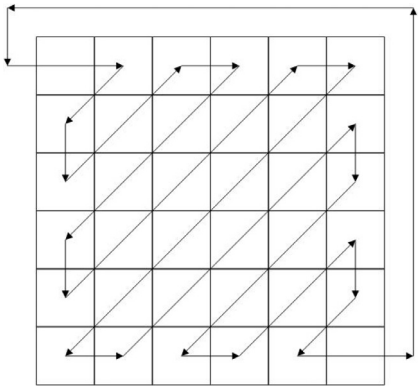

Fig. 1. The zigzag path.

2.2.2. Secrecy of PCS based image encryption

Although PCS can be prioritized in terms of complexity and the storage space in the process of designing a secure image cryptosystem, the secrecy of PCS needs to be further improved. Considering the following special encryption system: suppose that the matrix to be encrypted is a unit matrix $I \in R^{N \times N}$, $I = [x_1, x_2, \ldots, x_N]$, where $x_i \in R^{N \times 1}$, and the measurement matrix $\Phi \in R^{M \times N}$ satisfies the RIP. Then, the encoding process can be formalized as $y_i = \Phi x_i$. Through the analyses above, the adversary who has access to the encoding oracle obtains the perfect measurement matrix $\Phi = [y_1, y_2, \cdots\cdots, y_N]$, where $y_i \in R^{M \times 1}$. It is noteworthy that the most fatal reason why an adversary can acquire accurate measurement matrix is that the measurement matrix used for each column is the same. To this end, the counter mode will be introduced to the image encryption cryptosystem. The detailed description is elaborated in the next subsection.

2.3. PCS Counter mode based encryption

In modern cryptography, the counter mode, which can be immune to CPA, is widely adopted in block cipher encryption. In light of the analysis above, encryption that only adopts PCS cannot resist CPA, so counter mode will be introduced in our work. The counter mode is described as follows:

Step 1: The encoding side sets a random initialization vector $N_0 = IV$.

Step 2: Derive the other nonces from N_0 by counting onward as

$$N_i = (N_{i-1} + 1) \bmod 2^n, \quad i = 1, 2, \ldots, N, \ l \cdot N < 2^n, \quad (10)$$

where N represents the columns of the image and l denotes the number of the encrypted images. The specific process of how to combine PCS and counter mode will be described in the Section 4.

2.4. Zigzag confusion

Zigzag confusion can be regarded as the variant of zigzag path [39] depicted in Fig. 1. Zigzag confusion aims at disturbing the location of the entries in the matrix, which can be performed by

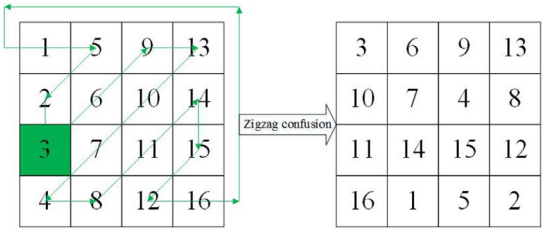

Fig. 2. Results for zigzag confusion with the starting location (3,1).

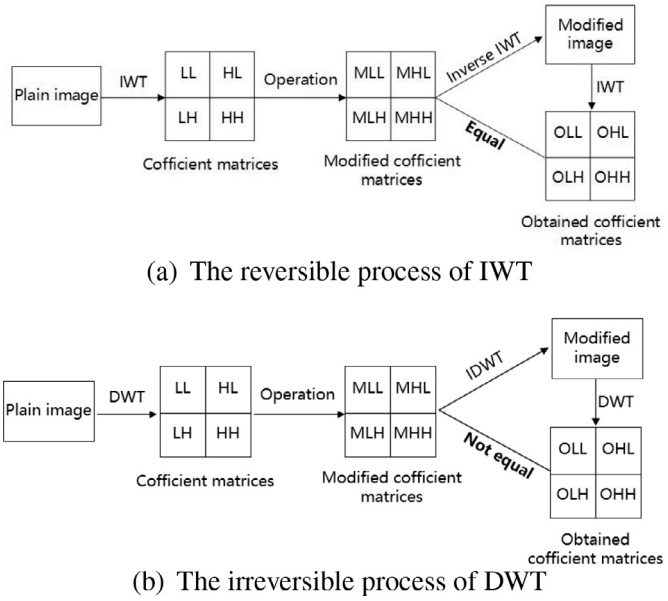

Fig. 3. Reversibility comparison between DWT and IWT.

firstly selecting the starting pixel, and then traversing the matrix from the starting pixel with zigzag path. The uniformity of the non-zero element distribution in the sparse matrix obtained by transforming plain image using sparse representation basis has a significant effect on the reconstruction of the image. In order to improve the security level of the proposed scheme and achieve better accuracy for image construction, the zigzag confusion will be adopted in our work. The matrices after zigzag confusion are different as a result of the different starting locations for plain image. For example, for a 4×4 matrix, if the starting location is (3,1), the matrix will be traversed from the location (3,1). The matrices before and after Zigzag confusion are presented in Fig. 2.

2.5. Reversibility discussion for DWT and IWT

IWT and inverse integer discrete wavelet transform are completely reversible and they can map an integer to an integer, which indicates that the coefficient matrices and the corresponding plain image can be perfectly exchanged. For a more intuitive understanding, the reversible process of IWT is depicted in Fig. 3(a). One can observe that the obtained coefficient matrices by applying IWT to the modified image, *OLL, OLH, OHL, OHH*, are the same as the modified coefficient matrices, *MLL, MLH, MHL, MHH*, since IWT is completely reversible. However, in contrast to IWT, as the characteristics of DWT and inverse discrete wavelet transform (IDWT), the obtained coefficient matrices by DWT have many decimals. Consequently, as depicted in Fig. 3(b), the coefficient matrices obtained by applying DWT to the modified image, *OLL, OLH, OHL, OHH*, are not equal to the modified coefficient matrices, *MLL, MLH, MHL, MHH*. This irreversibility comes from the change between a

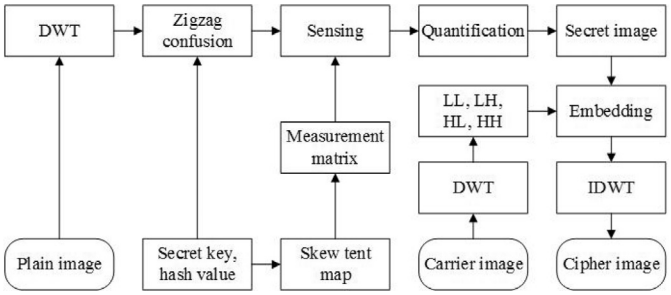

Fig. 4. The schematic of the encryption process of [34].

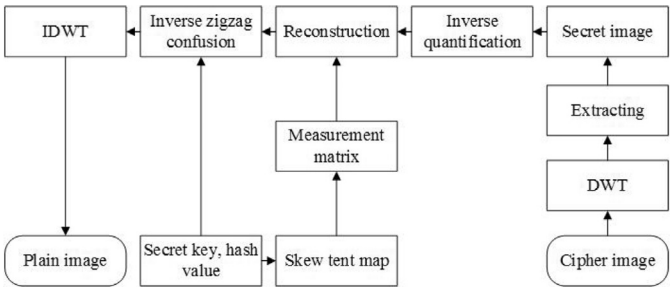

Fig. 5. The schematic of the decryption process of [34].

decimal number and an integer. For this reason, IWT will be applied to the carrier image in our proposed scheme.

3. Chai's scheme

Chai's scheme in [34] includes encryption process and decryption process, which are illustrated in Fig. 4 and Fig. 5, respectively. The encryption process contains encoding phase and embedding phase. The decryption process is composed of extracting phase and decoding phase. The encoding phase encrypts the plain image P with the secret key set K_s controlled by the SHA 256 hash value of the plain image. The DWT coefficient matrix of the plain image is subsequently confused via the zigzag confusion and sampled via the measurement matrix $\Phi_{M \times N}$ to obtain the secret image S. The embedding phase embeds the secret image into the carrier image O to generate a visually secure meaningful cipher image which is similar to the carrier image from appearance. It uses DWT to decompose the carrier image into four coefficient matrices *LL, LH, HL* and *HH*, and then uses secret image to substitute *LH* and *HL* to generate the cipher image. The extracting phase and decoding phase are the inverse operations of embedding phase and encoding phase, respectively. In the extracting phase, the recovered secret image is achieved via applying IDWT to cipher image. Finally, the recovered image can be calculated with the assistance of reconstruction algorithm. More details of Chai's encryption process and decryption process are presented in Algorithm 1 and Algorithm 2, respectively.

However, the following drawbacks exist in Chai's scheme. Firstly, the SHA 256 hash value of the plain image needs to be transmitted each time to the receiver, otherwise the decryption cannot begin. Besides, as shown in Section 2.5, since DWT is not completely reversible, the values of *IT* and *MV* in the embedding phase are different from the values of *IT*2 and *MV*2 in the extracting phase. To ensure smooth extracting and decoding, the matrix *IT* and the medium value *MV* in the encryption process have to be transmitted to the receiver, which also results in extra transmission burden. To verify the argument above, different carrier images are used for test. Table 1 shows the values of *MV* and *MV*2 , as well as the number of different element (NDE) between *IT* and *IT*2, where

Algorithm 1 The encryption process of Chai's scheme.

Input: Plain image P , secret key set K_s and carrier image O
Output: Cipher image C

Encoding phase
(1): Apply DWT to the plain image to obtain the coefficient matrix, and then confuse and modify the entries of the coefficient matrix to get the modified matrix.
(2): Construct the measurement matrix $\Phi_{M\times N}$ by using the skew tent map.
(3): Sample the modified matrix with $\Phi_{M\times N}$ to calculate the measurement value matrix. Secret image S is obtained by changing the entries of measurement value matrix into [0,255].
Embedding phase
(1): Apply DWT to the carrier image to obtain four matrices LL, LH, $HL$and HH .
(2):
for $i = 1toM$ **do**¡¡¡¡

for $j = 1toN$ **do**
$D1(i, j) = s(i, j)$ mod 10
$D2(i, j) = floor(s(i, j)/10)$

(3): Construct an empty matrix IT and calculate the medium value MV of LL matrix.
if $LL(i, j) \geq MV$ **then**¡¡¡¡¡¡¡¡¡
$IT(i, j) = 1$; $LH(i, j) = D1(i, j)$; $HL(i, j) = D2(i, j)$¡¡¡¡
else¡¡¡¡¡¡¡¡¡
$IT(i, j) = 0$; $LH(i, j) = D2(i, j)$; $HL(i, j) = D1(i, j)$
(4): Perform IDWT to the combination of LL, the modified LH, the modified HL and HH to obtain the cipher image.

Algorithm 2 The decryption process of Chai's scheme.

Input: Cipher image C and secret key set K_s
Output: The recovered image

Extracting phase
(1): Apply DWT to the cipher image to obtain four matrices $LL1$, $LH1$, $HL1$, $HH1$.
(2): Construct an empty matrix $IT2$ and calculate the medium value $MV2$ of $LL1$ matrix.
if $LL1(i, j) \geq MV2$ **then**
$IT2(i, j) = 1$; $D1(i, j) = LH2(i, j)$; $D2(i, j) = HL2(i, j)$;
else
$IT2(i, j) = 0$; $D2(i, j) = LH2(i, j)$; $D1(i, j) = HL2(i, j)$;
(3): Obtain the recovered secret image.
Decoding phase
(1): Calculate the measurement value matrix by inverse quantification.
(2): Construct the measurement matrix $\Phi_{M\times N}$ by using the similar method like the (2) in encoding phase. The modified matrix is obtained by using the reconstruction algorithm.
(3): Apply inverse confusion and IDWT to the obtained modified matrix to get the recovered image.

Table 1
IT and *MV* comparison between the encryption and decryption process.

Carrier image	NDE	*MV*	*MV*2
Aerial	106	361.1435	361.6432
Baboon	79	258.2940	258.7933
Barbara	56	224.8935	225.3921
Zero matrix	33832	0	6.2064

the plain image is Lena image of size 512×512. The differences are obvious. Secondly, since the elements of LH and HL are directly substituted by the portions of element of secret image, attackers can obtain secret image via calculating the coefficient matrices of carrier image. Thirdly, the carrier image is destroyed to a large extent so that the cipher image exhibits unsatisfactory performance in terms of imperceptibility. What's more, the quality of the reconstructed image is dependent of the carrier image as the DWT is not completely reversible.

4. The proposed scheme

The proposed encryption scheme is illustrated in Fig. 6. As can be seen, it includes two primary stages. In the first stage, the PCS and zigzag confusion are applied on the plain image to produce its encrypted version called secret image. All the entries of the measurement matrix are determined by Logistic-Tent system whose control parameter and initial state value serve as the secret key. Then, in the second stage, the secret image is incorporated into the carrier image to generate the cipher image. To disturb the embedding order in the second stage, all the key chaotic sequences are generated from the 3-D cat map whose initial state value and control parameters act as the secret key.

4.1. Encryption process

The operation processes can be summarized as below under the assumption that the plain image P is with the size $N \times N$, and the coefficient matrix is sampled in a column-wise manner via PCS by utilizing the different measurement matrix Φ of size $M \times N$.

4.1.1. Generating the secret image based on the PCS and zigzag confusion (PCSZ)

Step 1: Set the pair of initial state value and control parameter (r_0, t_0) of Logistic-Tent system, and a random initialization vector $N_0 = IV$ of nth length.

Step 2: Compute the other nonces N_i $(i = 1, 2, \ldots, N)$ by referring to Eq. (10). Then, the secret key pairs (r_i, t_i) $(i = 1, 2, \ldots, N)$, which are used to generate the corresponding measurement matrix for each column, are subsequently calculated according to

$$r_i = (N_i \times 2^{-n} + r_0) \bmod 4, \tag{11}$$

and

$$t_i = (N_i \times 2^{-n} + t_0) \bmod 1. \tag{12}$$

Step 3: By multiplying the orthogonal wavelet matrix Ψ, the plain image P and the inverse version Ψ' together, the sparse coefficient matrix $P1$ of size $N \times N$ is subsequently obtained according to

$$P1 = \Psi \times P \times \Psi'. \tag{13}$$

Step 4: The matrix $P2$ of size $N \times N$ can be obtained by enforcing the partial entries of the coefficient matrix $P1$ to zero if their values are smaller than a set threshold. Then, the zigzag confusion is applied on the matrix $P2$ to obtain the modified coefficient matrix $P3$.

Step 5: Construct the measurement matrix Φ_i $(i = 1, 2, \ldots, N)$ by iterating Logistic-Tent system with (r_i, t_i). The construction process will be elaborated in Algorithm 3.

Step 6: Apply the measurement matrix Φ_i to the corresponding column of the modified coefficient matrix $P3$ to produce the corresponding measurements. Then the measurement value matrix $P4$ of size $M \times N$ is obtained via splicing the measurements into a matrix.

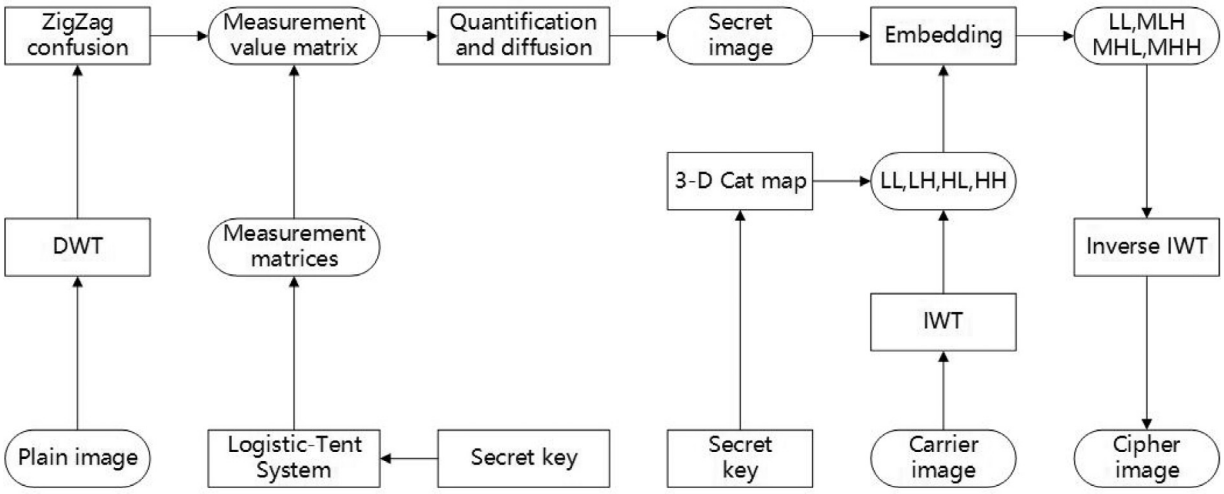

Fig. 6. The schematic of the proposed encryption scheme

Step 7: Quantize the measurement value matrix $P4$ to the range of [0,255], and result matrix is marked as $P5$. The process is formulated as

$$P5 = floor[\frac{255(P4 - \min)}{(\max - \min)}], \tag{14}$$

where $floor(x)$ represents the maximum integer value that is not greater than x.

Step 8: Iterate Logistic-Tent system $n_0 + MN$ times with (r_0, t_0) and discard the former transitional n_0 values to generate the sequence $b = [b(1), b(2), \ldots, b(MN)]$, and then transform it into the integer sequence

$$v(i) = mod(floor(b(i) \times 10^{14}), 256). \tag{15}$$

The values of secret image S are denoted as $S(i)$. Secret image can be computed by

$$S(i) = P5(i) \oplus v(i) \oplus S(i-1), \tag{16}$$

set an integer $S(0) \in [0, 255]$ in advance, and reshape S to a $M \times N$ sized matrix.

4.1.2. Embedding the secret image into the carrier image

In this subsection, the secret image is embedded into the carrier image to obtain the visually secure cipher image. The detailed operation processes can be elaborated as follows under the assumption that the carrier image O is with the size $N \times N$. It is remarkable that the size of the carrier image is not limited to $N \times N$, and the image whose size is larger than the original image can also be selected as the carrier image to satisfy the different visual quality and secure level requirements.

Step 1: In order to avoid possible embedding overflow, the elements of the carrier image O are firstly quantized into the range of [8,247] by rounding $[8 + 0.9373 \times O(i, j)]$. By applying IWT on the carrier image O, an approximation coefficients LL matrix and three detail coefficients matrices HL, LH and HH are subsequently obtained. The three detail coefficients matrices HL, LH and HH are selected for embedding the secret image. The transformation effect of IWT is displayed in Fig. 7, where the plain image Peppers of size 512×512 is shown in Fig. 7(a), and its coefficient image is demonstrated in Fig. 7(b).

Step 2: Stretch the secret image into one-dimensional array $SR = (s_1, s_2, \ldots, s_{MN})$. Then, quantize every element value of the array SR to 8 bits.

Step 3: Embed the array SR into the three detail coefficients matrices HL, LH and HH of the carrier image. The embedding process will be described in Algorithm 4.

(a) Plain image (b) the coefficient image

Fig. 7. The transformation effect of IWT.

Algorithm 3 The measurement matrix Φ_i construction.

Input: A distance d, the constant n_0, and the secret key pairs (r_i, t_i) $(i = 1, 2, \ldots, N)$.

Output: measurement matrix Φ_i $(i = 1, 2, \ldots, N)$.

(1): Iterate Logistic-Tent system $MNd + n_0$ times with the initial value $t_i \in (0, 1)$ and control parameter $r_i \in (0, 4]$ to obtain the chaotic sequence $T(r_i, t_i, d) := \{t_{n_0+jd}\}_{j=1}^{MN}$ by sampling the chaotic values with distance d, where t_{n_0+jd} denotes the jth obtained chaotic value and n_0 is set to obtain the real chaotic sequence.

(2): Let ω_j denote the regularization of t_{n_0+jd}, where $\omega_j = 1 - t_{n_0+jd}$ and $\omega_j \in (-1, 1)$.

(3): Construct the measurement matrix Φ_i by using the chaotic sequence $\{\omega_j\}_{j=1}^{MN}$ in a column-wise manner. Finally, the measurement matrix Φ_i can be described as

$$\Phi_i = \sqrt{\frac{2}{M}} \begin{bmatrix} \omega_1 & \omega_{M+1} & \cdots & \omega_{MN-M+1} \\ \omega_2 & \omega_{M+2} & \cdots & \omega_{MN-M+2} \\ \vdots & \vdots & \ddots & \vdots \\ \omega_M & \omega_{2M} & \cdots & \omega_{MN} \end{bmatrix}. \tag{17}$$

Step 4: By applying inverse IWT to the combination of an approximation coefficients LL matrix and three modified detail coefficients matrices MHL, MLH and MHH, a visually secure cipher image C is obtained. Then the encoding procedure is complete.

4.2. Decryption process

This section is the inverse operation of the encryption process. The decryption process is illustrated in Fig. 8. As can be seen, the proposed decryption algorithm includes two primary stages: the first one is to extract the secret image from the cipher image and

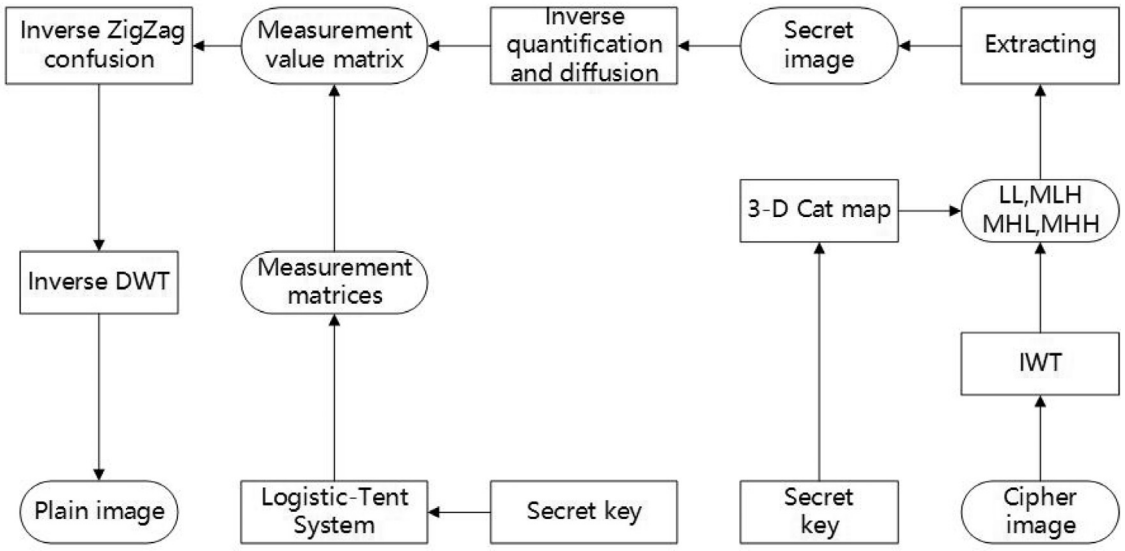

Fig. 8. The schematic of the decryption process

Algorithm 4 The embedding process of Step 3.

Input: The array $SR = (s_1, s_2, \ldots, s_{MN})$, the three detail coefficients matrices *HL*, *LH* and *HH* of the carrier image, the initial state value (x_0, y_0, z_0) and the constant n_1. Here, $M = 0.25N$

Output: The three modified detail coefficients matrices *MHL*, *MLH* and *MHH* .

(1): Iterate the 3-D cat map $MN + n_1$ times with the initial value (x_0, y_0, z_0) to obtain the chaotic sequences $X = \{x_{i+n_1}\}_{i=1}^{MN}$, $Y = \{y_{j+n_1}\}_{j=1}^{MN}$ and $Z = \{z_{t+n_1}\}_{t=1}^{MN}$, where n_1 is set to obtain the real chaotic sequence and x_{i+n_1}, y_{j+n_1}, z_{t+n_1} denote the ith, jth and tth obtained chaotic values of X, Y, Z, respectively.

(2): Let *sort*1, *sort*2, *sort*3 represent the permutations which sort the chaotic sequences X, Y, Z, respectively.

(3): Stretch the three detail coefficients matrices *HL*, *LH* and *HH* into one-dimensional array $\{hl\}_{i=1}^{MN}$, $\{lh\}_{i=1}^{MN}$, $\{hh\}_{i=1}^{MN}$, respectively.

(4): Use *sort*1, *sort*2, *sort*3 to sort $\{hl\}_{i=1}^{MN}$, $\{lh\}_{i=1}^{MN}$, $\{hh\}_{i=1}^{MN}$ into $\{hl'\}_{i=1}^{MN}$, $\{lh'\}_{i=1}^{MN}$, $\{hh'\}_{i=1}^{MN}$, respectively.

(5): Quantize the elements of $SR = (s_1, s_2, \ldots, s_{MN})$ and $\{hl'\}_{i=1}^{MN}$, $\{lh'\}_{i=1}^{MN}$, $\{hh'\}_{i=1}^{MN}$ to 8 bits.

(6):

for $i = 1 to MN$ **do**¡¡¡¡

$hl'_{i6}hl'_{i7}hl'_{i8} = s_{i1}s_{i2}s_{i3}$

$lh'_{i6}lh'_{i7}lh'_{i8} = s_{i4}s_{i5}s_{i6}$

$hh'_{i7}hh'_{i8} = s_{i7}s_{i8}$

(7): Quantize the element of $\{hl'\}_{i=1}^{MN}$, $\{lh'\}_{i=1}^{MN}$, $\{hh'\}_{i=1}^{MN}$ to decimal number.

(8): Apply the inverse of permutations *sort*1, *sort*2, *sort*3 to $\{hl'\}_{i=1}^{MN}$, $\{lh'\}_{i=1}^{MN}$, $\{hh'\}_{i=1}^{MN}$ to obtain $\{mhl\}_{i=1}^{MN}$, $\{mlh\}_{i=1}^{MN}$, $\{mhh\}_{i=1}^{MN}$, respectively.

(9): Reshape $\{mhl\}_{i=1}^{MN}$, $\{mlh\}_{i=1}^{MN}$, $\{mhh\}_{i=1}^{MN}$ into *MHL*, *MLH* and *MHH*.

the latter is to recover the plain image. It is worthy of noting that IWT is perfectly reversible and can transform an integer to an integer. Consequently, the extracted secret image is the same as the secret image.

4.2.1. Extracting the secret image from the cipher image

The operation processes can be summarized as below under the assumption that the secret key (x_0, y_0, z_0) and the constant n_1 have been transmitted to the receiver.

Step 1: By applying IWT to the cipher image, the approximation coefficients *LL* matrix and three modified detail coefficients matrices *MHL*, *MLH* and *MHH* are subsequently obtained.

Step 2: Extract the array $SR = (s_1, s_2, \ldots, s_{MN})$ from the three modified detail coefficients matrices *MHL*, *MLH* and *MHH*. The extracting process will be described in Algorithm 5.

Algorithm 5 The extracting process of Step 2.

Input: The initial state value (x_0, y_0, z_0) , the constant n_1, and the three modified detail coefficients matrices *MHL*, *MLH* and *MHH*

Output: The array $SR = (s_1, s_2, \ldots, s_{MN})$.

(1): Stretch the three modified detail coefficients matrices *MHL*, *MLH* and *MHH* into one-dimensional array $\{mhl\}_{i=1}^{MN}$, $\{mlh\}_{i=1}^{MN}$, $\{mhh\}_{i=1}^{MN}$, respectively.

(2): Perform (1) and (2) in Algorithm 4 to calculate the permutations *sort*1, *sort*2 and *sort*3.

(3): $\{hl'\}_{i=1}^{MN}$, $\{lh'\}_{i=1}^{MN}$, $\{hh'\}_{i=1}^{MN}$ can be calculated by applying the permutations *sort*1, *sort*2, *sort*3 to $\{mhl\}_{i=1}^{MN}$, $\{mlh\}_{i=1}^{MN}$, $\{mhh\}_{i=1}^{MN}$, respectively.

(4): Quantize the elements of $\{hl'\}_{i=1}^{MN}$, $\{lh'\}_{i=1}^{MN}$, $\{hh'\}_{i=1}^{MN}$ to 8 bits.

(5):

for $i = 1 to MN$ **do**¡¡¡¡

$s_{i1}s_{i2}s_{i3} = hl'_{i6}hl'_{i7}hl'_{i8}$

$s_{i4}s_{i5}s_{i6} = lh'_{i6}lh'_{i7}lh'_{i8}$

$s_{i7}s_{i8} = hh'_{i7}hh'_{i8}$

(6): Change the binary representation $s_{i1}s_{i2}s_{i3}s_{i4}s_{i5}s_{i6}s_{i7}s_{i8}$ to decimal number s_i. Then the array $SR = (s_1, s_2, \ldots, s_{MN})$ is calculated.

Step 3: Reshape the array $SR = (s_1, s_2, \ldots, s_{MN})$ to the secret image *S*.

4.2.2. Recovering the plain image

In this section, the plain image is recovered from the secret image. The detailed operation processes can be elaborated as follows under the assumption that the secret keys, including the distance d, the constant n_0, the pair (min , max) of the secret image, the initial state value and control parameter (r_0, t_0) of Logistic-Tent system, and a random initialization vector $N_0 = IV$, are transmitted to the receiver.

Step 1: Perform the inverse diffusion process on the secret image *S* to obtain the matrix *RP*5, and implement inverse quantization on the matrix *RP*5, to obtain the recovered measurement value

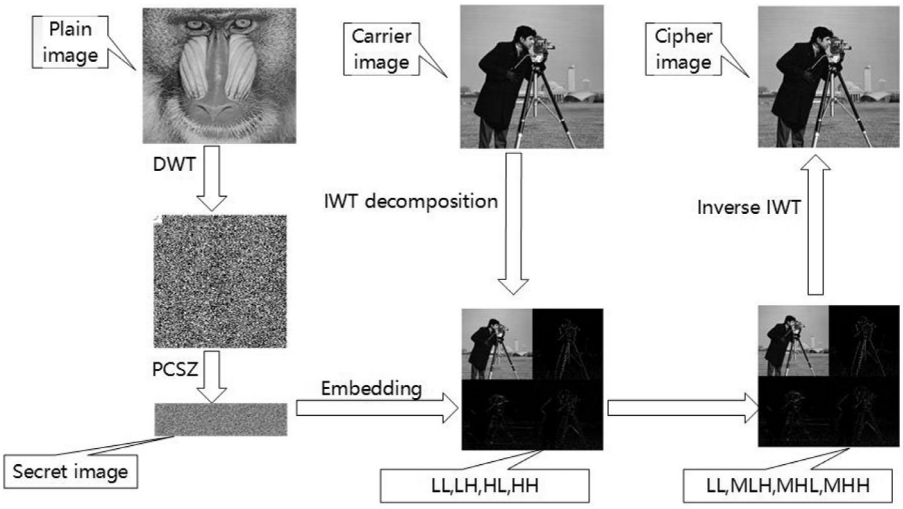

Fig. 9. A visual example of the proposed scheme

matrix $RP4$ as follows

$$RP4 = \frac{RP5 \times (\max - \min)}{255} + \min . \tag{18}$$

Step 2: Calculate the secret key pairs (r_i, t_i) using a random initialization vector $N_0 = IV$ by referring to Eqs. (10)–(12).

Step 3: Perform Algorithm 3 to construct the measurement matrix Φ_i $(i = 1, 2, \ldots, N)$ by iterating Logistic-Tent system with (r_i, t_i).

Step 4: Apply the orthogonal matching pursuit algorithm on the recovered measurement value matrix $RP4$ to obtain the recovered confused sparse coefficient matrix, and the recovered sparse coefficient matrix $RP1$ can be calculated via inverse zigzag confusion (IZC):

$$RP1 = IZC(OMP(RP4, \Phi_i)). \tag{19}$$

Step 5: By multiplying the inverse version of orthogonal wavelet matrix Ψ' , the sparse coefficient matrix $RP1$ and the orthogonal wavelet matrix Ψ together, the recovered plain image RP of size $N \times N$ is subsequently obtained according to

$$RP = \Psi' \times RP1 \times \Psi. \tag{20}$$

5. Simulation and security analysis

The simulation of the proposed scheme is presented, and the security of the scheme is verified from the aspects of histogram analysis, key space, and immunity to classical attacks and so on. Twelve 256 gray scale images of size 256×256 or 512×512 pixels are employed as the test images, as depicted in Figs. 9 and 10, including Baboon256 (256×256), Cameraman (256×256), Brain (256×256), Finger (256×256), Girl (512×512), Barbara (512×512), Lena (512×512), Jet (512×512), Bridge (512×512), Peppers (512×512), Goldhill (512×512), Baboon (512×512). The reconstruction algorithm for PSC is OMP, and the secret keys are selected as $r_0 = 3.148957521688942$, $t_0 = 0.622419853658712$ for Logistic-Tent system and $x_0 = 0.384912579381427$, $y_0 = 0.617825234962247$, $z_0 = 0.812479356648124$ for the 3-D cat map. The simulation experiments are performed in Matlab R2016a platform and a desktop machine with 3 GHz and 4GB memory.

5.1. Encryption and decryption results

The encryption and decryption performances are shown in this section. In order to intuitively express the idea of the proposed algorithm, we subject images Baboon256 and Cameraman to the proposed scheme, and the simulation result is displayed in Fig. 9. The simulation results of other test images are presented in Fig. 10, where the plain images and secret images are displayed in the first and second row, respectively. As can be seen, the volume of all plain images is compressed to be quarter. Particularly, the secret images are not regarded as cipher images to transmit in an insecure channel, so the security level of the proposed scheme is improved from the visual perspective. The compression and encryption performances are well demonstrated. We further verify the imperceptibility of the carrier images. Carrier images and cipher images are plotted in the third and fourth row of Fig. 10, respectively. It is obvious that cipher images are visually meaningful and there is no apparent quality degradation compared to the carrier images, which indicates that the secret images are embedded in the carrier images successfully and the probability for the attackers to be aware of the existence of secret image from the cipher image can be neglected. We also calculate the Peak Signal Noise Ratio (PSNR) to measure the performances of imperceptibility. The cipher images are with PSNRs of 36.9356dB, 35.5617dB, 32.3430dB, 36.1142dB, 37.1058dB, respectively. Experimental results show that the algorithm has good invisibility for secret images. Then, we further test the reconstruction performances. The reconstructed images are depicted in the fifth row of Fig. 10, from which one can see the recovered image is meaningful and visually similar to the plain image presented in the first row with high probability. Similarly, the PSNR values of reconstructed images are also computed, and the results are as follows: 32.2663dB, 34.2626dB, 28.4422dB, 33.4204dB, 31.4662dB, which indicates the image reconstruction quality is satisfactory to certain extent. The above results imply that the proposed algorithm has the significance of simultaneous imperceptibility, compression and encryption of images, which has the potential for the special security and compression requirements in practical applications.

5.2. Histogram analysis

The frequency of the image pixel intensity values can be displayed via the image histogram. The histogram distribution is always not uniform for meaningful plain images as the pixel values distribution of the plain image is relatively concentrated. An effective image encryption algorithm should generate the encrypted image with uniform histogram. Since the proposed algorithm generates the meaningful images, we aim to demonstrate that the his-

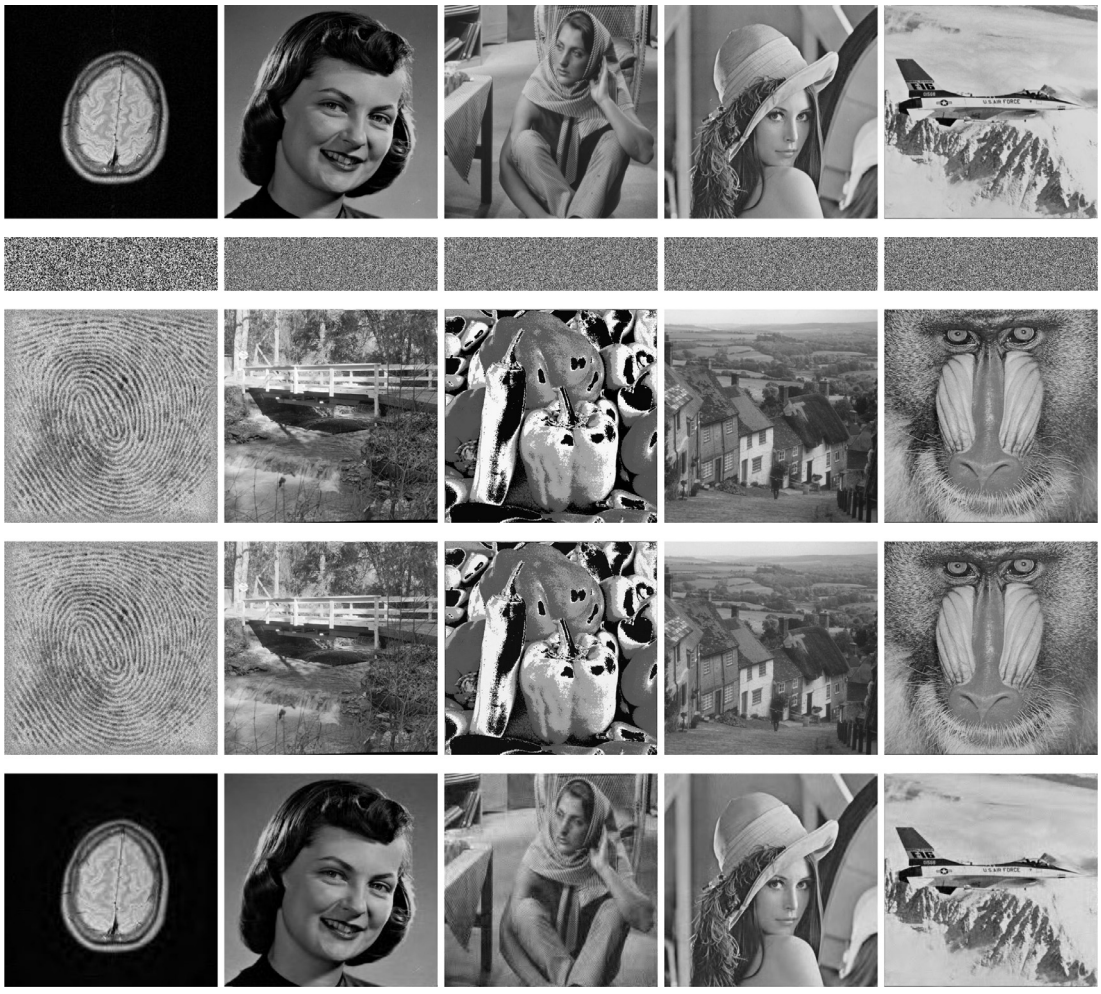

Fig. 10. Simulation results of the proposed algorithm: the plain images, secret images, carrier images, cipher images and reconstructed images are listed from the first to the fifth row, respectively.

tograms of the carrier image and cipher image differ slightly. We successively subject images Brain and Cameraman, Girl and Barbara, Lena and Goldhill, Jet and Baboon to the proposed scheme, and the simulation results are shown in Fig. 11, where the first four rows denote the carrier images, the histograms of the carrier images, the cipher images and the histograms of the cipher images, respectively. One can observe that the histogram of cipher image is similar to that of its corresponding carrier image. Numerically, histogram intersection [40] is introduced to evaluate the similarity between the carrier images and cipher images. The distance of histogram intersection is defined as

$$H(J,V)=\frac{\sum_{k=1}^{L}\min(J_k,V_k)}{\sum_{k=1}^{L}V_k}, \tag{20}$$

where J and V are a pair of histograms, and each contains L bins. The range of values of $H(J, V)$ is between 0 and 1. If the value is s to 1, it means that more similarity between two histograms exists. The simulation results are presented in Table 2, from which one can see that the distances are closer to 1, which indicates that the proposed scheme can achieve satisfactory visual security of cipher image.

Table 2
The difference between the histograms of carrier images and cipher images.

Plain images	Carrier images	Distance
Brain	Cameraman	0.8162
Girl	Barbara	0.9305
Lena	Goldhill	0.9312
Jet	Baboon	0.9474

5.3. Key space

The key space is a set of the possible secret keys which can be employed in the cryptosystem. As suggested in [41], the key space of an effective image encryption cryptosystem should be at least 2^{100}. The key space of the proposed scheme includes the key space of generating the secret image and the key space of the embedding stage. The pairs of chaotic initial state value and control parameter (r_0, t_0) of Logistic-Tent system and (x_0, y_0, z_0) of the 3-D cat map are regarded as secret keys. Supposing that the precision of the 64-bit double precision number is about 10^{-15}, the secret keys $(r_0, t_0, x_0, y_0, z_0)$ consist of five parameters. Consequently, the key space of the proposed image encryption cryptosystem is

$$Key\ space = 10^{15}\times 10^{15}\times 10^{15}\times 10^{15}\times 10^{15} = 10^{75} > 2^{249}. \tag{21}$$

Furthermore, other parameters, such as distance d, the constant n_0, can also be used as the part of the secret key, which can improve the security level of the proposed algorithm. In light of the analysis above, the key space provided by the proposed scheme is large enough to resist brute-force attack.

Fig. 11. Histogram analysis: the first four rows denote carrier images, the histograms of the carrier images, the cipher images and the histograms of the cipher images, respectively.

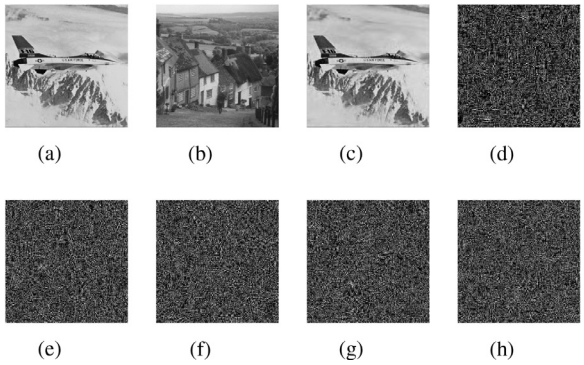

Fig. 12. Key sensitivity analysis: (a) plain image; (b) cipher image; (c) decrypted image with the correct key; (d) decrypted image with the modified key $r_0 + 10^{-15}$; (e) decrypted image with the modified key $t_0 + 10^{-15}$; (f) decrypted image with the modified key $x_0 + 10^{-15}$; (g) decrypted image with the modified key $y_0 + 10^{-15}$; (h) decrypted image with the modified key $z_0 + 10^{-15}$.

5.4. Efficiency analysis

The computational complexity of the proposed scheme includes the execution time of generating the secret image and the execution time of embedding secret image into the carrier image. Referring to the secret image generation based on PCSZ in Section 4, one can observe that the running time of generating the secret image depends on the size of the measurement matrix and the plain image. The complexity is $O(MN^2)$. Since the construction procedure of Φ_i can be operated simultaneously, the complexity theoretically can be reduced to $O(MN)$. For the stage of embedding the secret image into the carrier image, one can observe that all the steps are linear except Step 2 in Algorithm 4 for the carrier image of size $4MN$ and the secret image of size MN. As the time consumption of the embedding stage mainly comes from the workloads of the sort of the chaotic map, the computational complexity is as low as $O(MN + MN \log MN)$ based on the sorting algorithm.

In the following, the running speed for different test images of size 256×256 are analyzed and compared with other CS based image encryption schemes [30,31,34,42]. Here, the image Cameraman is selected as the test carrier image. For the proposed scheme, since the each column of the modified coefficient matrix is sampled individually by different measurement matrices, the process of generating secret image can be processed in parallel. In addition, for a same algorithm, the running speed for different nature images is similar, and thus the average running speed of different algorithms can be compared objectively. The performance of encryption efficiency is presented in Table 3, from which we can see that the encryption efficiency of the proposed scheme is similar to [34], and faster than [42]. Although the efficiency of the proposed scheme seems slower than the ones in [30,31], one should notice that the one in [31] needs more decryption time presented in Table 4, and the proposed scheme can achieve visual security by embedding the secret image into the carrier image, which will consume some time.

Similarly, Table 4 presents the performance of decryption efficiency. From Table 4, it is obvious that the decryption efficiency of the proposed scheme is similar to [30,31,34], and slower than [42]. The reason why decryption time is longer than encryption time is that the optimal solution needs to be solved in the decryption procedure, which will consume much time. It should be noted that the proposed scheme needs to extract the secret image from the cipher image, which will consume some time.

5.5. Sensitivity analysis

Key sensitivity is an important metric to evaluate an effective cryptosystem. In this subsection, key sensitivity analysis in decryption is preformed and the results are illustrated in Fig. 12. To evaluate the key sensitivity, we subject the plain image Jet and carrier image Goldhill to the encryption scheme, and the cipher image subsequently is obtained with the secret key $r_0 = 3.148957521688942$, $t_0 = 0.622419853658712$, $x_0 = 0.384912579381427$, $y_0 = 0.617825234962247$, $z_0 = 0.812479356648124$. Then, the same decryption process is operated with the modified secret key by introducing a tiny change (10^{-15}) to the secret key. The corresponding decrypted images with the modified key are displayed in Fig. 12(d-h), i.e. Fig. 12(d) shows the decrypted image with the modified key $r_0 + 10^{-15}$; Fig. 12(e) shows the decrypted image with the modified key $t_0 + 10^{-15}$; Fig. 12(f) shows the decrypted image with the modified key $x_0 + 10^{-15}$; Fig. 12(g) shows decrypted the image with the modified key $y_0 + 10^{-15}$; Fig. 12(h) shows the decrypted image with the modified key $z_0 + 10^{-15}$. One can obviously see that the decrypted images with incorrect secret key do not leak any useful information. Numerically, to assess the difference between the correctly and incorrectly decrypted images, the number of pixel change rate (NPCR) [43] is introduced, which is calculated by

$$NPCR = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N}\delta_{I_1(i,j),I_2(i,j)}}{MN} \times 100\%, \tag{22}$$

where I_1 and I_2 are two images of size $M \times N$, if $I_1(i, j) = I_2(i, j)$, then $\delta_{I_1(x,y),I_2(x,y)} = 0$; otherwise $\delta_{I_1(x,y),I_2(x,y)} = 1$. The difference between the correctly decrypted image presented in Fig. 12(c) and the incorrectly decrypted images presented in Fig. 12(d), 12(e),12(f),12(g),12(h) are 0.9987, 0.9987, 0.9987, 0.9985, and 0.9988, respectively, which indicate that the proposed scheme has high sensitivity to secret key.

The plain sensitivity results are shown in Fig. 13. Without loss of generality, Lena is selected as test image, and the carrier image

Table 3
Encryption efficiency comparison.

Algorithm	Finger		Baboon256		Average	
	Encryption time (*s*)	Encryptionspeed (*MB*/*s*)	Encryption time (*s*)	Encryption speed (*MB*/*s*)	Encryption time (*s*)	Encryption speed (*MB*/*s*)
[30]	0.0819	0.8002	0.0782	0.8381	0.0801	0.8192
[31]	0.0310	2.1141	0.0284	2.3076	0.0297	2.2108
[34]	0.1159	0.5655	0.1181	0.5549	0.1170	0.5601
[42]	0.4536	0.1445	0.4607	0.1423	0.4572	0.1434
proposed	0.1544	0.4245	0.1523	0.4303	0.1533	0.4274

Table 4
Decryption efficiency comparison.

Algorithm	Finger		Baboon256		Average	
	Decryption time (*s*)	Decryption speed (*MB*/*s*)	Decryption time (*s*)	Decryption speed (*MB*/*s*)	Decryption time (*s*)	Decryption speed (*MB*/*s*)
[30]	2.2841	0.0287	2.2818	0.0287	2.2830	0.0287
[31]	2.6227	0.0250	2.6416	0.0248	2.6322	0.0249
[34]	2.2295	0.0294	2.3225	0.0282	2.2760	0.0288
[42]	1.1374	0.0576	1.1413	0.0574	1.1393	0.0575
proposed	2.2489	0.0291	2.2870	0.0287	2.2679	0.0289

Fig. 13. The results of plain sensitivity.

is Goldhill showed in Fig. 12(b). In order to test the plain sensitivity, we firstly encrypt the plain image to obtain its corresponding cipher image, as presented in Fig. 13(c). Then, we change one bit of the last plaintext image pixel value to obtain the modified plain image, which is subsequently encrypted as the corresponding modified cipher image, as presented in Fig. 13(d). From the appearance, the two images showed in Fig. 13(c) and 13(d) are both similar to the carrier image showed in Fig. 12(b), which is consistent with our visually secure goal. It should be emphasized that each column of the modified coefficient matrix is sampled individually by different measurement matrices, so the sampled result of each column is independent on others. In addition, unlike other meaningless cipher images, the cipher images of the proposed scheme need to be visually secure. The performance of the security level is higher if the visually secure cipher image is more similar to the carrier image. The carrier image plays an important role in generating visually secure cipher images, and thus the modified plain image has a small influence on the cipher image.

Table 5
Correlation coefficients of plain image, secret image, carrier image and cipher image.

Image	Horizontal	Vertical	Diagonal
Plain image	0.9750	0.9714	0.9501
Secret image	0.0062	−0.0107	0.0052
Carrier image	0.9259	0.9447	0.9041
Cipher image	0.9265	0.9402	0.9022

5.6. Correlation coefficients analysis

Correlation coefficients are usually employed to assess the correlation of adjacent pixels in image. In order to assess the correlation between adjacent pixels, 3000 pairs of adjacent pixels (x_i, y_i) are randomly selected from the plain image, secret image, carrier image and cipher image, and then correlation coefficients are calculated in horizontal, vertical and diagonal directions according to

$$r_{xy} = \frac{E(x - E(x))E(y - E(y))}{\sqrt{D(x)} \times \sqrt{D(y)}}, \tag{23}$$

where $E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i$ and $D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2$. We subject the plain image Goldhill and carrier image Bridge to the encryption scheme, and obtain the secret image and cipher image subsequently. Correlation coefficients performances of the proposed scheme have been presented in Fig. 14 and Table 5, from which one can see that the correlation coefficients of secret image has been reduced dramatically, while the correlation coefficients of the plain image are close to 1. In addition, the correlation plots of the cipher image are similar to that of the carrier image, and the correlation coefficients of both are also close to 1, which indicates that the correlation of the carrier image is preserved.

5.7. Information entropy

Information entropy is usually employed to assess the randomness of an information source. The entropy $H(s)$ of an information source s is calculated by

$$H(s) = -\sum_{i=0}^{2^{\kappa}-1} p(s_i)\log_2 p(s_i), \tag{24}$$

where $p(s_i)$ denotes the probability of s_i, κ is the total number bits to represent s_i. If $p(s_i)$ is equal for each symbol s_i, the max-

Table 6
Information entropy of the plain image, secret image, carrier image and cipher image.

Plain image	Carrier image	Entropy			
		Plain image	Secret image	Carrier image	Cipher image
Brain	Cameraman	5.0330	7.9884	7.0097	7.0516
Barbara	Girl	7.4664	7.9970	7.0818	7.2550
Lena	Goldhill	7.4455	7.9968	7.4778	7.4058
Jet	Baboon	5.5716	7.9970	7.3579	7.2682

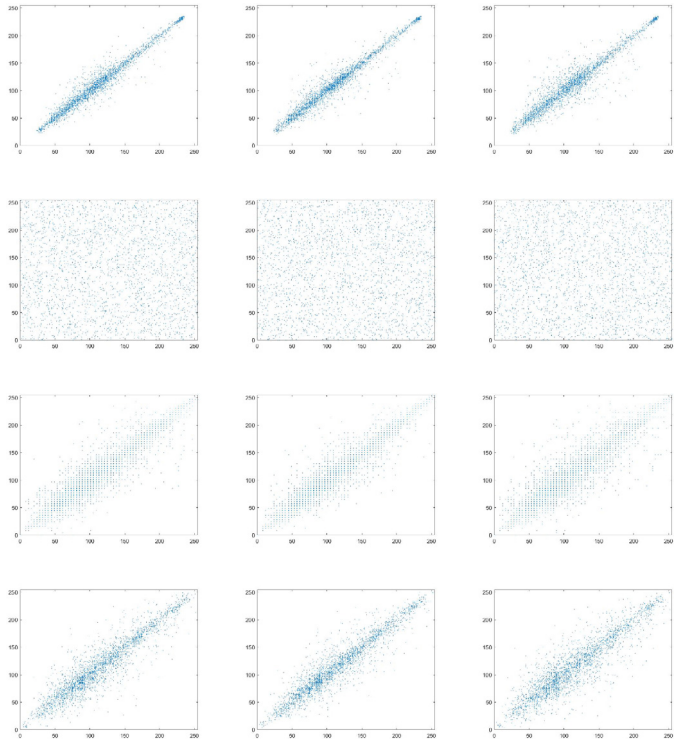

Fig. 14. Correlation coefficients analysis: the correlation plots in horizontal, vertical and diagonal directions of plain image, secret image, carrier image and cipher image are listed from the first to the fourth row, respectively.

imum $H(s)$ will be obtained. Accordingly, as to 256 gray image, $\kappa = 8$, and the ideal image entropy is equal to 8. In order to assess the information entropy of the secret image and the cipher image, the images showed in the first row of Fig. 10 are selected as the test plain images, and the corresponding Bridge, Peppers, Goldhill, Baboon showed in the third row of Fig. 10 are selected as the test carrier images. Then corresponding secret images and cipher images will be obtained. Information entropy performances of the proposed scheme have been presented in Table 6, from which one can see that the values of entropy for different secret images, as listed in fourth column, are close to 8. In addition, as listed in last two columns of Table 6, the values of entropy of carrier images and their corresponding cipher images are close to each other, which indicates that the randomness of the carrier image is also preserved well.

5.8. Various attacks

The resistance against noise attack and cropping attack is an important feature of an effective encryption scheme. During the transmission, it is possible for the cipher image to be contaminated by cropping attack and various noises, such as salt and pepper noise, and Gaussian noise. In our work, the capability of the proposed scheme to resist noise attack and cropping attack is tested.

Table 7
The reconstructed image performance comparison.

Algorithm	PSNR(dB)
[34]	29.0562
[36]	<33.5276
[44]	<26
proposed	33.4204

To evaluate the aforementioned metric, the plain image Girl and the carrier image Goldhill are subjected to the cryptosystem with the secret key $r_0 = 3.148957521688942$, $t_0 = 0.622419853658712$, $x_0 = 0.384912579381427$, $y_0 = 0.617825234962247$, $z_0 = 0.812479356648124$), and then the simulation results are depicted in Fig. 15.

To test the resistance capability against the cropping attack for the proposed scheme, the cipher images with 16×16, 32×32 and 64×64 data loss are shown in Fig. 15(b-d), respectively, and the corresponding reconstructed images are depicted in Fig. 15(f-h). Simulations results demonstrate that the proposed scheme can resist cropping attack with a certain degree.

In the rest of this section, we begin by adding salt and pepper noise with intensities 0.0001%, 0.001%, 0.01% and 0.05% to the cipher image presented in Fig. 15(a). The resulting images and the corresponding reconstructed plain images are shown in Fig. 15(i-l) and Fig. 15(m-p), respectively. Similarly, the contaminated images Fig. 15(q, r-t) are obtained after subjecting cipher image to gaussian noise with intensity 0.0001%, speckle noise with intensities 0.0001%, 0.0002%, 0.0003%, respectively; then the corresponding decrypted image are obtained subsequently shown in Fig. 15(u, v-x). Obviously, with various noise attacks, the reconstructed decrypted images are still readable.

6. Comparison with related schemes

Comparison experiments among the proposed scheme and other existing related schemes are presented in this subsection. For fair comparison, the experimental data of the compared schemes are directly extracted from the cited source paper. If that is not recorded in the cited source paper, then the corresponding experimental data will not be given or is calculated using the secret key provided by the source paper. In this subsection, the image Lena is selected as the plain image, and the default compression rate is set as 0.25.

From the perspective of visual security for cipher image, the volume of the cipher image generated based on the proposed scheme is equal to the plain image; while the cipher image volumes of the existing image encryption schemes in [32,33] are at least twice of the plain image. Smaller cipher image can reduce the storage space and improve the efficiency of transmission. From the perspective of compression, the comparison tests with respect to the image reconstruction quality are performed among the proposed scheme and the ones in [34,36,44]. The experimental results are listed in Table 7. The PSNRs of the schemes in [36,44] are inferred from the recorded results shown in corresponding source

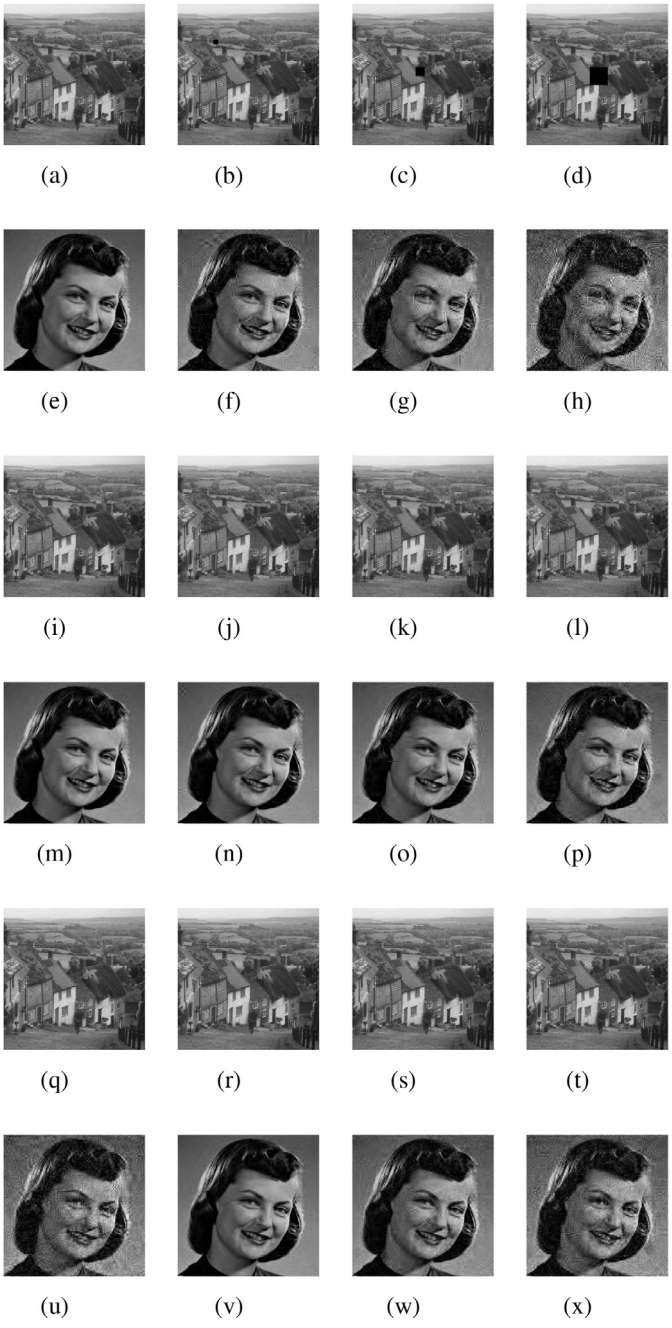

Fig. 15. Various attack analyses: (a) cipher image; (b-d) cipher image with cropped 16×16, 32×32 and 64×64, respectively; (e-h) decrypted image of (a-d); (i-l) contaminated cipher image with salt and pepper noise with intensities 0.0001%, 0.001%, 0.01% and 0.05% , respectively; (m-p) decrypted image of (i-l) ; (q) contaminated cipher image with gaussian noise; (r-t) contaminated cipher image with speckle noise with intensities 0.0001%, 0.0002%, 0.0003%, respectively; (u-x) decrypted image of (q-t).

papers, as the exact experimental data is not recorded in source paper when the compression rate is 0.25. For the scheme in [34], the PSNR value is calculated under the assumption that the image Jet is selected as the carrier image. One can easily observe that the PSNR value of the scheme in [44] is less than 26dB and that of the scheme in [36] is 33.5276dB when the compression rate is 0.5, while the PSNR value of the proposed scheme is 33.4204 dB when the compression rate is 0.25. In addition, the reconstructed image has higher quality in comparison with [34] under the same condition.

Table 8
Comparison of the PSNR values of cipher images.

Plain image	Carrier image	PSNR(dB)	
	[34]	Proposed	
Lena	Peppers	18.5136	32.3513
Jet	Baboon	23.3967	37.1058
Brain	Cameraman	24.8700	34.8967
Girl	Goldhill	28.2318	36.1125
Barbara	Bridge	25.2321	35.5629
Average		**24.0488**	**35.2058**

Table 9
Comparison of the MSSIM values of cipher images.

Plain image	Carrier image	MSSIM	
	[34]	Proposed	
Lena	Peppers	0.6726	0.9257
Jet	Baboon	0.6991	0.9833
Brain	Cameraman	0.6488	0.9381
Girl	Goldhill	0.7021	0.9666
Barbara	Bridge	0.7337	0.9783
Average		**0.6913**	**0.9584**

Since only the visually secure image scheme in [34] is based on CS, we focus on it in the following for further comparison in the aspects of the secret key components, the security for embedding, the imperceptibility of cipher image and the reconstruction image quality under the assumption that a same plain image is embedded in different carrier images.

Firstly, with respect to key components, for the proposed scheme, the key generation process can be achieved without assistance from the plain image; while for the scheme in [34], it cannot be accomplished without the help of SHA 256 hash value of the plain image. What is more, some intermediate key matrices have to be transmitted for possible decryption. For the scheme in [34], the main motivation to employ the SHA 256 hash value of the plain image to calculate the secret key is to ensure that the cipher images are related to the plain image so as to resist CPA. However, the hash value has to be transmitted to the receiver as the extra burden, otherwise the decryption cannot begin. In contrast, for the proposed scheme, since PCS counter mode is introduced to construct different measurement matrices for different plain images, it can be immune to CPA without any extra transmission burden. Particularly, the encryption time can be further reduced with the help of PCS under the assumption that the measurement matrices are constructed offline. In light of the analyses above, the proposed scheme outperforms the scheme in [34] in the aspect of secret key generation.

Secondly, as aforementioned in Section 3, it is shown that the embedding phase in [34] is performed sequentially, which embeds the secret image elements into the coefficient matrices *HL* and *LH* without any order disruption. This operation directly results in a possibility for the attackers to calculate the secret image by applying DWT to the carrier image. Suppose that the key generation process without introducing SHA 256, the algorithm security in [34] is entirely dependent on CS security and zigzag confusion. In this case, once the measurement matrix is reused to encrypt different plain images, it cannot resist CPA, as pointed out in [29]. The above analyses indicate that there is potential security loophole in the embedding phase of the scheme in [34].

Thirdly, with respect to the imperceptibility of cipher image, the comparison results are presented in Tables 8 and 9. As can be observed, the proposed scheme exhibits superior performance on the quality of the cipher image compared with the scheme in [34]. To be more specific, the average PSNR of the five cipher images of the scheme in [34] is 24.0488dB; while the average PSNR of our

Fig. 16. Comparison results of the image reconstruction performance: the first four rows are the cipher images generated by Chai et al. [34], the corresponding decrypted image of the first row, the cipher images generated by the proposed scheme and the corresponding decrypted image of the third row.

Table 10
Comparison of the PSNR values of the reconstruction images.

Carrier image	PSNR (*dB*)	
	[34]	Proposed
Lena	28.4808	28.4422
Bridge	18.4706	28.4422
Girl	12.8477	28.4422
Peppers	12.3628	28.4422
Average	**18.0405**	**28.4422**

scheme is 35.2058*dB*, more than 46.39% better than the former. Similarly, the mean structural similarity index (MSSIM) of the five cipher images of the scheme in [34] is 0.6913; while the average MSSIM of our scheme is 0.9584, more than 38.64% better than the former.

Fourthly, with respect to the reconstruction image quality, the reconstructed image PSNR values are also conducted under the assumption that the same plain image is embedded into different carrier images. The results are depicted in Fig. 16, where the first and second rows are the ciphered images encrypted by the scheme in [34] and the corresponding decrypted images; while the third and fourth row are the ciphered images encrypted by the proposed scheme and the corresponding decrypted images. More specific comparison results are presented in Tables 10 and 11. As can be observed, the reconstructed image quality is apparently related to the carrier image for the scheme in [34]; while for the proposed scheme, no matter which kind of image is selected as the carrier image, the reconstructed image performance still exhibits

Table 11
Comparison of the MSSIM values of the reconstruction images.

Carrier image	MSSIM	
	[34]	Proposed
Lena	0.8142	0.8128
Bridge	0.3210	0.8128
Girl	0.1083	0.8128
Peppers	0.0782	0.8128
Average	**0.3304**	**0.8128**

better over [34]. The leading reason for the above result is that the DWT used in [34] is not completely invertible while the IWT used in the proposed scheme is completely invertible. That is to say, the proposed scheme can achieve visual security without sacrificing reconstructed image quality, and hence the proposed scheme is more suitable for practical applications.

7. Conclusions

In this paper, a visually secure image encryption scheme is proposed to achieve simultaneous image encryption and cipher image imperceptibility, which is based on the PCS counter mode and embedding technique. The PCS counter mode can improve efficiency and resist CPA with no use of the hash value of the plain image. The embedding technique can enhance the security level of the proposed algorithm with the assistance of chaotic maps. In addition, the obtained cipher image exhibits superior imperceptibility performance. Furthermore, the reconstructed image exhibits more satisfactory quality, which is independent of the carrier image by virtue of IWT. The experimental results demonstrate that the proposed scheme outperforms other related schemes and has the potential for practical applications.

Acknowledgement

The work was funded by the National Natural Science Foundation of China (Grant Nos. 61572089, 61633005), the Chongqing Research Program of Basic Research and Frontier Technology (Grant No. cstc2017jcyjBX0008), the Project Supported by Graduate Student Research and Innovation Foundation of Chongqing (Grant No. CYB17026), the Chongqing Postgraduate Education Reform Project (Grant No. yjg183018), the Chongqing University Postgraduate Education Reform Project (Grant No. cquyjg18219), the Fundamental Research Funds for the Central Universities (Grant Nos., 106112017CDJQJ188830, 106112017CDJXY180005), and the Research Program of Chongqing Education Commission (Grant Nos. JK15012027, JK1601225).

References

[1] C. Wang, B. Zhang, K. Ren, J. Roveda, Privacy-assured outsourcing of image reconstruction service in cloud, IEEE Trans. Emerg. Top. Comput. 1 (1) (2013) 166–177.
[2] Y. Zhang, D. Xiao, Y. Shu, J. Li, A novel image encryption scheme based on a linear hyperbolic chaotic system of partial differential equations, Signal Process. Image Commun. 28 (3) (2013) 292–300.
[3] J. Fridrich, Symmetric ciphers based on two-dimensional chaotic maps, Int. J. Bifurc. Chaos 08 (06) (1998) 1259–1284.
[4] L. Zhang, X. Hu, Y. Liu, K. Wong, J. Gan, A chaotic image encryption scheme owning temp-value feedback, Commun. Nonlinear Sci. Numer. Simul. 19 (10) (2014) 3653–3659.
[5] Y. Zhou, L. Bao, C. Chen, A new 1d chaotic system for image encryption, Signal Process. 97 (7) (2014) 172–182.
[6] Z. Hua, Y. Zhou, Image Encryption Using 2D Logistic-Adjusted-Sine Map, Elsevier Science Inc., 2016.
[7] M.A. Murillo-Escobar, C. Cruz-Hernndez, F. Abundiz-Prez, R. Lpez-Gutirrez, O.A.D. Campo, A rgb image encryption algorithm based on total plain image characteristics and chaos, Signal Process. 109 (2015) 119–131.

[8] M. Mollaeefar, A. Sharif, M. Nazari, A novel encryption scheme for colored image based on high level chaotic maps, Multimed. Tools Appl. 76 (2017) 607–629.
[9] F. Abundiz-Prez, C. Cruz-Hernndez, M.A. Murillo-Escobar, R.M. Lpez-Gutirrez, A. Arellano-Delgado, A fingerprint image encryption scheme based on hyperchaotic Rossler map, Math. Probl. Eng. 2016 (5) (2016) 1–15.
[10] T. Lin, X. Wang, J. Meng, A chaotic color image encryption using integrated bit-level permutation, Multimed. Tools Appl. 77 (10) (2017) 6883–6896.
[11] R. Zhou, Y. Sun, P. Fan, Quantum image gray-code and bit-plane scrambling, Quantum Inf. Process. 14 (5) (2017) 1717–1734.
[12] Y. Yang, J. Tian, H. Lei, Y. Zhou, W.M. Shi, Novel quantum image encryption using one-dimensional quantum cellular automata, Inf. Sci. (Ny) 345 (2016) 257–270.
[13] Y. Zhang, D. Xiao, W. Wen, K. Wong, On the security of symmetric ciphers based on dna coding, Inf. Sci. (Ny) 289 (1) (2014) 254–261.
[14] T. Hu, Y. Liu, L. Gong, S. Guo, H. Yuan, Chaotic image cryptosystem using dna deletion and dna insertion, Signal Process. 134 (2017) 234–243.
[15] J. Chen, Z. Zhu, L. Zhang, Y. Zhang, B. Yang, Exploiting self-adaptive permutation diffusion and dna random encoding for secure and efficient image encryption, Signal Process. 142 (2018) 340–353.
[16] J. Bahram, R. Philippe, Optical image encryption based on input plane and fourier planerandom encoding, Opt. Lett. 20 (7) (1995) 767–769.
[17] X. Wang, G. Zhou, C. Dai, J. Chen, Optical image encryption with divergent illumination and asymmetric keys, IEEE Photon. J. 9 (2) (2017) 1.
[18] D. Donoho, Compressed sensing, IEEE Trans. Inf. Theory 52 (4) (2006) 1289–1306.
[19] E.J. Candes, T. Tao, Near-optimal signal recovery from random projections: universal encoding strategies? IEEE Trans. Inf. Theory 52 (12) (2006) 5406–5425.
[20] Y. Rachlin, D. Baron, The secrecy of compressed sensing measurements, in: Proceedings of the Allerton Conference on Communication, Control and Computing, 2008, pp. 813–817.
[21] L. Tong, F. Dai, Y. Zhang, J. Li, D. Zhang, Compressive sensing based video scrambling for privacy protection, in: Proceedings of the Visual Communications and Image Processing, 2011, pp. 1–4.
[22] T. Bianchi, V. Bioglio, E. Magli, Analysis of one-time random projections for privacy preserving compressed sensing, IEEE Trans. Inf. Forensics Secur. 11 (2) (2017) 313–327.
[23] L. Zeng, X. Zhang, L. Chen, Z. Fan, Y. Wang, Scrambling-based speech encryption via compressed sensing, EURASIP J. Adv. Signal Process. 2012 (1) (2012) 1–12.
[24] X. Huang, G. Ye, H. Chai, O. Xie, Compression and encryption for remote sensing image using chaotic system, Secur. Commun. Netw. 8 (18) (2016) 3659–3666.
[25] Y. Zhang, J. Zhou, F. Chen, L. Zhang, K. Wong, X. He, D. Xiao, Embedding cryptographic features in compressive sensing, Neurocomputing 205 (C) (2016) 472–480.
[26] X. Wu, S. Tang, P. Yang, Low-complexity cloud image privacy protection via matrix perturbation, Comput. Sci. (2014).
[27] B. Kim, B. Lee, G. Situ, I. Muniraj, N. Rawat, Compressive sensing based robust multispectral double-image encryption, Appl. Opt. 54 (7) (2015) 1782–1793.
[28] L. Zhang, K. Wong, Y. Zhang, J. Zhou, Bi-level protected compressive sampling, IEEE Trans. Multimed. 18 (9) (2016) 1720–1732.
[29] R. Fay, C. Ruland, Compressive sensing encryption modes and their security, in: Internet Technology and Secured Transactions, 2017, pp. 119–126.
[30] G. Hu, D. Xiao, Y. Wang, T. Xiang, An image coding scheme using parallel compressive sensing for simultaneous compression-encryption applications, J. Vis. Commun. Image Represent. 44 (C) (2017) 116–127.
[31] G. Hu, D. Xiao, Y. Wang, T. Xiang, Q. Zhou, Securing image information using double random phase encoding and parallel compressive sensing with updated sampling processes, Opt. Lasers Eng. 98 (2017) 123–133.
[32] L. Bao, Y. Zhou, Image encryption: generating visually meaningful encrypted images, Inf. Sci. (Ny) 324 (2015) 197–207.
[33] A. Kanso, M. Ghebleh, An algorithm for encryption of secret images into meaningful images, Opt. Lasers Eng. 90 (2017) 196–208.
[34] X. Chai, Z. Gan, Y. Chen, Y. Zhang, A visually secure image encryption scheme based on compressive sensing, Signal Process. 134 (2017) 35–51.
[35] A. Calderbank, I. Daubechies, W. Sweldens, B. Yeo, Wavelet transforms that map integers to integers, Appl. Comput. Harmon Anal. 5 (3) (1998) 332–369.
[36] J. Chen, Y. Zhang, L. Qi, C. Fu, L. Xu, Exploiting chaos-based compressed sensing and cryptographic algorithm for image encryption and compression, Opt. Laser Technol. (2018) 238–248.
[37] H. Fang, S. Vorobyov, H. Jiang, O. Taheri, Permutation meets parallel compressed sensing: how to relax restricted isometry property for 2d sparse signals, IEEE Trans. Signal Process. 62 (1) (2014) 196–210.
[38] J. Tropp, A. Gilbert, Signal recovery from random measurements via orthogonal matching pursuit, IEEE Trans. Inf. Theory 53 (12) (2007) 4655–4666.
[39] P.N.P. Vinod, S. Krishan, Diffusion-Substitution Based Gray Image Encryption Scheme, 23, Academic Press, Inc., 2013.
[40] M.J. Swain, D. Ballard, Color indexing, 7, Kluwer Academic Publishers, 1991.
[41] G. Alarez, S. Li, Some basic cryptographic requirements for chaos-based cryptosystems, Int. J. Bifurc. Chaos 16 (08) (2006) 2129–2151.
[42] X. Chai, X. Zheng, Z. Gan, D. Han, Y. Chen, An image encryption algorithm based on chaotic system and compressive sensing, Signal Process. 148 (2018) 124–144.
[43] M. Preishuber, T. Htter, S. Katzenbeisser, A. Uhl, Depreciating motivation and empirical security analysis of chaos-based image and video encryption, IEEE Trans. Inf. Forensics Secur. 13 (9) (2018) 2137–2150.
[44] N. Zhou, S. Pan, S. Cheng, Z. Zhou, Image compression - encryption scheme based on hyper-chaotic system and 2d compressive sensing, Opt. Laser Technol. 82 (2016) 121–133.