A robust image encryption algorithm based on Chua's circuit and compressive sensing

A robust image encryption algorithm based on Chua's circuit and compressive sensing

Yuling Luo[1], Jia Lin[1], Junxiu Liu[1*], Duqu Wei[1], Lvchen Cao[2], Ronglong Zhou[1], Yi Cao[3], Xuemei Ding[4,5]

[1] School of Electronic Engineering, Guangxi Normal University, Guilin, China, 541004

[2] School of Information and Electronics, Beijing Institute of Technology, Beijing, China, 100081

[3] Management Science and Business Economics Group, Business School, University of Edinburgh, Edinburgh, UK, EH8 9JS

[4] Faculty of Software, Fujian Normal University, Fuzhou, China, 350108

[5] School of Computing, Engineering and Intelligent Systems, Ulster University, Northern Ireland, UK, BT48 7JL

Abstract: In terms of Chua's circuit system, compressive sensing (CS) and Haar wavelet, a novel image compression-encryption scheme (CES) is proposed in this paper. Firstly, the plaintext image is decomposed into approximate component and detail components through Haar wavelet. Then the approximate component is diffused by the threshold processing of local binary patterns (LBP) operator-based chaotic sequence which is produced by the combination of Chua's circuit and Logistic map. Next, the Lissajous map is applied to generate the chaos-combined asymptotic deterministic random measurement matrices (CADRMM) which are employed to measure the detail components in different compression ratios. In addition, the combination of mapped approximate and detail components is shuffled by the Logistic map. The experimental results and simulation analysis prove that the proposed cryptosystem is capable of reducing data for transmission and has good security performance under various attacks, especially for the shear and noise attacks.

Keywords: cryptosystem; compressive sensing; Chua's circuit system; Haar wavelet; CADRMM

1. Introduction

The flourishing development of the information industry has made the security of multimedia information become a major challenge [1]–[5], especially, image security is one of the most crucial problems in many application fields such as military, medical and commercial areas. Therefore, the design of image compression-encryption scheme (CES) has aroused more attention to effectively protect the image data during transmission and storage [6]–[10]. Even though traditional cryptographic approaches, such as Data Encryption Standard (DES) or Advanced Encryption Standard (AES), can protect the digital information well, the inherent characteristics of images are not considered, such as strong correlation between two adjacent pixels and redundancy, so that it makes the algorithms invalid to some extent [11]. As one alternative solution, the chaos-based image cryptosystem is widely investigated recently [1]–[10]. Meanwhile, considering fast transmission and less storage resource, compressive sensing (CS) technology has been gradually applied to many image

encryption algorithms recently, with the aims at reducing the amount of data in different proportions [12]–[20].

Due to the good ergodicity, unpredictability, mixing property, and high sensitivity to initial keys and system parameters, the chaos becomes a good approach to construct the cryptosystem [21]–[27]. Former previous, some simple chaotic systems such as one-dimensional chaotic maps are widely proposed and applied [28]–[30]. However, one-dimensional chaotic maps may lead to weak key space and are vulnerable to known/chosen plaintext attack and brute-force attack is proved [31]. In contrast, large key space is able to bring favourable performance to resist brute-force attack and provide security of high level. Then multidimensional chaotic systems are applied in numerous image encryption method [30]–[33]. Especially, a coupled two-dimensional piecewise nonlinear chaotic map to replace the one-dimensional chaotic systems to design cryptosystem is introduced [32], where the combination of a masking process and external secret key with the length of 256-bit enables the scheme to have adequately large keys space and make the brute-force attack ineffective. Another image cryptosystem integrated with compression simultaneously [33], where the original image is shuffled by the 2-D hyperchaotic system is presented, and the Chinese remainder theorem is introduced to confuse and compress on disarranged image synchronously. In order to improve the degradation under limited precision, a method to constitute three different rules by 3-D chaotic Cat map to judge the procedure of shuffle, scrambling and mixing of every pixel is proposed [34]. Moreover, for strengthening the encryption scenario security, several hyper-chaotic systems are introduced, e.g. a hyperchaotic image cryptography on the basis of a pixel-permutation and bit-confusion mechanism is put forward [35], which can overcome the common weaknesses of the algorithm by using low-dimensional chaotic map. Besides, Deoxyribonucleic acid (DNA) encoding technique is also widely introduced in chaos-based image cryptosystem [36]–[39]. For example, an algorithm where the pixels are thoroughly scrambled via addition and complement is introduced [36]. In [39], an original image is transformed into a DNA matrix, wave-based permutation and row-by-row diffusion operations are performed on it, and it is combined with chaotic system and SHA-256 hash function. In addition, image encryption is not only limited to pixel level operation but also extends to decompose an image into binary bit-plane by using a specific decomposition method. A novel color image cryptosystem by permutating every bit data and employing high-dimensional chaotic map is introduced [40]. To enhance the sensitivity to plain-text to make the chosen plaintext attack vulnerable, a novel bit-level image cryptosystem on the basis of the cyclic shift and swapping operation is presented [41].

In the meantime, considering the convenience and security of data storage and transmission, the compressive sensing (CS) theory is simultaneously introduced to image cryptosystem [42]–[47]. There are two types of measurements matrices that can be used in compressive sensing. The first method is to take the

entire measurement matrix as the key that should be transmitted to result in much space required in the process [48]–[50]. However, due to the chaos maps can also dominate the property of measurement matrix, the second method of producing the measurement matrix by chaos map is more suitable for image encryption. The space of the keys to recover the plain image will be greatly reduced compared to use the entire measurement matrix as the keys. A CES which uses the partial Hadamard matrix to produce measurement matrix of CS is proposed [51]. Besides, 2-D CS and nonlinear fractional Mellin transform are introduced to construct the image CES [52], in which, the measurement matrices which are controlled by a chaotic map is applied to measure the original image from different directions and then the measured result is re-encrypted via nonlinear fractional Mellin transform. Moreover, another CES which the order of the atoms in the discrete cosine transform (DCT) dictionary is scrambled by the logistic map is proposed [53], and the analysis sparse representation of the original image can be obtained with the atom scrambled dictionary and considered as an encrypted version. Analysis results show that it is capable of withstanding noise quite well, while the simulation results of the algorithm need to be further improved under the shear attack. Besides, a mechanism to embed the encrypted image into a carrier image is introduced [54], in which the zigzag path is found to confuse the wavelet coefficients of the plaintext image after wavelet transform. After the compressing by using the CS, the encrypted image is finally obtained. Then the carrier image is acquired by embedding the encrypted image into it. This method can achieve dual security of image information and image appearance. The size of the encrypted image equals to the size of the plain image, i.e. no additional memory space is required.

In order to improve the security of the CES, a novel and robust image CES by using Chua's circuit and CS is proposed in this paper. If the CS theory is directly applied to the plain-image, it will be difficult to recognize the reconstruction image when the cipher images suffer malicious shear attack and noise attack in the transport channel. Therefore, the following procedures have been proposed to eliminate this defect. Firstly, the plain image is decomposed into approximate component and detail components by discrete wavelet transform (DWT) in this work. The approximate component contains the main information of the image, and the security of this component should be enhanced. Secondly, the corresponding approximate component is mapped to 8-bit integer values. As for the diffusion of the approximate component, the threshold processing of local binary patterns (LBP) operator-based permutation is employed to scramble the chaotic sequence which is produced by Chua's circuit. Besides, considered the high space consumption of random measurement matrices, the decision of the measurement matrix is depended on the second method in our proposed algorithm. Hence, the remaining detailed components are measured by chaos-combined asymptotic deterministic random measurement matrices (CADRMM) generated by the Lissajous map. The main contributions of this paper are briefly summarized as follows. (1) A modified measurement matrix CADRMM is developed. (2) A new

method for generating diffusion matrix is introduced. (3) Based on the Chua's circuit, Lissajous map, logistic map and compressive sensing, a robust compression-encryption image cryptosystem is designed. (4) The robustness of the scheme is improved to be capable to defend the shear and noise attacks. (5) The performance simulation and security analysis of this system are displayed.

The rest part of the paper is arranged as follows. Section 2 provides basic knowledge of chaotic maps, compressive sensing, Lissajous map and the threshold processing of LBP operator. The CADRMM and a new method of generating diffusion matrix are also given in detail. Section 3 gives the structure of encryption method, and the corresponding decryption process is briefly involved. Section 4 reports experimental simulations and analysis of the security performance. Finally, Section 5 concludes the paper.

2. Fundamental knowledge

2.1. Two chaotic maps

2.1.1. Logistic map

The Logistic map is defined by

$$x_{n+1} = \mu x_n(1 - x_n), \tag{1}$$

where x_n represents the state value after the iterations of n times and $x_n \in (0,1)$, and x_{n+1} represents the next iteration value of x_n. The system has chaotic behaviours when the control parameter $\mu \in [3.57,4]$. As its small computation cost and good chaotic behaviour, the Logistic map is frequently used in image cryptosystem [6][22][28][55].

2.1.2. Chua's circuit

Chua's circuit [56] represents the nonlinear electronic circuit system, and has several excellent properties, e.g. complex dynamical characteristics, outstanding pseudorandom, unpredictability and sufficient key spaces [57], [58]. It is defined by

$$\begin{cases} \dot{x} = \alpha\big(y - x - f(x)\big); \\ \dot{y} = x - y + z; \\ \dot{z} = -\beta y, \end{cases} \tag{2}$$

where function $f(x)$ represents the electrical response of the nonlinear resistor, which is described as $f(x) = bx + (a - b)(|x + 1| - |x - 1|)/2$, where a and b denote the slope of the inner and outer segments of the piecewise-linear function, α and β are determined by the specific values of the circuit elements, the state variables x, y correspond to the voltage on capacitors, and z indicates the current on inductor. With the increase of α, the system produces a series of asymmetrical bifurcation lines, which gradually form two asymmetrical attractors, i.e., a double vortex chaos attractor. This system includes four

linear elements (two capacitors, one inductor and one resistor) and one nonlinear resistor (Chua's diode), which can be constructed by off-the-shelf opamps. The double vortex chaos attractor appears when $\alpha = 10.0$, $\beta = 15.68$, $a = -1.2768$, $b = -0.6888$ with the parameters of $x = 0.1$, $y = 0.1$ and $z = 0.1$. The attractors are displayed in **Fig. 1**.

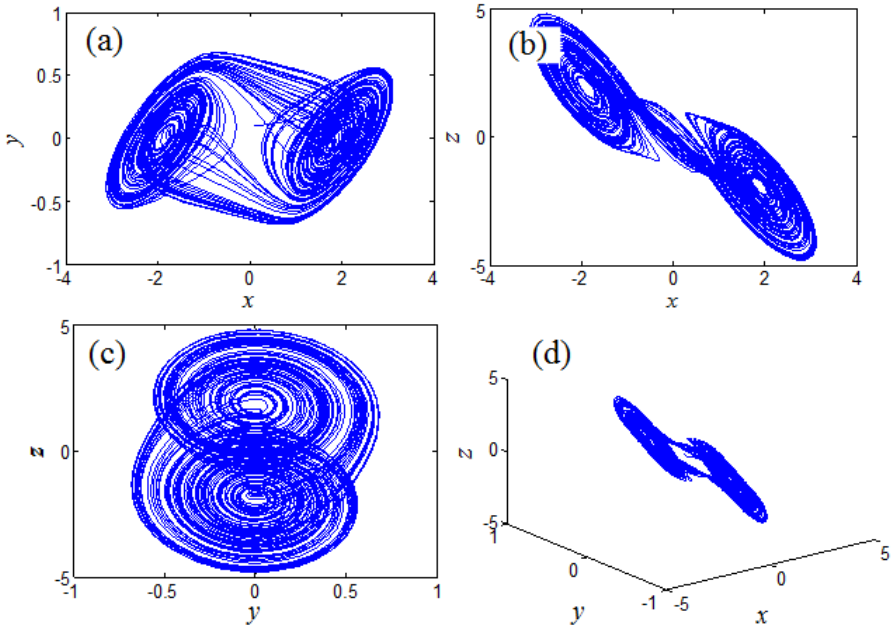


Fig. 1. Attractors of Chua's circuit system. (a) in x and y plane, (b) in x and z plane, (c) in y and z plane, (d) in x, y and z space.

2.2. Compressive sensing

Compressive sensing (CS) [59] has ability to sample and compress synchronously, the sample needed in the reconstruction processing is much fewer than Nyquist sampling theorem. To ensure the signal can be successfully recovered, the following preparation steps should be applied on the original signals.

Firstly, for signal $\boldsymbol{x}$ with dimensions of $N \times 1, \boldsymbol{x} \epsilon R^N$, it is sparse in some transform domains such as DCT and DWT. It can be represented in those sparse domains, i.e.,

$$\boldsymbol{x} = \sum_{i=1}^{N} \psi_i s_i = \boldsymbol{\psi}\mathbf{s}, \tag{3}$$

where ψ_i is each column orthonormal basis of an $N \times N$ orthogonal transform matrix $\boldsymbol{\psi}$, $\mathbf{s}$ represents $N \times 1$ sparse coefficient vector. It is a K-sparse when K entries of $\mathbf{s}$ are non-zero.

Secondly, a measurement matrix is also needed in the whole sampling and compressing process, which is described by

$$\boldsymbol{y} = \phi\boldsymbol{x} = \phi\boldsymbol{\psi}\mathrm{s} = \Theta\mathrm{s}, \tag{4}$$

where ϕ is a measurement matrix with the size of $M \times N$ $(M < N)$ and $M = N/r$, r represents the compression ratio, Θ indicates the product of ϕ and $\boldsymbol{\psi}$, which is the sensing matrix. In order to recover the

signal $\boldsymbol{x}$ from measurement value $\boldsymbol{y}$, the sensing matrix Θ need to meet the condition of restricted isometry property (RIP) which can retain the approximate Euclidean distance of k sparse signal. When k sparse signal is not in the null space of Θ, it is guaranteed that the signal $\boldsymbol{x}$ can be recovered successfully. The conditions are concluded by:

$$(1-\delta_k)\|\mathrm{s}\|_2^2 \leq \|\phi\mathrm{s}\|_2^2 \leq (1+\delta_k)\|\mathrm{s}\|_2^2, \tag{5}$$

where the δ_k is the isometry constant, and ϕ should be highly incoherent with $\boldsymbol{\psi}$. Measurement matrix usually includes Partial Hadamard random matrix, circulant random matrix and Gaussian random matrix etc., Non-convex optimization problem is employed to estimate original signal $\boldsymbol{x}$, the process of solving the sparse estimation is

$$\min\|\mathrm{s}\|_0 \quad \text{s.t} \quad \mathrm{y} = \phi\boldsymbol{\psi}\mathbf{s}, \tag{6}$$

where $\|\mathrm{s}\|_0$ represents the l_0-norm of vector $\mathbf{s}$. Solving this problem is a NP-hard problem. Then, solving l_1-norm optimization problem instead can overcome it, which is described by

$$\min\|\mathrm{s}\|_1 \quad \text{s.t} \quad \mathrm{y} = \phi\boldsymbol{\psi}\mathbf{s}. \tag{7}$$

In general, some common methods of recovering $\boldsymbol{x}$ from $\boldsymbol{y}$ have been proposed, for instance, orthogonal matching pursuit (OMP) [60], subspace pursuit (SP) [61], basis pursuit (BP) [62], compressive sampling matching pursuit (CoSaMP) [63] etc.

2.3. Lissajous map

Lissajous map illustrates that the return map of the nonlinear dynamical system is a perfect Lissajous curve [64]. The nonlinear dynamical system is given by

$$x_{n+1} = f(af^{-1}(x_n)), \tag{8}$$

$$y_n = f(bf^{-1}(x_n)), \tag{9}$$

where $a = p/q > 2$ is a relative prime fraction number, p, q are relative prime numbers, $b = q^N$ is on the condition of $f(t) = sin^2(t), cos^2(t), cos(t)$ or $b = 2(pq)^N$ when $f(t) = sin(t)$, N denotes that the asymptotic deterministic randomness theory can not be predicted in N steps. In this paper, $f(t)$ is taken as $f(t) = sin(t)$, and the nonlinear dynamical system is defined by

$$x_{n+1} = \sin(asin^{-1}(x_n)), \tag{10}$$

$$y_n = sin(bsin^{-1}(x_n)). \tag{11}$$

2.4. Chaos-combined asymptotic deterministic random measurement matrix (CADRMM)

The design of measurements matrix is the kernel of the signal sampling's quality and it affects whether the signal could be easily sampled by hardware or not. Using random measurement matrix may lead to large space consumption during transmission and storage. Due to the defects mentioned above, Lissajous map in section 2.3 is used to generate a sequence with asymptotic deterministic randomness. Then, the asymptotic deterministic random sequence constructs the measurement matrix in CS. According to Eqs. (10)-(11), considering that the relative prime fraction number a in original theory is constant, that is to say, p and q are fixed parameters. In the case of the asymptotic deterministic random sequence meet the conditions of compressive sensing, Logistic map is introduced to improve the variability of the sequence. The generation of measurement matrix includes the following steps and **Fig. 2** is an example of the generation of CADRMM.

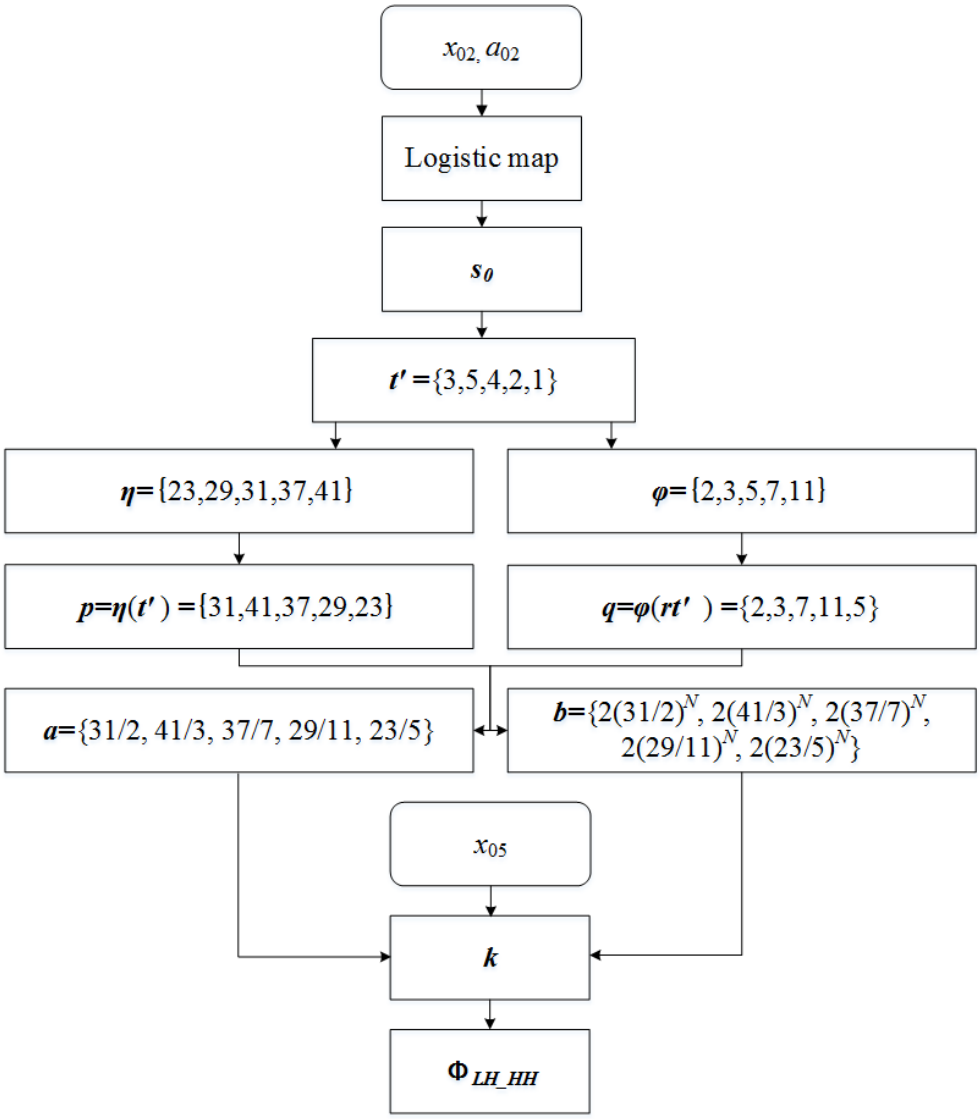


Fig. 2. An example of CADRMM.

Step 1. Two prime number sequences $\boldsymbol{\eta} = [\eta_1, \eta_2, \ldots, \eta_{M\times N}]$ and $\boldsymbol{\varphi} = [\varphi_1, \varphi_2, \ldots, \varphi_{M\times N}]$ are listed in successive order to ensure p and q are co-prime in the aforesaid system, $\boldsymbol{\eta}$ represents numerators and $\boldsymbol{\varphi}$ is the corresponding denominators, and $\eta_{min} > 2\varphi_{max}$ should be guaranteed, where η_{min} is described

as the minimum value of $\boldsymbol{\eta}$, φ_{max} is the maximum value in sequence $\boldsymbol{\varphi}$.

Step 2. Suppose the size of the plain image is $M_1 \times N_1$. After applying DWT on it, the image is divided into four subbands including low frequency partial decomposition coefficient (LL), horizontal direction decomposition coefficient (LH), vertical direction decomposition coefficient (HL) and diagonal direction decomposition coefficient (HH). The size of each subbband is $\frac{M_1}{2} \times \frac{N_1}{2}$. Two chaotic sequences $\boldsymbol{s_0}$ and $\boldsymbol{s_1}$ with length of $\frac{M_1 \times N_1}{2r_1}$ and $\frac{M_1 \times N_1}{2r_2}$ are generated by Logistic map at first, where r_1 and r_2 are the various compression ratios for compressing different component, respectively. The initial parameters of Logistic map are x_{02} and a_{02}. Sort $\boldsymbol{s_0}$ and $\boldsymbol{s_1}$ with descending order after abandoning the foregoing $\frac{M_1 \times N_1}{4r_1}$ and $\frac{M_1 \times N_1}{4r_2}$ elements, then obtain two index sequences $\boldsymbol{t'}$and $\boldsymbol{t''}$, and they are denoted by

$$\boldsymbol{t'} = \left[t'_{\frac{M_1 \times N_1}{4r_1}+1}, t'_{\frac{M_1 \times N_1}{4r_1}+2}, \dots, t'_{\frac{M_1 \times N_1}{2r_1}}\right], \tag{12}$$

$$\boldsymbol{t''} = \left[t''_{\frac{M_1 \times N_1}{4r_2}+1}, t''_{\frac{M_1 \times N_1}{4r_2}+2}, \dots, t''_{\frac{M_1 \times N_1}{2r_2}}\right]. \tag{13}$$

Step 3. Select the numerator $\boldsymbol{\eta}(\boldsymbol{t'})$ from sequence $\boldsymbol{\eta}$ one by one, $\boldsymbol{\eta}(\boldsymbol{t'})$ is the $(t')^{th}$ value of $\boldsymbol{\eta}$ and then choose denominator $\boldsymbol{\varphi}(\boldsymbol{rt'})$ from sequence $\boldsymbol{\varphi}$, $\boldsymbol{\varphi}(\boldsymbol{rt'})$ is the $(M \times N - t')^{th}$ value of $\boldsymbol{\varphi}$. Because the choices of p and q are determined by the chaotic system, the corresponding parameters a and b are not fixed in each iteration. Even if the initial value in Eq. (10) and (11) is known, the right measurement matrix cannot been obtained without the correct coefficient sequences of $\boldsymbol{a}$ and $\boldsymbol{b}$. Compared to use the fixed a and b values in the original equation, the advantage of this process is that the randomness of the measurement matrix can be enhanced. After that, define the numerator sequence as $\boldsymbol{p} = \left[p_1, p_2 \dots, p_{\frac{M_1 \times N_1}{4r_1}}\right]$ and denominator sequence as $\boldsymbol{q} = \left[q_1, q_2, \dots, q_{\frac{M_1 \times N_1}{4r_1}}\right]$. Therefore, the coefficients $\boldsymbol{a} = [\frac{p_1}{q_1}, \frac{p_2}{q_2}, \dots, \frac{p_{\frac{M_1 \times N_1}{4r_1}}}{q_{\frac{M_1 \times N_1}{4r_1}}}]$ in Eq. (8) are obtained. Then calculate the other coefficients $\mathbf{b} = [2(p_1 q_1)^N, 2(p_2 q_2)^N, \dots 2(\frac{p_{\frac{M_1 \times N_1}{4r_1}}}{q_{\frac{M_1 \times N_1}{4r_1}}})^N]$, where N denotes that the asymptotic deterministic randomness theory can not be predicted in N steps. The chaos-combined asymptotic deterministic random sequence $\boldsymbol{k} = \left[k_1, k_2, \dots, k_{\frac{M_1 \times N_1}{4r_1}}\right]$ for detail components LH and HH is produced by iterating the Eq. (10) and (11) for $\frac{M_1 \times N_1}{4r_1}$ times with initial value x_{05} generated by

SHA-256. Similarly, $\boldsymbol{k}' = \left[k'_1, k'_2, \ldots, k'_{\frac{M_1 \times N_1}{4r_2}}\right]$ for HL component is generated by operating the same process.

Step 4. Transform the two chaos-combined asymptotic deterministic random sequence $\boldsymbol{k}$ and $\boldsymbol{k}'$ into two measurement matrices by

$$\boldsymbol{\Phi_{LH\_HH}} = \begin{bmatrix} k_1 & \ldots & k_{\frac{N_1}{2}} \\ k_{\frac{N_1}{2}+1} & \ldots & k_{N_1} \\ \ldots & \ldots & \ldots \\ k_{\left(\frac{M_1}{2r_1}-1\right)\times\frac{N_1}{2}+1} & \ldots & k_{\frac{M_1 \times N_1}{4r_1}} \end{bmatrix}, \tag{14}$$

$$\boldsymbol{\Phi_{HL}} = \begin{bmatrix} k'_1 & \ldots & k'_{\frac{N_1}{2}} \\ k'_{\frac{N_1}{2}+1} & \ldots & k'_{N_1} \\ \ldots & \ldots & \ldots \\ k'_{\left(\frac{M_1}{2r_2}-1\right)\times\frac{N_1}{2}+1} & \ldots & k'_{\frac{M_1 \times N_1}{4r_2}} \end{bmatrix}. \tag{15}$$

where $\boldsymbol{\Phi_{LH\_HH}}$ is the measurement matrix for LH and HH component, and $\boldsymbol{\Phi_{HL}}$ represents the measurement matrix for HL component.

2.5. Threshold processing of LBP operator

The LBP is an operator in the field of digital image processing which can be used to represent local texture characteristics of an image originally. In this work, it is combined with Chua's circuit to produce chaotic mask to diffuse approximate component. The original LBP operator is defined in the window of 3×3, where the window sets the center pixel as the threshold. If the eight neighbours of the pixel are larger than the threshold, it is marked as 1, otherwise 0 is instead. Through this method, every 8-bit binary number is generated by one threshold. **Fig. 3** describes the transform process in detail.

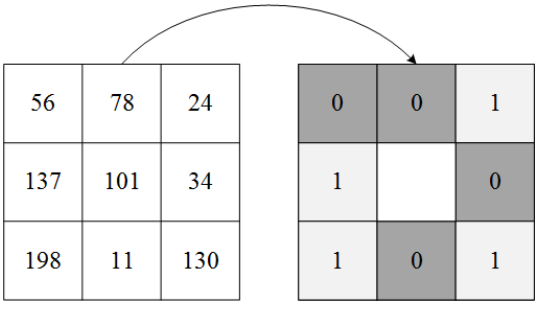


Fig. 3. The example for threshold processing of LBP operator-based transform process.

2.6. A novel method to generate the diffusion matrix

For a chaotic matrix $\mathbf{T} \in R^{M_1 \times N_1}$ generated by Chua's circuit, it can be further scrambled and diffused to get the diffusion matrix by the following steps,

Step 1. Compare each value in matrix $\mathbf{T}$ with its 8-adjacent areas. For example, if $\mathbf{T}_{i,j}$ is the comparison object, $\mathbf{T}_{i,j}$ should be compared with the value $\mathbf{T}_{i-1,j-1}$, $\mathbf{T}_{i-1,j}$, $\mathbf{T}_{i-1,j+1}$, $\mathbf{T}_{i,j-1}$, $\mathbf{T}_{i,j+1}$, $\mathbf{T}_{i+1,j-1}$, $\mathbf{T}_{i+1,j}$ and $\mathbf{T}_{i+1,j+1}$ in eight directions around it, where $\mathbf{T}_{i,j}$ represents the value in row i and column j. Similarly, each value in this entire matrix $\mathbf{T}$ should be traversed by the comparison approach mentioned in section 2.5.

Step 2. Suppose that $\mathbf{T}_{i-1,j-1}$ is larger than $\mathbf{T}_{i,j}$, then $\mathbf{T}_{i-1,j-1}$ is marked as 1 otherwise mark as 0 instead. Consequently, a matrix $\mathbf{T}'$ composed of 0 and 1 is produced and turn $\mathbf{T}' \in R^{8M_1 \times N_1}$ into $\mathbf{T}'' \in R^{1\times 8M_1N_1}$ with the aim to facilitate the follow-up scrambling operation on it.

Step 3. Iterate the Logistic map with initial conditions x_{03} and a_{03} to get chaotic sequence and then sort it in ascend order to obtain the index sequence $\boldsymbol{q} = [q_1, q_2, \dots, q_i, \dots, q_{8M_1\times N_1}]$, where q_i indicates the i^{th} element in $\boldsymbol{q}$. Then the sequence $\boldsymbol{q}$ is used to disturb $\mathbf{T}''$ in the terms of,

$$\mathbf{T}'''(1,i) = \mathbf{T}''(1,q_i),\ i=1, 2, \dots, 8M_1 \times N_1 \tag{16}$$

where q_i represents the sequential index of the i^{th} number in sequence $\boldsymbol{q}$, and $\mathbf{T}''' \in R^{1\times 8M_1N_1}$ in which there will be a better randomness between each two adjacent binary elements. Specifically, the i^{th} element $\mathbf{T}'''(1,i)$ of the sequence $\mathbf{T}'''$ is substituted by the $q_i{}^{th}$ value of sequence $\mathbf{T}''$, where $i = 1, 2, \dots, 8M_1 \times N_1$. The length of the sequences $\mathbf{T}''$ and $\mathbf{T}'''$ is $8M_1 \times N_1$.

Step 4. Transform every 8 elements in $\mathbf{T}'''$ to a value which ranges from 0 to 255 by

$$f_i = \mathbf{T}'''_{1+8\,(i-1)} \times 2^7 + \mathbf{T}'''_{2+8\,(i-1)} \times 2^6 + \mathbf{T}'''_{3+8(i-1)} \times 2^5 + \mathbf{T}'''_{4+8((i-1)} \times 2^4 + \mathbf{T}'''_{5+8(i-1)} \times 2^3 + \mathbf{T}'''_{6+8\,(i-1)} \times 2^2 + \mathbf{T}'''_{7+8(i-1)} \times 2^1 + \mathbf{T}'''_{8+8(i-1)} \times 2^0 \tag{17}$$

where f_i indicates the i^{th} value of matrix $\boldsymbol{f}$, $\mathbf{T}'''_a$ is the a^{th} value of matrix $\mathbf{T}'''$. The diffusion matrix $\boldsymbol{f}' \in R^{M_1\times N_1}$ is constructed by rearranging $\boldsymbol{f} \in R^{8M_1\times N_1}$.

3. The proposed compression-encryption procedure

The proposed image CES is put forward based on gray image, and the complete working flow chart is described in **Fig. 4**.

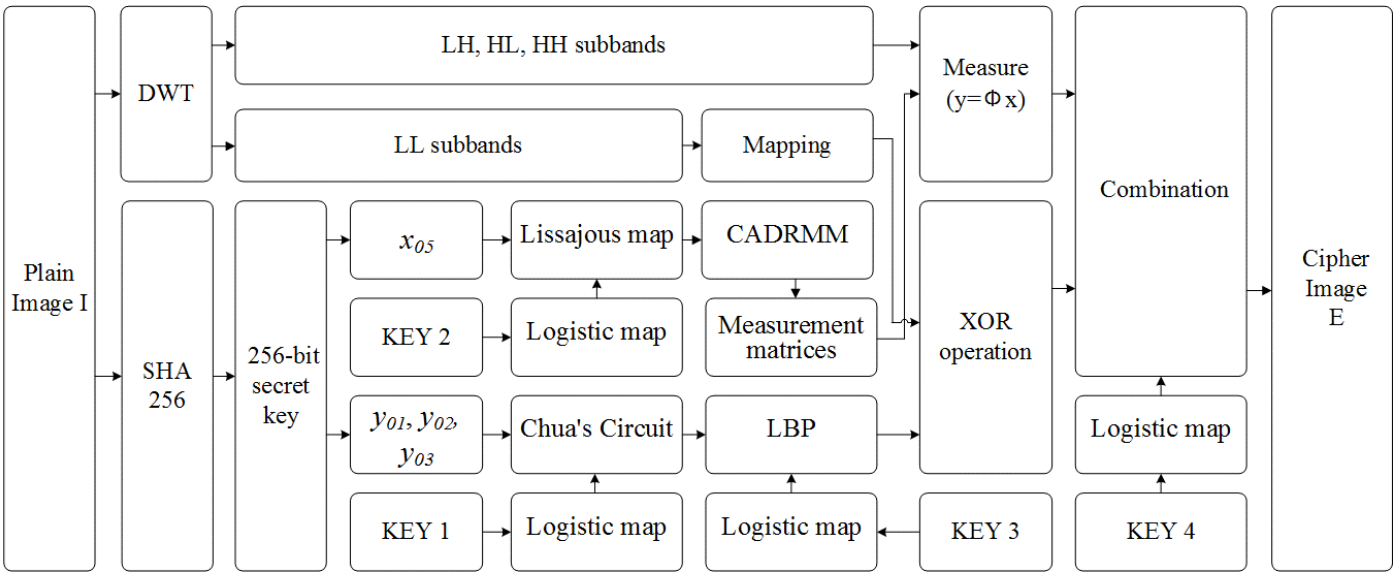


Fig. 4. The proposed compression-encryption procedure.

In this proposed algorithm, the measurement matrix CADRMM is mainly generated by Lissajous map and the logistic map, therefore, only several parameters are needed during transmission or storage. With the correct secret keys, the reconstruction of recovered image can be accomplished successfully. Compared with the method of transmitting the whole random measurement matrix in [49], the space consumption problem can be solved by this proposed CDARMM. Besides, the proposed algorithm has strong robustness against noise attack and occlusion attack. The complete process of this image CES can be described in the following steps.

Step 1. Firstly, based on the original image information, SHA-256 is applied to produce the keys y_{01}, y_{02}, y_{03} of the Chua's circuit and x_{05} of CADRMM. Specifically, the final hash value generated by SHA-256 can be denoted as $= k^1, k^2, k^3 \ldots, k^{32}$ ($k^i = \{k_0^i, k_1^i, k_2^i, \ldots, k_7^i\}$ where for each k_j^i, i is the character number and j represnets the j^{th} bit in k^i). The keys for Chua's circuit and CADRMM are obtained by

$$\begin{cases} y_{01} = \frac{1}{256}(k^1 \oplus k^8 \oplus k^2 \oplus k^7 + k^3 \oplus k^6 \oplus k^4 \oplus k^5) \\ y_{02} = \frac{1}{256}(k^9 \oplus k^{16} \oplus k^{10} \oplus k^{15} + k^{11} \oplus k^{14} \oplus k^{12} \oplus k^{13}) \\ y_{03} = \frac{1}{256}(k^{17} \oplus k^{24} \oplus k^{18} \oplus k^{23} + k^{19} \oplus k^{22} \oplus k^{20} \oplus k^{21}) \\ x_{05} = \frac{1}{256}(k^{25} \oplus k^{32} \oplus k^{26} \oplus k^{31} + k^{27} \oplus k^{30} \oplus k^{28} \oplus k^{29}) \end{cases} \quad (18)$$

where $\oplus$ is the bitxor operation. Due to the strongly sensitivity to the plain image for SHA-256, so the tiny change of original image will bring out completely different secret keys.

Step 2. Suppose the dimension of the original image I is $M \times N$, and it is decomposed into low frequency partial coefficient LL, detail components LH, HL and HH by DWT. The size of these subbands

LL, LH, HL and HH is $M_1 \times N_1$.

Step 3. Iterate Chua's circuit $M_1 \times N_1/3$ times with the initial values y_{01}, y_{02} and y_{03} which are generated by SHA-256 and the y_{01}, y_{02} and y_{03} correspond to parameters x, y, z and $\alpha = -1.2768$, $\beta = -0.6888$, $a = -1.2768$, $b = -0.6888$ in Eq. (2), respectively. The length of sequences l_1, l_2 and l_3 is $M_1 \times N_1/3$. Then integrate these three sequences into a chaotic sequence $|l_4| \in R^{1\times M_1 N_1}$, where $|a|$ is the absolute value of a. To reduce the correlation between adjacent values of the $|l_4|$, the logistic map with initial conditions x_{01} and a_{01} is employed to generate another chaotic sequence $\boldsymbol{q} = [q_1, q_2, \dots, q_{M_1\times N_1}]$. Then ergodic rearrangement is applied by sorting the sequence in an ascend order to obtain the index sequence $\boldsymbol{s} = [s_1, s_2, \dots, s_{M_1\times N_1}]$. After that, $|l_4|$ is scrambled according to sequence $\boldsymbol{s}$ and the permutated chaotic sequence is denoted as $|l_4|'$.

Step 4. To transform $|l_4|'$ into integer sequence $\boldsymbol{z} = [z_1, z_2, \dots, z_{M_1\times N_1}]$ and enhance the difference intensity between every two adjacent values, the corresponding calculation is taken as

$$z_i = \lfloor |l_4|'_i \times 10^{16} \bmod 256 \rfloor \tag{19}$$

where $\lfloor a \rfloor$ indicates the nearest integer smaller than a, i is the i^{th} value in the sequence, and then transform $\boldsymbol{z}$ into matrix $\boldsymbol{z}'$ by using

$$\boldsymbol{z}' = \begin{bmatrix} z_1 & \cdots & z_{N_1} \\ z_{N_1+1} & \cdots & z_{2N_1} \\ \cdots & \cdots & \cdots \\ z_{(M_1-1)N_1+1} & \cdots & z_{M_1\times N_1} \end{bmatrix}. \tag{20}$$

Step 5. According to section 2.4, the initial parameters x_{02}, a_{02} are used to produce chaotic sequences $\boldsymbol{t}'$and $\boldsymbol{t}''$. Both of them are used to choose numerators from $\boldsymbol{\eta}$ and denominators from $\boldsymbol{\varphi}$ for parameters a and b in Eq. (10) and (11), respectively. The measurement matrix $\boldsymbol{\Phi_{LH\_HH}}$ is generated by iterating Eq. (10) and (11) $M_1 \times N_1/r_1$ times with initial value x_{05}, and it is used to measure LH and HH with compression ratio $r_1 = 4$. Similarly, do $M_1 \times N_1/r_2$ times iteration to bring out $\boldsymbol{\Phi_{HL}}$ to measure HL with compression ratio $r_2 = 2$.

Step 6. Extend LH, HL and HH components in Ψ domain to obtain α_{LH}, α_{HL} and α_{HH}. Apply $\boldsymbol{\Phi_{LH\_HH}}$ to measure α_{LH}, and α_{HH}. Meanwhile, measure α_{HL} by $\boldsymbol{\Phi_{HL}}$. The measured results are described by

$$y_{LH} = \boldsymbol{\Phi_{LH\_HH}}\alpha_{LH} = \boldsymbol{\Phi_{LH\_HH}}\Psi^T LH; \tag{21}$$

$$y_{HH} = \boldsymbol{\Phi_{LH\_HH}}\alpha_{HH} = \boldsymbol{\Phi_{LH\_HH}}\Psi^T HH; \tag{22}$$

$$y_{HL} = \boldsymbol{\Phi_{HL}}\alpha_{HL} = \boldsymbol{\Phi_{HL}}\Psi^T HL, \tag{23}$$

where $y_{LH} \in R^{M_1 \times N_1 / r_1}$, $y_{HH} \in R^{M_1 \times N_1 / r_1}$ and $y_{HL} \in R^{M_1 \times N_1 / r_2}$.

Then transform the measured results into 8-bit integers using

$$y_{LH}{}'_{i,j} = \text{round}\left[255 \times \left(y_{LH_{\text{i,j}}} - y_{LH_{min}}\right) / \left(y_{LH_{max}} - y_{LH_{min}}\right)\right] \tag{24}$$

$$y_{HH}{}'_{i,j} = \text{round}\left[255 \times \left(y_{HH_{\text{i,j}}} - y_{HH_{min}}\right) / \left(y_{HH_{max}} - y_{HH_{min}}\right)\right] \tag{25}$$

$$y_{HL}{}'_{i,j} = \text{round}\left[255 \times \left(y_{HL_{\text{i,j}}} - y_{HL_{min}}\right) / \left(y_{HL_{max}} - y_{HL_{min}}\right)\right] \tag{26}$$

where round $[a]$ is the rounding operation, $y_{LH_{\text{i,j}}}$ indicates the value of row i and column j in y_{LH}, $y_{LH_{min}}$ is the minimum value of y_{LH} and $y_{LH_{max}}$ is the maximum value of y_{LH}, $y_{LH}{}'_{i,j}$ denotes the matrix after mapping. Similarly, $y_{HH}{}'_{i,j}$ and $y_{HL}{}'_{i,j}$ are produced by the same process.

Step 7. According to section 2.6, x_{03} and a_{03} are served as the secret keys in Logistic map. A novel method is applied to rearrange the chaotic matrix $\boldsymbol{z}'$ and an integer diffusion matrix $\boldsymbol{f}' \in R^{M_1 \times N_1}$ is constructed.

Step 8. Due to that the LL component is composed of wavelet coefficients, map LL to 0 to 255 by

$$LL'_{i,j} = \text{round}\left[255 \times \left(LL_{\text{i,j}} - LL_{min}\right) / \left(LL_{max} - LL_{min}\right)\right], \tag{27}$$

where round $[a]$ is the rounding operation, $LL_{\text{i,j}}$ indicates the value of row i and column j in LL, LL_{min} is the minimum value of LL and LL_{max} is the maximum value of LL, in addition, $LL'_{i,j}$ denotes the matrix after mapping.

Step 9. Diffuse the $LL'_{i,j}$ by XOR operation by

$$LL''_{i,j} = LL'_{i,j} \oplus \boldsymbol{f}'_{i,j} \tag{28}$$

where $LL'_{i,j}$ indicates the value of row i and column j in LL', $LL''_{i,j}$ indicates the value of row i and column j in LL'', $\boldsymbol{f}'_{i,j}$ denotes the value of row i and column j in $\boldsymbol{f}'$, and $\oplus$ denotes bitxor operation.

Step 10. Construct a new matrix $\mathbf{P}$ with y'_{LH} y'_{HH}, y'_{HL} and LL'', and the size of $\mathbf{P}$ is $M_1 \times N$. In this proposed scheme, LL'' is located in $\mathbf{P}(:, 1{:}N_1)$, and $\mathbf{P}(1{:}M_1 \times N_1 / r_1, N_1 + 1{:}N)$ is y'_{LH}, where $\mathbf{P}(:, 1{:}N_1)$ denotes the 1^{st} to N_1^{th} column vector of $\mathbf{P}$. Then locate y'_{HH} in the position of $\mathbf{P}(M_1 \times N_1 / r_1 + 1{:}2M_1 \times N_1 / r_1, N_1 + 1{:}N)$, and place y'_{HL} in $\mathbf{P}(2M_1 \times N_1 / r_1 + 1{:}M_1, N_1 + 1{:}N)$. Here, we

assume that the compression ratio r_1 of LH and HH equals to 4 and the compression ratio r_2 of HL is 2. **Fig. 5** shows the image after combination.

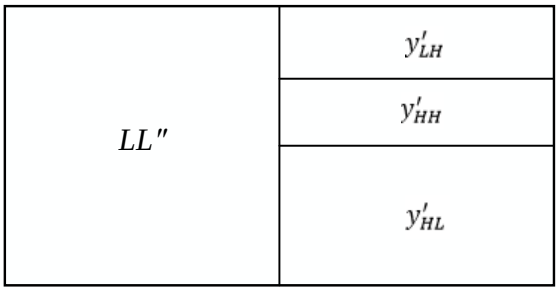


Fig. 5. The result **P** after combination.

Step 11. Finally, iterate Logistic map with the initial parameters $x_{04} = x'_{04} + x_{02}/100 + x_{05} \,/\, 100$ and $a_{04} = a'_{04} + a_{02}/100$, where $x'_{04} \in (0, 0.5]$ and $a'_{04} \in [3.57, 3.959]$. Sort the sequence $\boldsymbol{q}' = [q'_1, q'_2, \ldots, q'_{M_1 \times N}]$ in descending order and get the index sequence $\boldsymbol{s}' = [s'_1, s'_2, \ldots, s'_{M_1 \times N}]$. Disturb the matrix **P** by $\boldsymbol{s}'$ and the final encrypted image **E** is constructed.

In relevant decryption process, the encrypted result of the plain image is permutated in an inverse order, and the detail components LH, HL and HH are recovered by Orthogonal Matching Pursuit (OMP) algorithm. Approximate component LL is transformed to wavelet domain through inverse mapping. Then employ inverse discrete wavelet transform (IDWT) to recover the entire original image.

4. Experimental simulation and security analysis

The simulation results of the proposed CES are evaluated in the PC platform with 8GB RAM, a 3.7 GHz Core processor, and Intel(R) HD Graphics 530. Experimental results are provided in this section.

4.1 The cipher images and decrypted images

Test images of "Lena", "Cameraman", "Peppers", "House" and "Lake" with the size of 512×512 are shown in **Fig. 6**(a), (d), (g), (j) and (m), and that with the size of 256×256 are displayed in **Fig. 7**(a), (d), (g), (j) and (m). The parameters in the test are shown in **Table 1**. The approximate component and three sets of detail components are transformed into a 256×512 image. The cipher "Lena", "Cameraman", "Peppers", "House" and "Lake" with the size of 256×512 are shown by **Fig. 6**(b), (e), (h), (k) and (n). Without interference signal, **Fig. 6**(c), (f), (i), (l) and (o) display the decrypted image "Lena", "Cameraman", "Peppers", "House" and "Lake" with the correct secret keys, respectively. Similarly, the encrypted and decrypted results of the same test images (256×256) are shown in **Fig. 7**. The simulation results show that the size of cipher images is reduced by 50% and the recovered images after decryption look the same as the plain images visually.

Table 1. Test parameters.

Items	Parameter values
256-bit hash value (denoted in hexadecimal form)	B 6 8 A 4 1 6 0 2 7 0 0 1 8 3 7 0 1 9 1 7 9 3 7 A 5 8 1 E F D 6 9 D C 8 7 A F D 3 4 6 5 5 D 9 2 9 4 4 0 4 8 E 6 5 9 4 9 8 4 6 7
Logistic map	$x_{01} = 0.78,\ a_{01} = 3.98;\ x_{02} = 0.84,\ a_{02} = 3.99$ $x_{03} = 0.54,\ a_{03} = 3.96;\ x_{04} = 0.38 + \frac{x_{02}}{100} + \frac{x_{05}}{100},\ a_{04} = 3.89 + \frac{a_{02}}{100}$

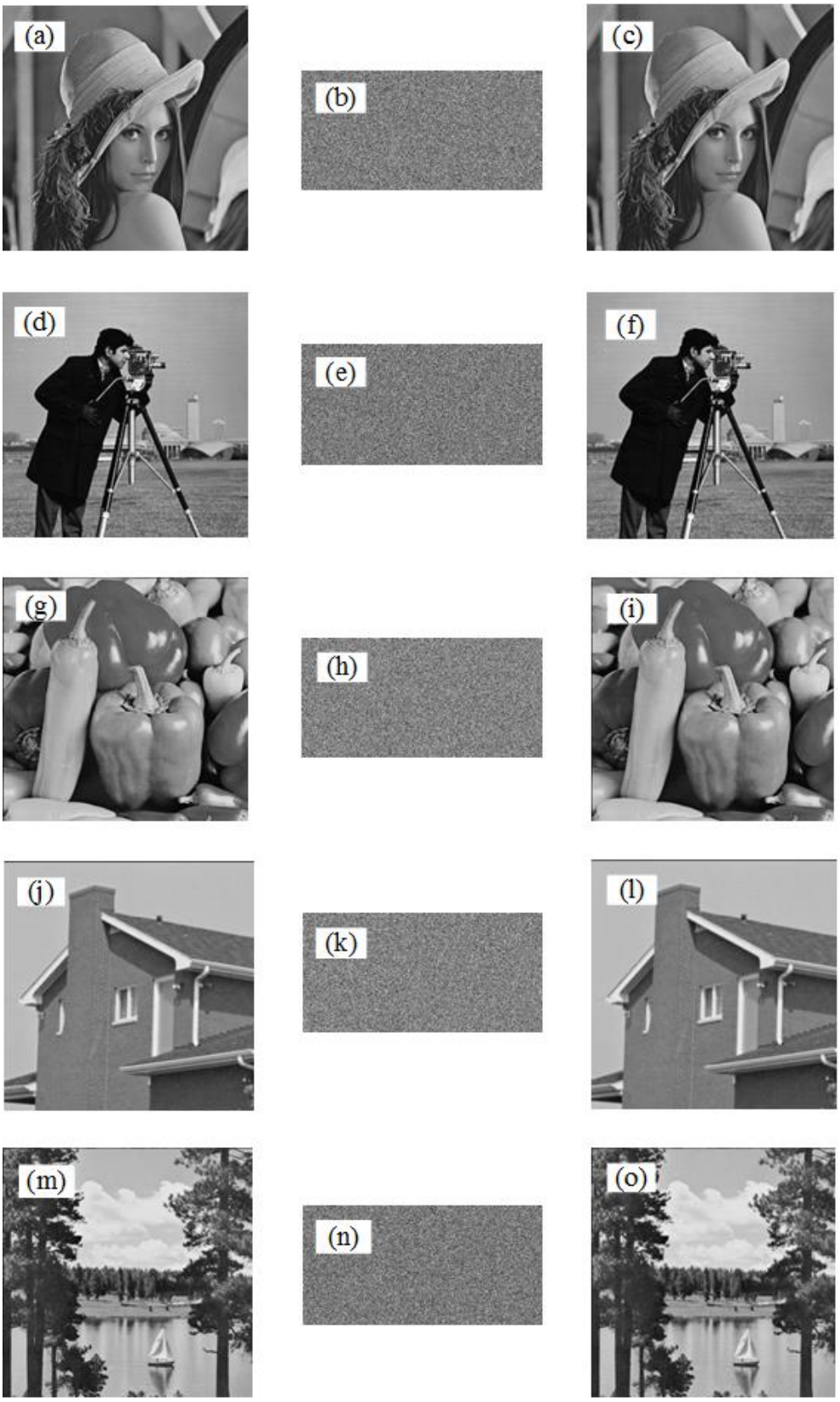


Fig. 6. Plain images (512×512) and the results of cipher images (256×512). (a), (b), (c) represent the original, cipher and decrypted images of "Lena", respectively. (d), (e), (f) represent the original, cipher and decrypted images of "Cameraman", respectively. (g), (h), (i) are the original, cipher and decrypted images of "Peppers", respectively. (j), (k), (l) are the original, cipher and decrypted images of "House", respectively. (m), (n), (o) are the original, cipher and decrypted images of "Lake", respectively.

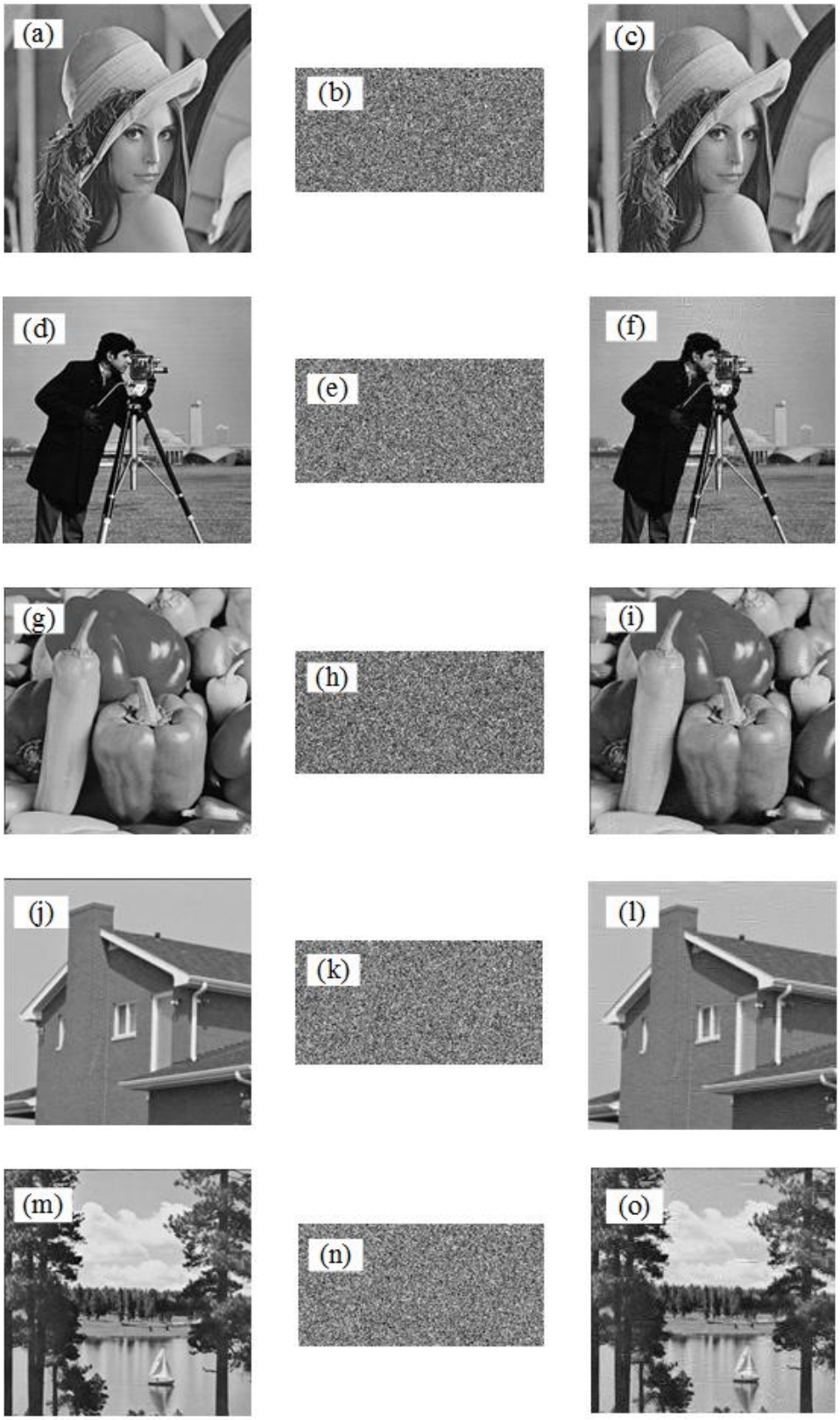


Fig. 7. Plain images (256×256) and the results of cipher images (128×256). (a), (b), (c) represent the original, cipher and decrypted images of "Lena", respectively. (d), (e), (f) represent the original, cipher and decrypted images of "Cameraman", respectively. (g), (h), (i) are the original, cipher and decrypted images of "Peppers", respectively. (j), (k), (l) are the original, cipher and decrypted images of "House", respectively. (m), (n), (o) are the original, cipher and decrypted images of "Lake", respectively.

4.2 Histogram analysis

Histogram distribution of encrypted result is one of the basic criteria to evaluate the security and effectiveness of the cryptosystem. In general, although the histograms of the test images are totally dissimilar,

the corresponding encrypted images should present similar histogram distributions[51]–[53][65]. **Fig. 8**(a), (c), (e), (g) and (i) display the histograms of the original images “Lena”, “Cameraman”, “Peppers”. “House” and “Lake” with the size of 512×512. **Fig. 8**(b), (d), (f), (h) and (j) are the histograms distribution of the corresponding cipher images. Similarly, histogram analysis is also applied on the same test with the size of 256×256. **Fig. 9**(a), (c), (e), (g) and (i) are the histograms of original “Lena”, “Cameraman”, “Peppers”. “House” and “Lake” with the size of 256×256, and the histograms of respective encrypted images are shown in **Fig. 9**(b), (d), (f), (h) and (j). As shown in **Fig. 8** and **Fig. 9**, the histograms distribution of three original images are quite diverse but their corresponding cipher images histograms are almost similar regardless of the image size. Therefore, the CES is capable of resisting the basic statistical analysis attack and preventing the attackers from getting the useful information by analysing the histogram distribution.

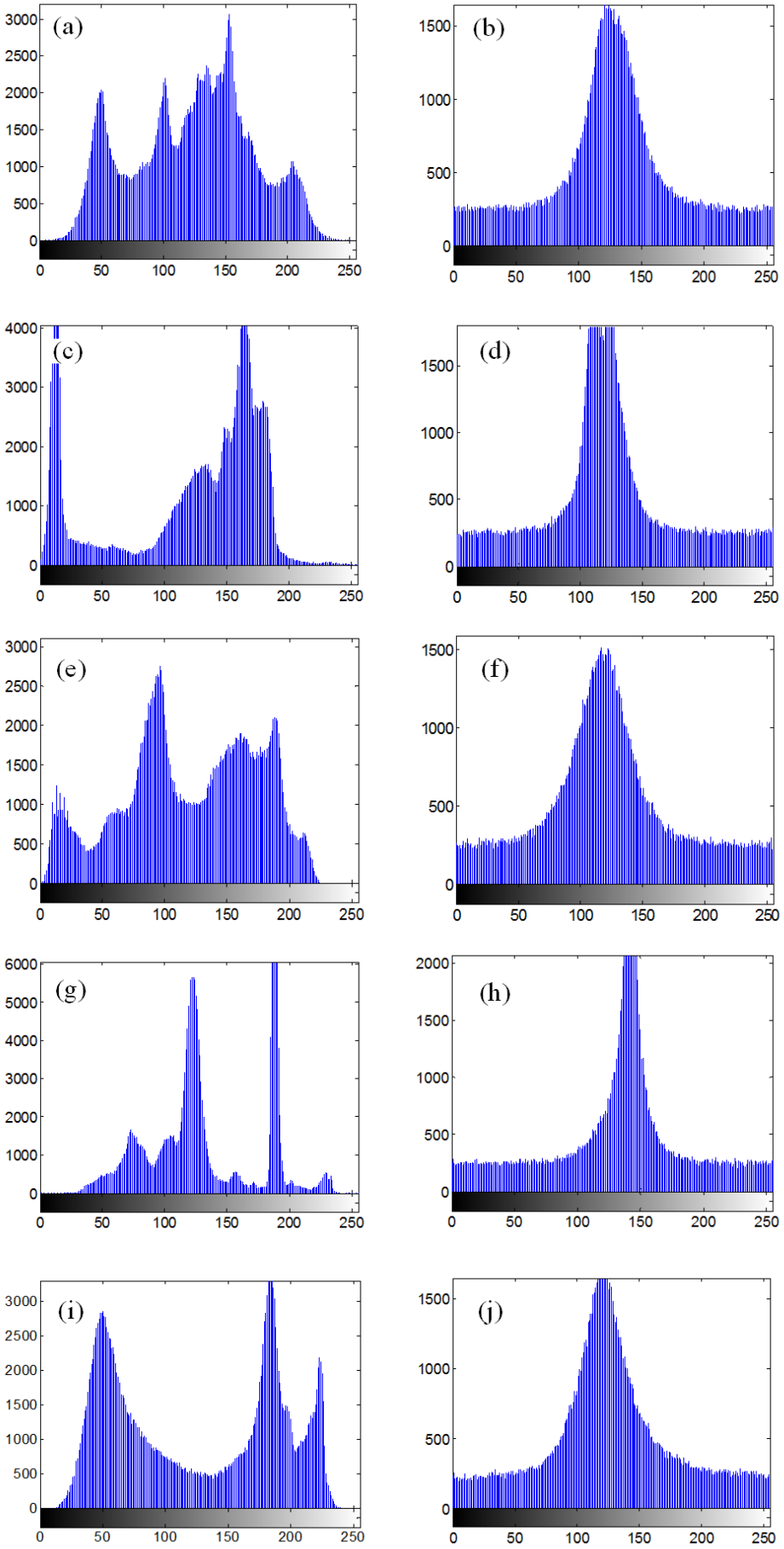


Fig. 8. Histograms of the different plain images (512×512) and encrypted images (256×512). (a) "Lena", (b) encrypted "Lena", (c) "Cameraman", (d) encrypted "Cameraman", (e) "Peppers", (f) encrypted "Peppers", (e) "House", (f) encrypted "House", (e) "Lake", (f) encrypted "Lake".

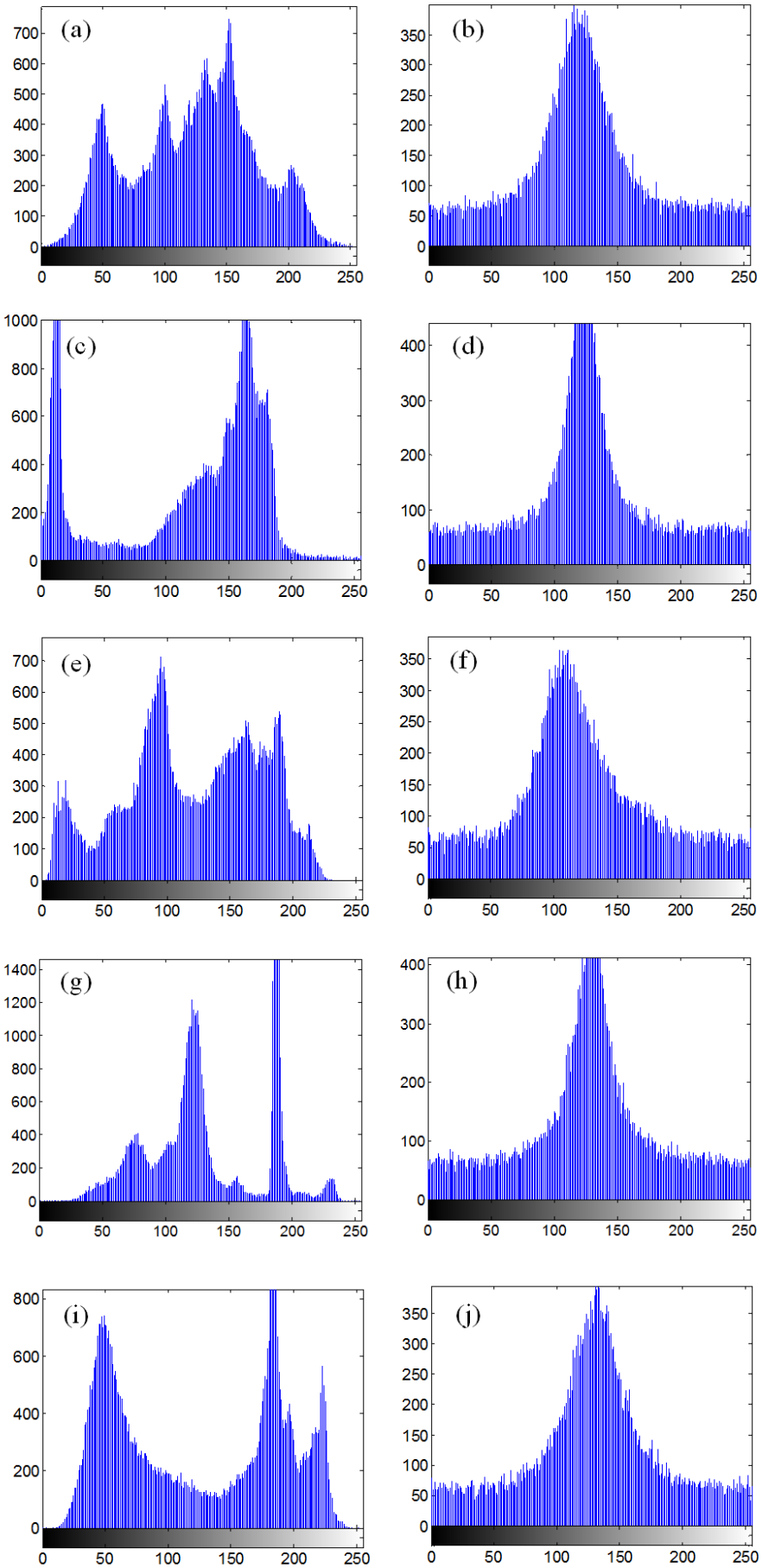


Fig. 9. Histograms of the different plain images (256×256) and encrypted images (128×256). (a) "Lena", (b) encrypted "Lena", (c) "Cameraman", (d) encrypted "Cameraman", (e) "Peppers", (f) encrypted "Peppers", (e) "House", (f) encrypted "House", (e) "Lake", (f) encrypted "Lake".

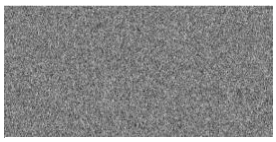
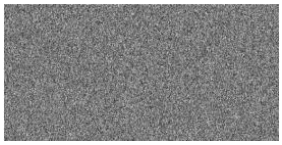
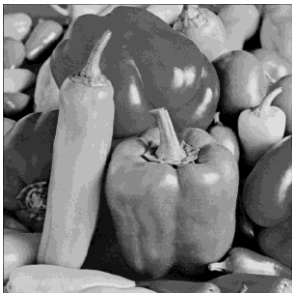
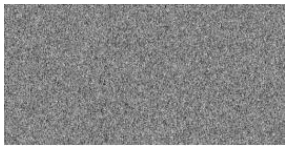
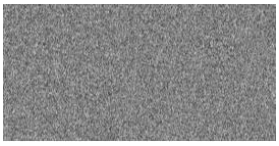
4.3 Compression performance

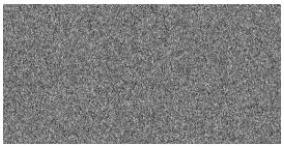
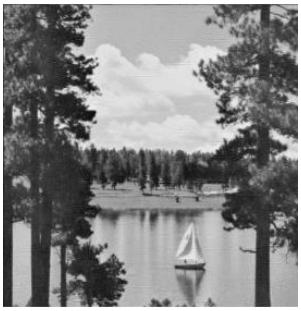
As for this CES architecture, CS is only used on the detail components of the wavelet domain. So the cipher data can be reduced, i.e., compression ratio (CR) of this CES is 0.5. Moreover, the peak signal-to-noise ratio (PSNR) is usually employed to estimate the quality of the decrypted image, and it can be calculated by

$$\mathrm{PSNR} = 10\log\frac{255^2}{(1/\mathrm{N}^2)\sum_{\mathrm{i}=1}^{\mathrm{N}}\sum_{\mathrm{j}=1}^{\mathrm{N}}[\mathrm{D(i,j)}-\mathrm{I(i,j)}]^2} \tag{29}$$

where $\mathrm{D(i,j)}$ and $\mathrm{I(i,j)}$ represent the reconstructed image and the plain image, respectively. And the PSNR test result is shown in **Table 2**. The experimental data illustrates the PSNR values of the images are all about 30dB which demonstrates the reconstructed images can be well recognized through the CES architecture.

Table 2. PSNR values of different images after reconstruction.

Original Image(512×512)	Compressed and encrypted image	Decrypted image	PSNR(dB)
			34.5560
			34.6995
			31.5132
			37.2577

29.2165

Besides, structural similarity index (SSIM) is an index of the similarity between two images [66] and human visual system (HSV) mainly obtains structural information from visible regions. Thus, the approximate information of image distortion can be perceived by detecting whether the structural information has any changes. Usually, mean SSIM (MSSIM) index is used to estimate the quality of the reconstructed images, and it is described by

$$\begin{cases} \mathrm{MSSIM}(X,Y) = \frac{1}{W}\sum_{p=1}^{W} \mathrm{SSIM}(X_p, Y_p) \\ \mathrm{SSIM}(X,Y) = L(\mathrm{X},\mathrm{Y}) \times C(\mathrm{X},\mathrm{Y}) \times S(\mathrm{X},\mathrm{Y}) \end{cases} \tag{30}$$

where $W = 64$, $L(X,Y) = \frac{2u_X u_Y + C_1}{u_X^2 + u_Y^2 + C_1}$, $C(\mathrm{X},\mathrm{Y}) = \frac{2\sigma_X \sigma_Y + C_2}{\sigma_X^2 + \sigma_Y^2 + C_2}$, and $S(\mathrm{X},\mathrm{Y}) = \frac{\sigma_{XY} + C_3}{\sigma_X \sigma_Y + C_3}$ in which X and Y are the pixel sequences of the original image and the reconstructed image, u_X and u_Y are the mean values of X and Y, σ_X and σ_Y are the standard deviations of X and Y, σ_X^2 and σ_Y^2 represent the variances of X and Y, σ_{XY} is the covariance of X and Y. Besides, C_1, C_2 and C_3 are the constants in order to avoid the denominator equalling to 0, that is, $C_1 = (K_1 \times L)^2$, $C_2 = (K_2 \times L)^2$, $C_3 = \frac{C_2}{2}$, $K_1 = 0.01$, $K_2 = 0.03$, and $L = 255$.

Generally, when the MSSIM value is close to 0, it illustrates the reconstructed image is hugely different from the original image, otherwise, it indicates the reconstructed image is very similar to the plaintext when the MSSIM value approximates to 1. The experimental results when the CR is 0.5 is shown in **Table 3**, which shows that the MSSIM values of different test images (512×512) are all very close to 1, and the MSSIM values of this work for Lena image and Pepper image are larger than that of [65]. Therefore, it can be seen the compression ability of the proposed scheme is good for different images and the volume of transferred data can be well reduced.

Table 3. The MSSIM values of the algorithms with CR=0.5.

Original image (512×512)	Algorithms	MSSIM
	Proposed algorithm	0.9995
	In [65]	0.9964

	Proposed algorithm	0.9991
	In [65]	N/A
	Proposed algorithm	0.9994
	In [65]	0.9727
	Proposed algorithm	0.9992
	In [65]	N/A
	Proposed algorithm	0.9996
	In [65]	N/A

4.4 Performance evaluation of proposed measurement matrix

The performance evaluation is tested by comparing the recovered results of the proposed measurement matrix with the same algorithm using other random measurement matrices including Gaussian matrix, Bernoulli matrix and Toeplitz matrix. PSNR value is treated as the evaluation criterion to describe the reconstruction performance in detail. In this paper, five different images “Lena”, “Cameraman”, “Peppers”, “House” and “Lake” with the size of 512×512 are used as the test images, and the CR is 0.5. Compressive sensing is applied on the encoding process of the proposed scheme with the above four measurement matrices. After that, the reconstructed images are obtained by doing decoding operation with the respective measurement matrix. As shown in **Fig. 10**, the proposed measurement matric generated by Lissajous map presents similar PSNR value compared to that of Gaussian matrix, Bernoulli matrix and Toeplitz matrix. Therefore, the test results prove that the measurement matrix of this work owns good performance and effectiveness in compressive sensing. Simultaneously, it has no negative effect on image reconstruction.

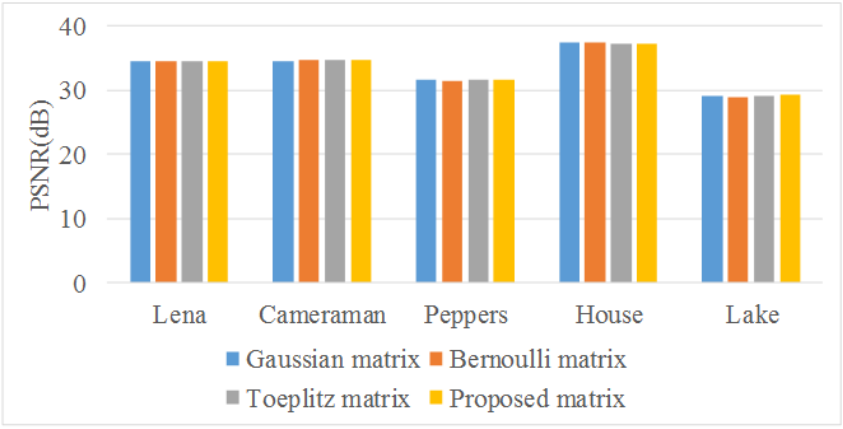


Fig. 10. PSNR values of the reconstruction results using different measurement matrices.

4.5 Correlation coefficient analysis

Natural image always has strong correlation (commonly close to 1) among pixels. However, the correlation of encrypted image is expected to be close to 0, which means the association between pixels is greatly eliminated. The correlation coefficient could be obtained by

$$C = \frac{\sum_{i=1}^{N}(x_i-\overline{x})(y_i-\overline{y})}{\sqrt{(\sum_{i=1}^{N}(x_i-\overline{x})^2)(\sum_{i=1}^{N}(y_i-\overline{y})^2)}}, \tag{31}$$

where $\overline{x} = (1/N)\sum_{i=1}^{N} x_i$, $\overline{y} = (1/N)\sum_{i=1}^{N} y_i$.

Table 4 gives the correlation coefficients between adjacent pixels of both the cipher and original image (256×256) in three directions (horizontal, vertical and diagonal directions), respectively. The pixels in natural images are strongly correlated to each other and correlation coefficients tend to be larger than 0.85. But the cipher image owns weak correlation between the neighbouring pixels and correlation coefficients almost equal to 0 commonly. Compared with the algorithms in [51], [52][67], the cryptosystem in this work obtains better performance from the data shown in **Table 4**. Besides, **Fig. 11** also shows the correlation between pixels of plain-text is very strong but that of the corresponding encrypted image is really weak. Therefore, it demonstrates that attackers cannot get effective information by using the statistical attack due to the weak correlation of cipher image.

Table 4. Correlation coefficients of adjacent pixels of the proposed method and other algorithms.

Algorithm	Image (256×256)	Horizontal	Vertical	Diagonal
	Original Lena	0.9250	0.8856	0.8526
Proposed algorithm	Encrypted Lena	0.0069	-0.0028	-0.0047
In [51]		0.0846	0.0583	0.0931
In [52]		0.0104	0.0299	0.0062
In [67]		0.0442	0.0382	0.0631
	Original Cameraman	0.9488	0.9129	0.8820
Proposed algorithm	Encrypted Cameraman	-0.0044	-0.0054	0.0025

In [51]		0.0639	0.0539	0.0848
In [52]		N/A	N/A	N/A
In [67]		N/A	N/A	N/A
	Original Peppers	0.9520	0.9436	0.9160
Proposed algorithm	Encrypted Peppers	0.0074	0.0035	0.0041
In [51]		0.0787	0.0582	0.0873
In [52]		0.0385	0.0296	0.0069
In [67]		0.0387	0.0182	0.0473
	Original House	0.9475	0.9719	0.9263
Proposed algorithm	Encrypted House	-0.0065	0.0072	-0.0044
In [51]		N/A	N/A	N/A
In [52]		N/A	N/A	N/A
In [67]		N/A	N/A	N/A
	Original Lake	0.9264	0.9325	0.8936
Proposed algorithm	Encrypted Lake	-0.0084	-0.0028	0.0033
In [51]		N/A	N/A	N/A
In [52]		N/A	N/A	N/A
In [67]		0.0239	0.0134	0.0448

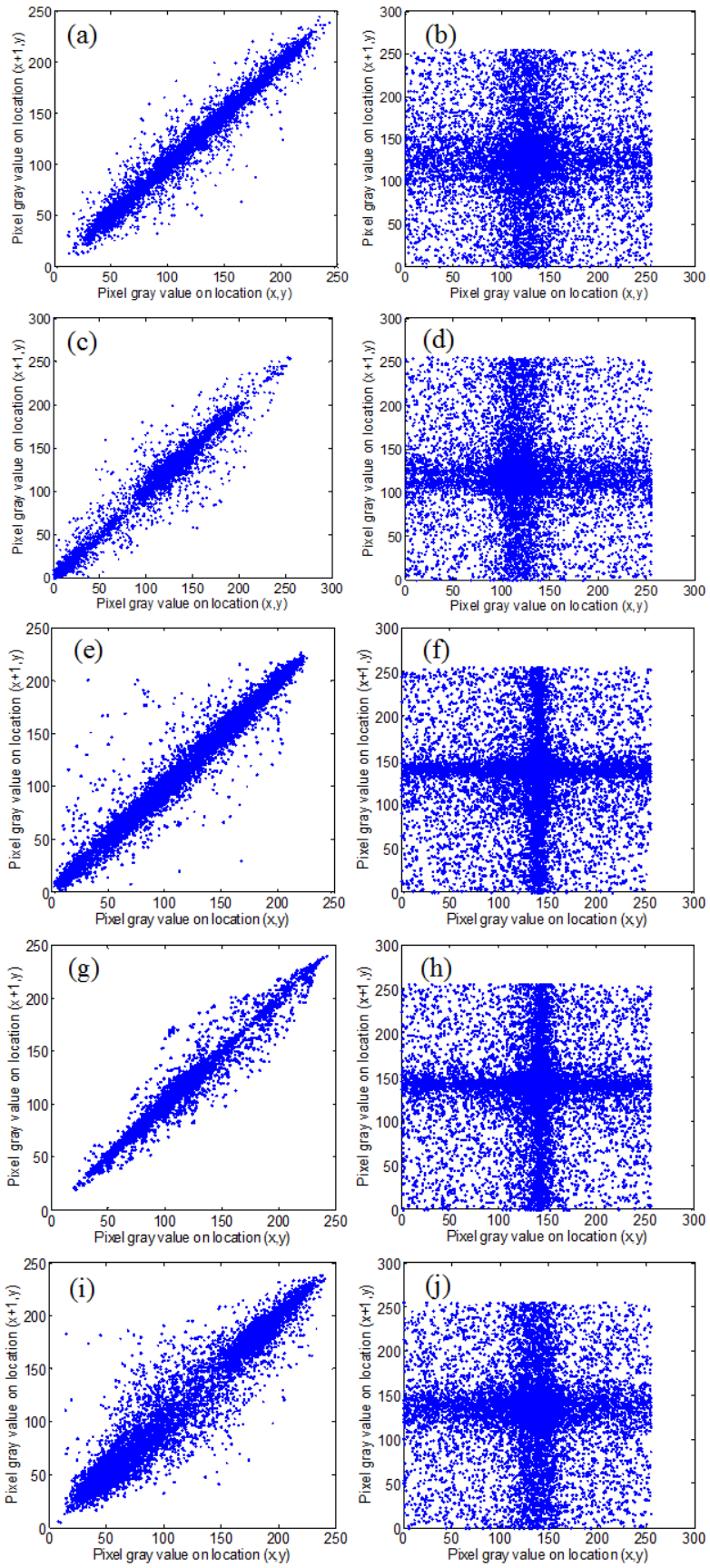


Fig. 11. Correlation distribution of the original images and the corresponding cipher images in the horizontal direction. (a) original "Lena", (b) encrypted "Lena", (c) original "Cameraman", (d) encrypted "Cameraman", (e) original "Peppers", (f) encrypted "Peppers", (g) original "House", (h) encrypted "House", (i) original "Lake", and (j) encrypted "Lake".

4.6 Key space analysis

Large key space can prevent the attackers from getting the correct keys and improve the ability of resisting the common attack such as brute-force attack. The key space can be assessed by using mean absolute error (MAE), which is given by

$$\mathrm{MAE}(\gamma,\gamma') = \frac{1}{M\times N}\sum_{I=1}^{M\times N}|\gamma_i - \gamma_i'|, \tag{32}$$

where γ_i and γ_i' represent the sequences generated by initial values x_{01} and $x_{01}+\Delta$ (Δ is the key deviation), length of γ_i and γ_i' are both $M\times N$. $1/\Delta_0$ is the key space of x_0, where Δ_0 is one of the value Δ that satisfies $\mathrm{MAE}(\gamma,\gamma')=0$. In this CES, the space of secret key x_{01} is 10^{15}. Similarly, $x_{02}, x_{03}, x_{04}, a_{01}, a_{02}, a_{03}, a_{04}$ have the same key space as x_{01}. Thus the whole key space of the 8 parameters is about 10^{120}, which is larger than 2^{360}. And the subspace of x_{05} equals to 10^{12} as well as the y_{01}, y_{02} and y_{03}. In summary, the total key space of this CES is $2^{360}+2^{144}$ which is much larger than that in the [51][68]–[71] from the data shown in **Table 5**. Therefore, the proposed algorithm owns a large key space and can be fairly effective against the exhaustive searching and brute-force attack.

Table 5. Key space comparison with other algorithms.

Algorithm	Proposed	In [51]	In [68]	In [69]	In [70]	In [71]
Key space	$2^{360}+2^{144}$	10^{34}	2^{276}	10^{56}	2^{149}	10^{60}

4.7 Key-sensitivity analysis

A secure cryptosystem should own good key sensitivity, i.e. a tiny variation in secret key should cause dramatic changes in the cipher image. To illustrate the difference between plaintext image and decrypted image with different keys, the key sensitivity is evaluated by the mean square error (MSE) and it can be defined by

$$\mathrm{MSE} = \frac{1}{M\times N}\sum_{i,j}[I(i,j)-D(i,j)]^2, \tag{33}$$

where $M\times N$ is the size of the image, *I* and *D* denote the plain image and decrypted image. **Fig. 12** displays the restored "Lena" by wrong keys where each time only one key with a tiny deviation and the others remain unchanged, i.e., **Fig. 12**(a)-(l) represent the decrypted "Lena" by the incorrect keys with a little change ($10^{-13}\sim10^{-14}$). From **Fig. 12**, it can be concluded that the plaintext image is covered up even if a tiny deviation happens to the keys. **Fig. 13** displays the MSE curve for all the keys with tiny deviations. It is obvious that the MSE value is very large when one key for the decryption process has a tiny deviation and the others remain unchanged. However, the MSE value is quite small if all the correct keys are given. Accordingly, the proposed CES owns quite high sensitivity to the secret keys which makes the attackers hardly obtain the useful information by the brute force.

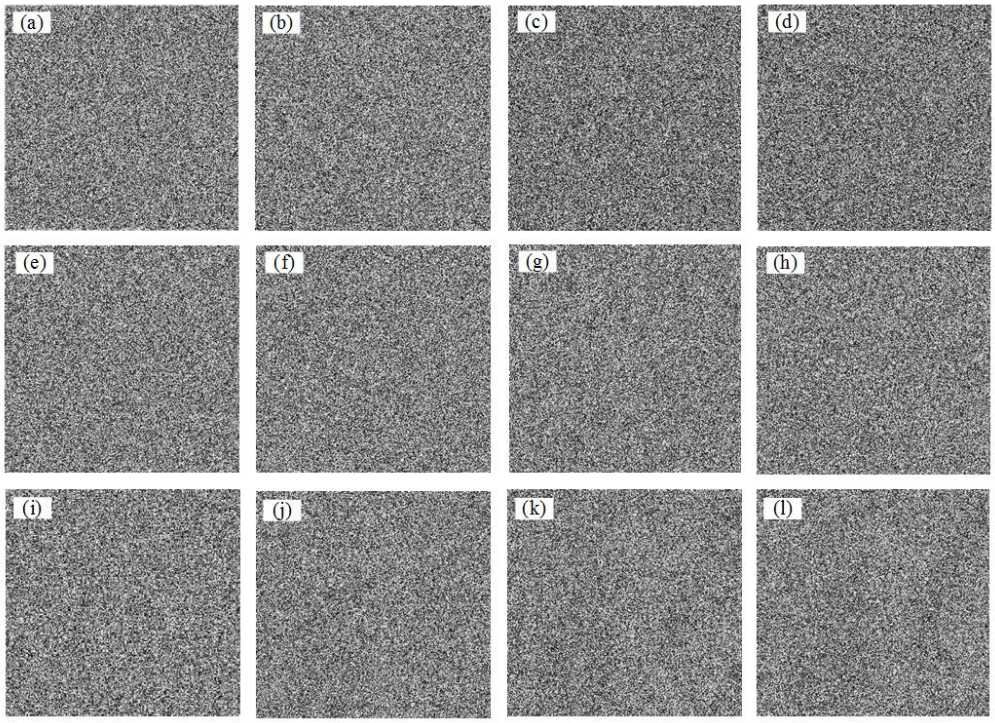


Fig. 12. Decrypted "Lena" using incorrect keys with the changes of (a) $x_{01} + 10^{-14}$, (b) $a_{01} + 14$, (c) $x_{02} + 10^{-14}$, (d) $a_{02} + 10^{-14}$, (e) $x_{03} + 10^{-14}$, (f) $a_{03} + 10^{-14}$, (g) $x_{04} + 10^{-14}$, (h) $x_{05} + 10^{-13}$, (i) $a_{04} + 10^{-14}$, (j) $y_{01} + 10^{-13}$, (k) $y_{02} + 10^{-13}$ and (l) $y_{03} + 10^{-13}$.

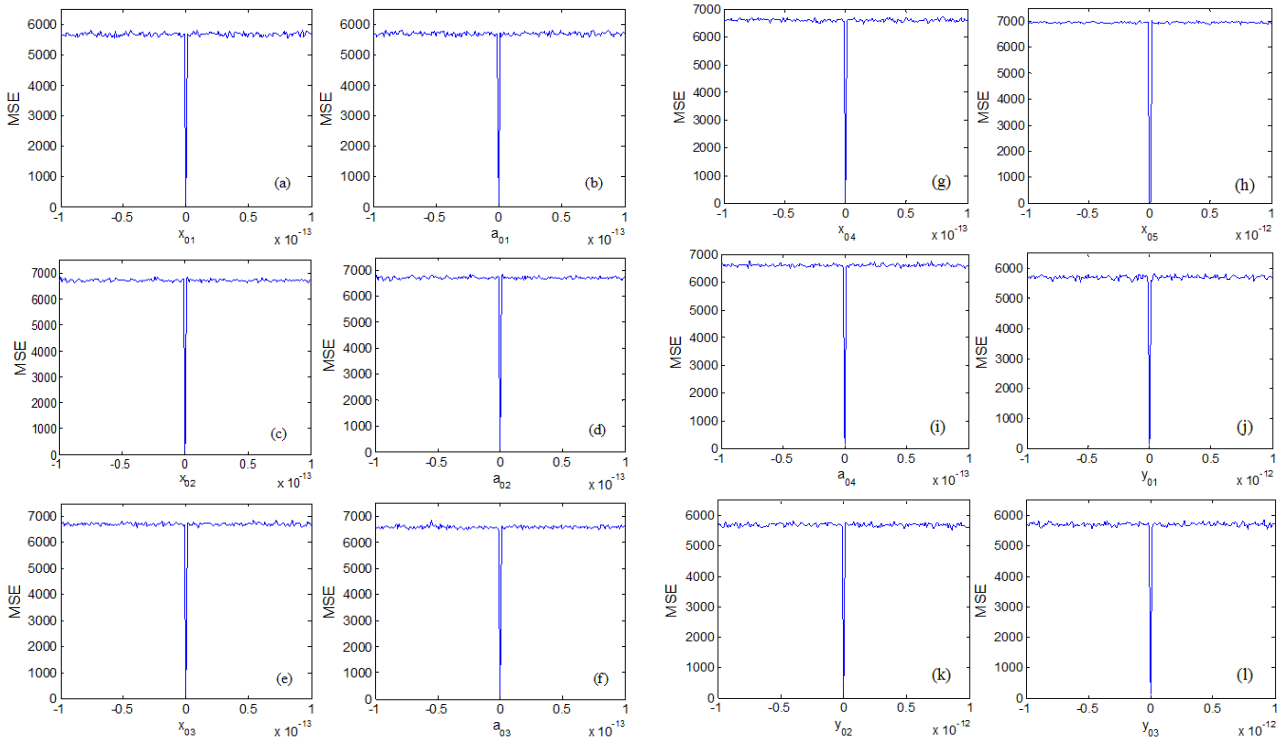


Fig. 13. MSE curves. (a) x_{01}, (b) a_{01}, (c) x_{02}, (d) a_{02}, (e) x_{03}, (f) a_{03}, (g) x_{04}, (h) x_{05}, (i) a_{04}, (j) y_{01}, (k) y_{02} and (l) y_{03}.

4.8 Known/Chosen plaintext attack

Known/chosen plaintext attack is commonly used to get the useful information of the original image. Therefore, some effective procedures are implemented to resist known/chosen plaintext attack. Specifically,

the low frequency partial coefficient LL is sensitive to the initial parameters y_{01}, y_{02}, y_{03}, which serve as the keys for Chua's circuit which is used to confuse the LL subband. In the proposed algorithm, y_{01}, y_{02}, y_{03} are produced by using SHA-256 hash function according to the plain image, so a tiny change in the original image may bring completely different keys. Hence, the LL subband which contains the main information of one image is prevented from known/chosen plaintext attack. In addition, the detail components LH, HL and HH have a strong relationship with control value x_{05}, which is also generated by SHA-256 hash function. Besides, x_{05} is used to iterate the Lissajous map to form the CADRMM, and the measurement matrices $\boldsymbol{\Phi_{LH\_HH}}$ for LH and HH subband, and $\boldsymbol{\Phi_{HL}}$ for HL subband will all vary according to the original image. Accordingly, the LH, HL and HH subband are also robust against known/chosen plaintext attack. Furthermore, the correlation between algorithm and the plaintext are improved. Without the correct diffusion matrix and measurement matrix, the attackers cannot obtain the original image by known/chosen plaintext attack.

4.9 Occlusion-attack analysis

The occlusion-attack may occur during transmission due to network breakdown, i.e., part of the encrypted image may be lost in transmission [72]. Robustness of CES is determined by whether the useful information can be restored correctly. The robustness is tested by dropping some information in different directions from the encrypted results. In this paper, the encrypted image (**Fig. 6**(b)) suffered the occlusion attack from different positions with diverse sizes. As shown in **Fig. 14**, **Fig. 14**(a1)-(a3) illustrate 1/32 data (64×64) of the encrypted image in left corner, middle and right corner is lost respectively, and the reconstructed images are displayed in **Fig. 14**(a4)-(a6). Analogously, the encrypted image with data loss of 1/16 data (64×128), 1/8 data (128×128), 1/4 data (128×256) and 1/2 data (256×256) in three different positions are shown in **Fig. 14**(b1)-(b3), **Fig. 14**(c1)-(c3), **Fig. 14**(d1)-(d3) and **Fig. 14**(e1)-(e3). The corresponding recovered images are indicated in **Fig. 14**(b4)-(b6), **Fig. 14**(c4)-(c6), **Fig. 14**(d4)-(d6) and **Fig. 14**(e4)-(e6), respectively. It can be obtained that the restored image becomes blurred as the amount of data loss increases. However, the outline of the image can still be identified even if half of the image is lost.

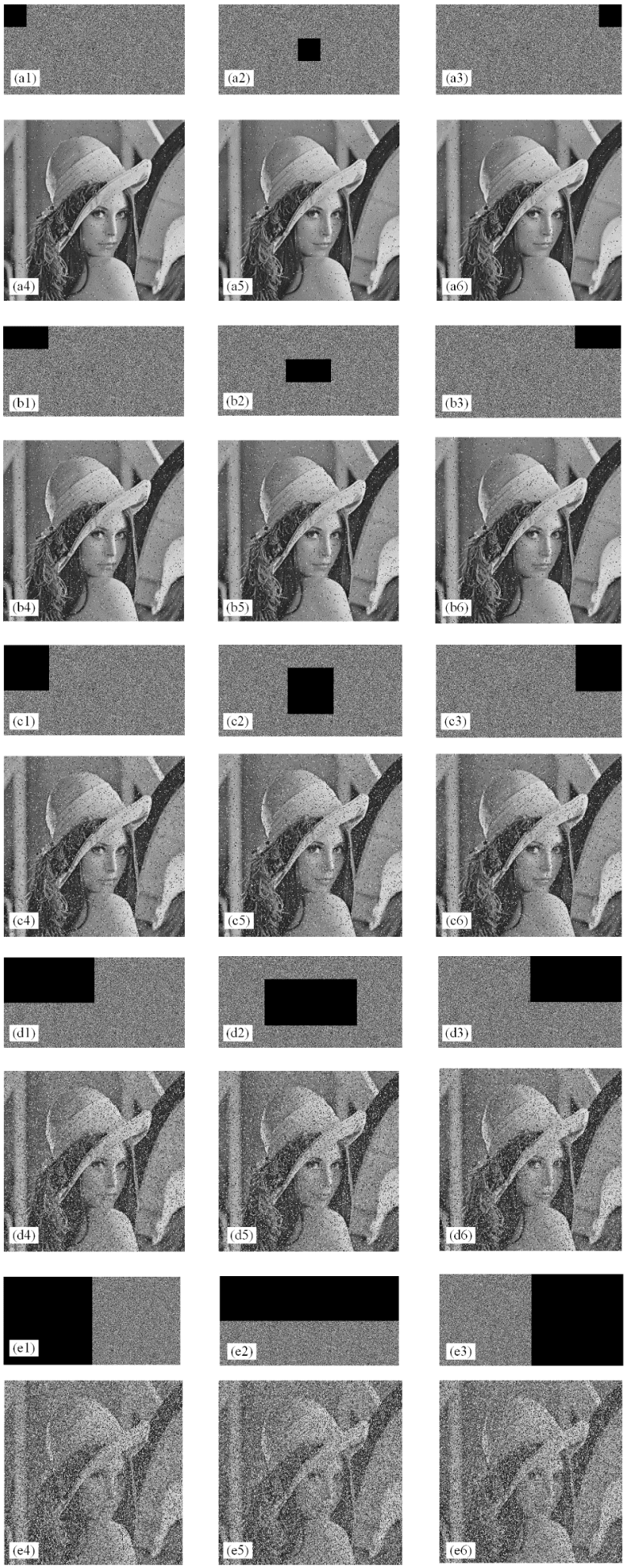


Fig. 14. The decrypted results of the encrypted image suffering from occlusion attack.

Moreover, PSNR value is another index to evaluate the performance of occlusion attack. **Table 6** illustrates that the PSNR is around 23.5804dB in three different positions when the size of data is 1/32. With the increase of information loss, the PSNR values gradually decline. When the half of the encrypted image is lost, the PSNR comes down to 12.0534dB in average.

Therefore, the proposed algorithm is capable of resisting serious occlusion-attack analysis. Accordingly, the robustness of the image in real time transmission channel can also be guaranteed.

Table 6. PSNR between the recovered images and the plain images with occlusion attack of different position and size.

Position and size	Left corner PSNR(dB)	Middle area PSNR(dB)	Right corner PSNR(dB)	Average PSNR(dB)
1/2 data loss	12.0874	12.0520	12.0209	12.0534
1/4 data loss	14.9623	14.8832	14.9057	14.9170
1/8 data loss	17.8726	17.8270	17.8443	17.8479
1/16 data loss	20.7884	20.6804	20.6902	20.7196
1/32 data loss	23.5937	23.6092	23.5384	23.5804

4.10 Noise attack analysis

During the transmission, images can be contaminated by different kinds of noises. Salt & Pepper noise(SPN), Gaussian noise(GN) and Speckle noise(SN) are three typical common noises in transmission [73]. So the noises are added to the cipher, and the ability of the proposed algorithm is evaluated according to the recovered images. In this paper, the noise level is set between 0.000001 and 0.000007. **Fig. 15**(a)-(d) show the encrypted images (**Fig. 6**(b)) with Salt & Pepper noise intensity equals to 0.000001, 0.000003, 0.000005 and 0.000007, respectively. The corresponding decryption images are shown in **Fig. 15**(e)-(h). Similarly, the reconstructed images under Gaussian noise and Speckle noise are displayed in **Fig. 16**(e)-(h) and **Fig. 17**(e)-(h). It can be seen that the extent of damage becomes more serious with the increase of noise intensity. However, the reconstructed images can still be recognized clearly, even if the noise intensity is 0.000007.

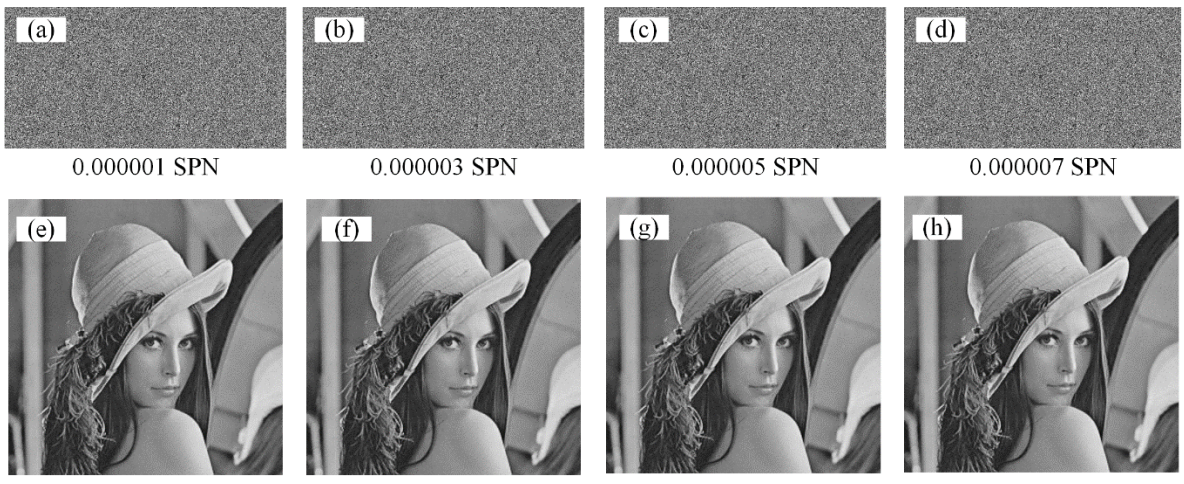


Fig. 15. The reconstructed images under Salt & Pepper noise attack with different noise intensities.

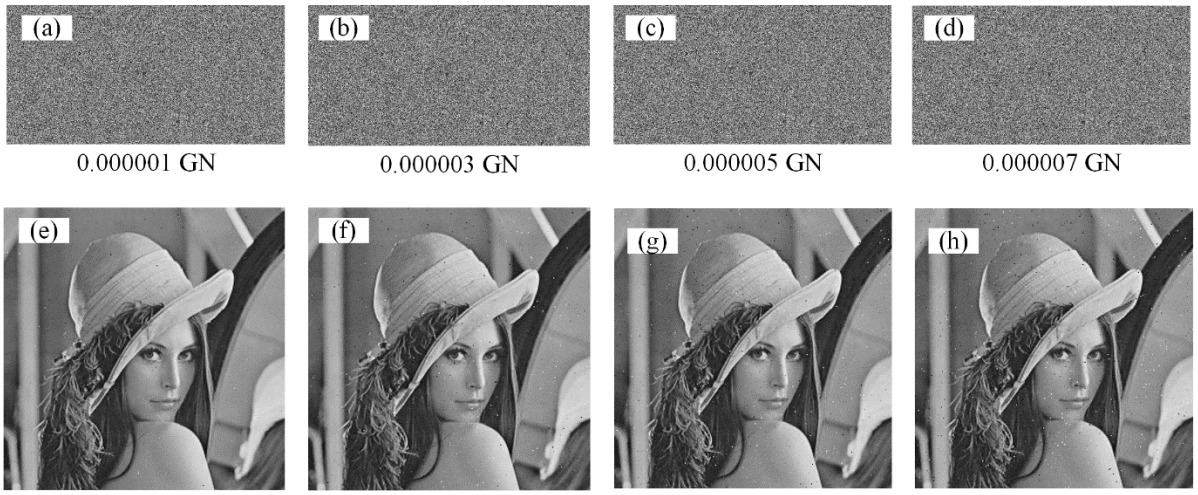


Fig. 16. The reconstructed images under Gaussian noise attack with different noise intensities.

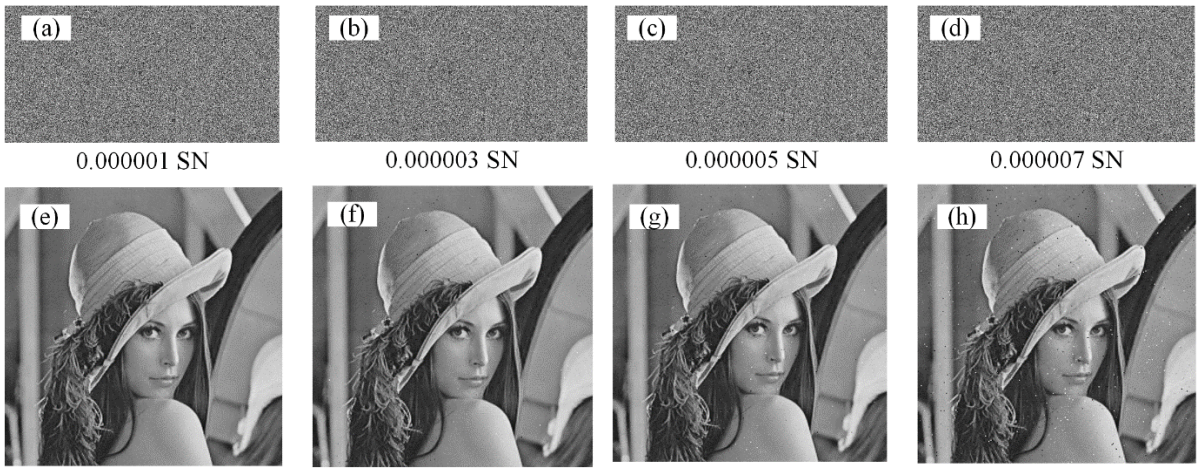


Fig. 17. The reconstructed images under Speckle noise attack with different noise intensities.

Moreover, the PSNRs of the reconstructed images for the plain image Lena in the case of different noise are fully illustrated in **Table 7.** Among the three kinds of noise, Gaussian noise has the greatest impact on restored images and the PSNRs change from 33.85dB to 29.46dB when the noise intensity varies from 0.000001 to 0.000007. Besides, the PSNRs of the Salt & Pepper noise stay at around 34.48dB with different intensities and it shows there is the excellent ability to resist Salt & Pepper noise for the proposed scheme. Besides, the PSNRs are limited in the range of [31.82dB, 34.49dB] when suffered from Speckle noise which illustrates there is little negative effect on the restored images for Speckle noise. In addition, **Fig. 18** shows the more detailed changing trend of PSNRs between the recovered image and original image under three noise attacks in this work and **Fig. 19** displays the trend in [65]. Compared with the decrypted results in [65], this proposed scheme has relatively higher PSNRs under the same conditions which demonstrates the proposed encryption algorithm has good robustness against different kinds of noise attacks under different intensities.

Table 7. Comparison with other algorithm under different noise.

Noise	Algorithm	Noise intensity	PSNR(dB)
SPN	Proposed algorithm	0.000001	34.49
	In [65]		31.05
	Proposed algorithm	0.000003	34.49
	In [65]		N/A
	Proposed algorithm	0.000005	34.48
	In [65]		N/A
	Proposed algorithm	0.000007	34.47
	In [65]		27.93
GN	Proposed algorithm	0.000001	33.85
	In [65]		30.10
	Proposed algorithm	0.000003	30.85
	In [65]		N/A
	Proposed algorithm	0.000005	30.07
	In [65]		N/A
	Proposed algorithm	0.000007	29.46
	In [65]		25.39
SN	Proposed algorithm	0.000001	34.49
	In [65]		31.05
	Proposed algorithm	0.000003	33.70
	In [65]		N/A
	Proposed algorithm	0.000005	32.87
	In [65]		N/A
	Proposed algorithm	0.000007	31.82
	In [65]		30.99

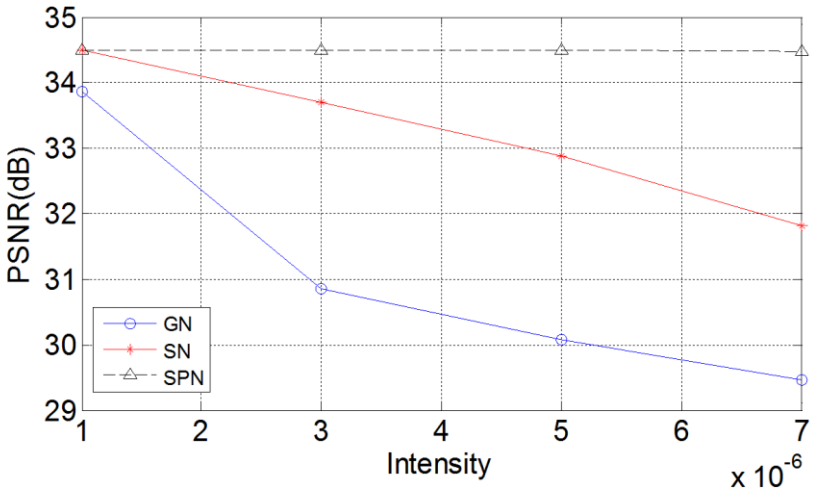


Fig. 18. PSNR between the recovered image and original image under three noise attacks.

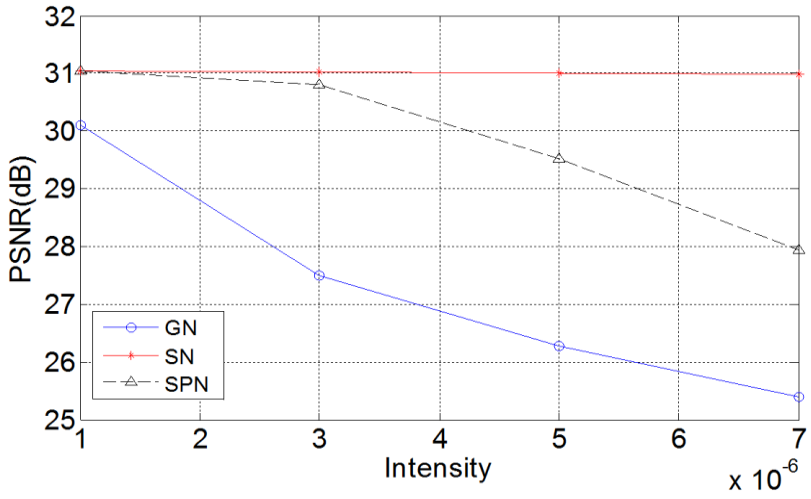


Fig. 19. PSNR under three noise attacks in [65].

4.11 Time analysis

Time consumption is another important criterion to test the performance of an encryption algorithm, and it is also considered in this work. Specifically, the encryption process includes five main operations: diffusion matrix generation, *LL* subband diffusion, measurement matrix generation, measurement process and matrix combination distribution. The corresponding time test distribution for the Lena (256×256) under the condition of CR=0.5 is shown in **Fig 20**, which illustrates 0.389459s is required to complete the whole encryption. Besides, it can be seen that the process of diffusion matrix generation occupies the most time in the whole encryption procedure, i.e., it takes around 53.15%. Meanwhile, the encrypted speed for different images is experimented and tested, and the results are shown in **Table 8** and **Table 9**. From **Table 8**, it can be seen the encryption time for the images with the size of 256×256 is around 0.4s and that of the images with size of 512×512 is around 1.2s. In addition, the corresponding decryption time is experimented and listed in **Table 10** and **Table 11**. Similarly, the decryption time for the images with 256×256 is about 0.9s and that of images with 512×512 is about 6.7s. Because in the decryption process, the measurement matrix is needed and it greatly related with the size of image. So, a larger image usually needs a larger measurement matrix to reconstruct to consume more time.

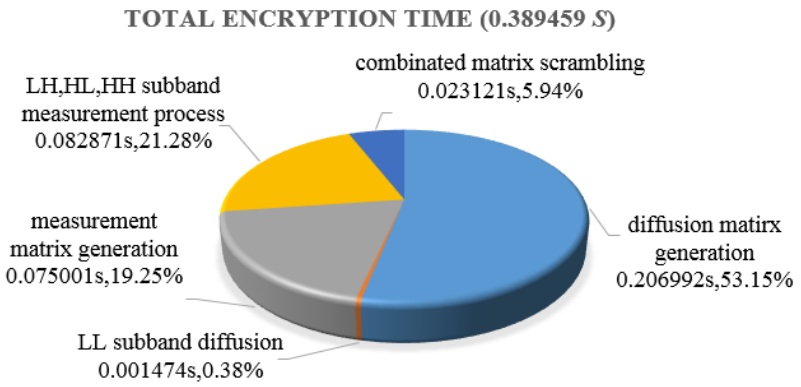


Fig 20. Total encryption time and time consumption percentage of each part in the algorithm for Lena (256×256).

Table 8. Encryption speed of the test images with the size of 256×256 (s).

Image (256×256)	Lena	Cameraman	Peppers	House	Lake	Baboon
Proposed algorithm	0.3895	0.3960	0.3987	0.3946	0.3924	0.4296

Table 9. Encryption speed of the test images with the size of 512×512 (s).

Image (512×512)	Lena	Cameraman	Peppers	House	Lake	Baboon
Proposed algorithm	1.1843	1.1926	1.1801	1.1894	1.1706	1.1715

Table 10. Decryption speed of the test images with the size of 256×256 (s).

Image (256×256)	Lena	Cameraman	Peppers	House	Lake	Baboon
Proposed algorithm	0.8751	0.9710	0.9254	0.9262	0.9041	0.9544

Table 11. Decryption speed of the test images with the size of 512×512 (s).

Image (512×512)	Lena	Cameraman	Peppers	House	Lake	Baboon
Proposed algorithm	6.6910	6.7360	6.6234	6.8272	6.7743	6.7308

To compare the effectiveness of this work, the execution time is compared with other related encryption schemes shown in **Table 12** and **Table 13**. The data in **Table 12** shows the proposed scheme has better encryption efficiency than that in [65] and [74], and the decryption time consumption of this work is also shorter than other reference schemes in **Table 13**. Thus, the proposed method provides sound security as well as low time complexity.

Table 12. Encryption speed comparison with other algorithms (s).

Image	Lena (256×256)	Baboon (256×256)	Peppers (256×256)	Cameraman (512×512)	House (512×512)	Lake (512×512)
Proposed algorithm	0.39	0.43	0.40	1.20	1.19	1.18
In [65]	0.58	0.47	0.66	N/A	N/A	N/A
In [74]	2.25	2.55	2.76	N/A	N/A	N/A

Table 13. Decryption speed comparison with other algorithms (s).

Image	Cameraman	Lake	Baboon	Lena	House	Peppers

	(256×256)	(256×256)	(256×256)	(512×512)	(512×512)	(512×512)
Proposed algorithm	0.98	0.91	0.96	6.70	6.83	6.63
In [65]	N/A	N/A	2.09	14.02	N/A	13.41
In [74]	N/A	N/A	N/A	N/A	N/A	N/A

5. Conclusion

A novel compression-encryption scheme is proposed in this paper, which is based on chaos-combined asymptotic deterministic random measurement matrices, Haar wavelet and Chua's circuit. Specifically, the plain image is decomposed into approximate component and detail components through Haar wavelet transform beforehand. The wavelet coefficients of the detail components are mapped to 8-bit integer numbers before XOR operation, and then a mixed system which combines Chua's circuit with logistic map and the threshold processing of LBP operator-based theory are used to generate mask. In addition, the chaos-combined asymptotic deterministic random sequence is used to produce the CADRMM to measure detail components in case of different compression ratios and improve scrambling degree. Finally, approximate component and detail components are assembled together before scrambling. Due to that the approximate component is retained and only the detail components are compressed, the robustness of this CES can be significantly improved, i.e., the experimental results demonstrate it still has good robustness even under the strong occlusion and noise attacks. In the meantime, the performance and security analysis indicate that the proposed scheme has a large key space, high key sensitivity, similar histogram distribution and weak coefficient correlation. Therefore the proposed scheme is not only able to reduce the data amount for the image transmission but also has a good security performance.

6. Acknowledgements

This research was supported by the National Natural Science Foundation of China under Grants 61801131, 61661008 and 11562004, the Guangxi Natural Science Foundation under Grants 2017GXNSFAA198180 and 2016GXNSFCA380017, the funding of Overseas 100 Talents Program of Guangxi Higher Education, 2018 Guangxi One Thousand Young and Middle-Aged College and University Backbone Teachers Cultivation Program, the Science and Technology Major Project of Guangxi under Grant AA18118004, the Doctoral Research Foundation of Guangxi Normal University under Grant 2016BQ005.

References

[1] Y. Luo, L. Cao, S. Qiu, H. Lin, J. Harkin, and J. Liu, "A chaotic map-control-based and the plain image-related cryptosystem," *Nonlinear Dyn.*, vol. 83, no. 4, pp. 2293–2310, 2016.

[2] Y. Luo and M. Du, "A self-adapting image encryption algorithm based on spatiotemporal chaos and ergodic matrix," *Chinese Phys. B*, vol. 22, no. 8, pp. 1–9, 2013.

[3] Y. Luo, M. Du, and J. Liu, "A symmetrical image encryption scheme in wavelet and time domain," *Commun. Nonlinear Sci. Numer. Simul.*, vol. 20, no. 2, pp. 447–460, 2015.

[4] Y. Zhang, H. Huang, Y. Xiang, Z. Leo Yu, and H. Xing, "Harnessing the hybrid cloud for secure big image data service," *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1380–1388, 2017.

[5] Y. Zhang *et al.*, "Low-cost and confidentiality-creserving data acquisition for internet of multimedia things," *IEEE Internet Things J.*, vol. 5, no. 5, pp. 3442–3451, 2018.

[6] C. Pak and L. Huang, "A new color image encryption using combination of the 1D chaotic map," *Signal Processing*, vol. 138, pp. 129–137, 2017.

[7] G. Ye and X. Huang, "An efficient symmetric image encryption algorithm based on an intertwining logistic map," *Neurocomputing*, vol. 251, no. C, pp. 45–53, 2017.

[8] R. Zahmoul, R. Ejbali, and M. Zaied, "Image encryption based on new Beta chaotic maps," *Opt. Lasers Eng.*, vol. 96, pp. 39–49, 2017.

[9] H. Huang, X. He, Y. Xiang, W. Wen, and Y. Zhang, "A compression-diffusion-permutation strategy for securing image," *Signal Processing*, vol. 150, pp. 183–190, 2018.

[10] Y. Zhang and L. Y. Zhang, "Exploiting random convolution and random subsampling for image encryption and compression," *Electron. Lett.*, vol. 51, no. 20, pp. 1572–1574, 2015.

[11] Q. Liu, P. Li, M. Zhang, Y. Sui, and H. Yang, "A novel image encryption algorithm based on chaos maps with Markov properties," *Commun. Nonlinear Sci. Numer. Simul.*, vol. 20, no. 2, pp. 506–515, 2015.

[12] S. N. George, "PWLCM based image encryption through compressive sensing," in *Recent Advances in Intelligent Computational Systems (RAICS)*, 2013, pp. 48–52.

[13] R. Huang and K. Sakurai, "A robust and compression-combined digital image encryption method based on compressive sensing," in *International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, 2011, pp. 2–5.

[14] AthiraV, S. N. George, and D. P. P, "A novel encryption method based on compressive sensing," in *International Mutli-Conference on Automation, Computing, Communication, Control and Compressed Sensing (iMac4s)*, 2013, pp. 271–275.

[15] Y. Zhang, L. Y. Zhang, J. Zhou, L. Liu, F. Chen, and X. He, "A review of compressive sensing in information security field," *IEEE Access*, vol. 4, pp. 2507–2519, 2016.

[16] D. Zhang, X. Liao, B. Yang, and Y. Zhang, "A fast and efficient approach to color-image encryption based on compressive sensing and fractional Fourier transform," *Multimed. Tools Appl.*, vol. 77, no. 9, pp. 2191–2208, 2018.

[17] Y. Zhang, Y. Xiang, L. Y. Zhang, Y. Rong, and S. Guo, "Secure wireless communications based on compressive sensing : A survey," *IEEE Commun. Surv. Tutorials*, pp. 1–19, 2018.

[18] L. Y. Zhang, K. Wong, Y. Zhang, and J. Zhou, "Bi-level protected compressive sampling," *IEEE Trans. Multimed.*, vol. 18, no. 9, pp. 1720–1732, 2016.

[19] Y. Zhang, K. Wong, L. Yu, and W. Wen, "Robust coding of encrypted images via structural matrix," *Signal Process. Commun.*, vol. 39, no. PA, pp. 202–211, 2015.

[20] Y. Zhang *et al.*, "A block compressive sensing based scalable encryption framework for protecting," *Int. J. Bifurc. Chaos*, vol. 26, no. 11, pp. 1–15, 2016.

[21] S. El Assad and M. Farajallah, "A new chaos-based image encryption system," *Signal Process. Commun.*, vol. 41, no. C, pp. 144–157, 2016.

[22] B. Wang, Y. Xie, C. Zhou, S. Zhou, and X. Zheng, "Evaluating the permutation and diffusion operations used in image encryption based on chaotic maps," *Opt. - Int. J. Light Electron Opt.*, vol. 127, no. 7, pp. 3541–3545, 2016.

[23] H. Liu, A. Kadir, and X. Sun, "Chaos-based fast colour image encryption scheme with true random number keys from environmental noise," *IET Image Process.*, vol. 11, no. 5, pp. 324–332, 2017.

[24] H. Liu, A. Kadir, and Y. Niu, "Chaos-based color image block encryption scheme using S-box," *Int. J. Electron. Commun.*, vol. 68, no. 7, pp. 676–686, 2014.

[25] A. Belazi, A. El-latif, and S. Belghith, "A novel image encryption scheme based on substitution-permutation network and chaos," *Signal Processing*, vol. 128, pp. 155–170, 2016.

[26] J. Chen, Z. Zhu, C. Fu, H. Yu, and L. Zhang, "A fast chaos-based image encryption scheme with a dynamic state variables selection mechanism," *Commun Nonlinear Sci Numer Simulat*, vol. 20, no. 3, pp. 846–860, 2015.

[27] G. Zhou, D. Zhang, Y. Liu, Y. Yuan, and Q. Liu, "A novel image encryption algorithm based on chaos and Line map," *Neurocomputing*, vol. 169, pp. 150–157, 2015.

[28] N. K. Pareek, V. Patidar, and K. K. Sud, "Image encryption using chaotic logistic map," *Image Vis. Comput.*, vol. 24, no. 9, pp. 926–934, 2006.

[29] X. Wu, H. Kan, and J. Kurths, "A new color image encryption scheme based on DNA sequences and multiple improved 1D chaotic maps," *Appl. Soft Comput. J.*, vol. 37, no. C, pp. 24–39, 2015.

[30] Y. Zhou, L. Bao, and C. L. P. Chen, "A new 1D chaotic system for image encryption," *Signal Processing*, vol. 97, no. 7, pp. 172–182, 2014.

[31] C. Li, S. Li, G. Alvarez, and G. Chen, "Cryptanalysis of a chaotic block cipher with external key and its improved version," *Chaos, Solitons and Fractals*, vol. 37, no. 1, pp. 299–307, 2008.

[32] S. Mohammad and S. Mirzakuchaki, "A fast color image encryption algorithm based on coupled two-dimensional piecewise chaotic map," *Signal Processing*, vol. 92, no. 5, pp. 1202–1215, 2012.

[33] H. Zhu, C. Zhao, and X. Zhang, "A novel image encryption-compression scheme using hyper-chaos and Chinese remainder theorem," *Signal Process. Commun.*, vol. 28, no. 6, pp. 670–680, 2013.

[34] A. Kanso and M. Ghebleh, "A novel image encryption algorithm based on a 3D chaotic map," *Commun Nonlinear Sci Numer Simulat*, vol. 17, no. 7, pp. 2943–2959, 2012.

[35] Y. Li, C. Wang, and H. Chen, "A hyper-chaos-based image encryption algorithm using pixel-level permutation and bit-level permutation," *Opt. Lasers Eng.*, vol. 90, pp. 238–246, 2017.

[36] Q. Zhang, L. Guo, and X. Wei, "Image encryption using DNA addition combining with chaotic maps," *Math. Comput. Model.*, vol. 52, no. 11–12, pp. 2028–2035, 2010.

[37] R. Enayatifar, A. Hanan, and I. F. Isnin, “Chaos-based image encryption using a hybrid genetic algorithm and a DNA sequence,” *Opt. Lasers Eng.*, vol. 56, pp. 83–93, 2014.

[38] X. Wang, Y. Zhang, and X. Bao, “A novel chaotic image encryption scheme using DNA sequence operations,” *Opt. Lasers Eng.*, vol. 73, pp. 53–61, 2015.

[39] X. Chai, Y. Chen, and L. Broyde, “A novel chaos-based image encryption algorithm using DNA sequence operations,” *Opt. Lasers Eng.*, vol. 88, pp. 197–213, 2017.

[40] H. Liu and X. Wang, “Color image encryption using spatial bit-level permutation and high-dimension chaotic system,” *Opt. Commun.*, vol. 284, no. 16, pp. 3895–3903, 2011.

[41] L. Xu, Z. Li, J. Li, and W. Hua, “A novel bit-level image encryption algorithm based on chaotic maps,” *Opt. Lasers Eng.*, vol. 78, pp. 17–25, 2016.

[42] H. Liu, D. Xiao, R. Zhang, Y. Zhang, and S. Bai, “Robust and hierarchical watermarking of encrypted images based on compressive sensing,” *Signal Process. Commun.*, vol. 45, no. C, pp. 41–51, 2016.

[43] M. Li, D. Xiao, and Y. Zhang, “Reversible data hiding in block compressed sensing images,” *Etri J.*, vol. 38, no. 1, pp. 159–163, 2016.

[44] G. Hu, D. Xiao, T. Xiang, S. Bai, and Y. Zhang, “A compressive sensing based privacy preserving outsourcing of image storage and identity authentication service in cloud,” *Inf. Sci. (Ny).*, vol. 387, pp. 132–145, 2017.

[45] H. Liu, D. Xiao, Y. Xiao, and Y. Zhang, “Robust image hashing with tampering recovery capability via low-rank and sparse representation,” *Multimed. Tools Appl.*, vol. 75, no. 13, pp. 7681–7696, 2016.

[46] Y. Zhang, L. Y. Zhang, J. Chen, and Y. Zhang, “On the security of optical ciphers under the architecture of compressed sensing combining with double random phase encoding,” *IEEE Photonics J.*, vol. 9, no. 4, pp. 1–11, 2017.

[47] Y. Zhang, J. Zhou, F. Chen, L. Yu, K. Wong, and X. He, “Embedding cryptographic features in compressive sensing,” *Neurocomputing*, vol. 205, pp. 472–480, 2016.

[48] X. Zhang, Y. Ren, G. Feng, and Z. Qian, “Compressing encrypted image using compressive sensing,” in *International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, 2011, pp. 222–225.

[49] R. Huang, K. H. Rhee, and S. Uchida, “A parallel image encryption method based on compressive sensing,” *Multimed. Tools Appl.*, vol. 72, no. 1, pp. 71–93, 2014.

[50] Sreedhanya.A.V and D. K. P. Soman, “Secrecy of cryptography with compressed sensing,” in *International Conference on Advances in Computing and Communications*, 2012, pp. 207–210.

[51] N. Zhou, A. Zhang, F. Zheng, and L. Gong, “Novel image compression-encryption hybrid algorithm based on key-controlled measurement matrix in compressive sensing,” *Opt. Laser Technol.*, vol. 62, no. 10, pp. 152–160, 2014.

[52] N. Zhou, H. Li, D. Wang, S. Pan, and Z. Zhou, “Image compression and encryption scheme based on 2D compressive sensing and fractional Mellin transform,” *Opt. Commun.*, vol. 343, pp. 10–21, 2015.

[53] Y. Zhang, B. Xu, and N. Zhou, “A novel image compression- encryption hybrid algorithm based on the analysis sparse representation,” *Opt. Commun.*, vol. 392, pp. 223–233, 2017.

[54] X. Chai, Z. Gan, Y. Chen, and Y. Zhang, “A visually secure image encryption scheme based on compressive sensing,” *Signal Processing*, vol. 134, pp. 35–51, 2017.

[55] N. Singh and A. Sinha, "Optical image encryption using Hartley transform and logistic map," *Opt. Commun.*, vol. 282, no. 6, pp. 1104–1109, 2009.

[56] C. T. Mullis *et al.*, "A Chaotic Attractor from Chua's Circuit," *IEEE Trans. Circuits Syst.*, vol. 31, no. 12, pp. 1055–1058, 1984.

[57] W. Yu and G. Bai, "A new high performance image encryption algorithm based on Chua's attractor," in *International Conference on Broadband Network and Multimedia Technology (IC-BNMT)*, 2010, pp. 874–878.

[58] C. Chupei, J. Li, and H. Deng, "An image encryption algorithm based on Chua's chaos and Baker's transformation," *Appl. Tech. Inf. Secur.*, pp. 36–43, 2015.

[59] R. G. Baraniuk, "Compressive Sensing," *IEEE Signal Process. Mag.*, vol. 24, no. 4, pp. 118–121, 2007.

[60] Y. C. Pati, R. Rezaiifar, and P. S. Krishnaprasad, "Orthogonal matching pursuit : recursive function approximation with applications to wavelet decomposition," in *Asilomar Conference on Signals Systems and Computers*, 1993, pp. 40–44.

[61] W. Dai and O. Milenkovic, "Subspace pursuit for compressive sensing signal reconstruction," *IEEE Trans. Inf. THEORY*, vol. 55, no. 5, pp. 2230–2249, 2009.

[62] S. S. Chen, D. L. Donoho, and M. A. Saunders, "Atomic decomposition by basis pursuit," *SIAM Rev.*, vol. 43, no. 1, pp. 129–159, 2001.

[63] D. Needell and J. A. Tropp, "CoSaMP : Iterative signal recovery from incomplete and inaccurate samples," *Appl. Comput. Harmon. Anal.*, vol. 26, no. 3, pp. 301–321, 2009.

[64] K. Wang, W. Pei, L. Zou, Y. Cheung, and Z. He, "The asymptotic deterministic randomness," *Phys. Lett. A*, vol. 368, no. 1–2, pp. 38–47, 2007.

[65] X. Chai, X. Zheng, Z. Gan, D. Han, and Y. Chen, "An image encryption algorithm based on chaotic system and compressive sensing," *Signal Processing*, vol. 148, pp. 124–144, 2018.

[66] Z. Wang, A. C. Bovik, H. R. Sheikh, and E. P. Simoncelli, "Image quality assessment : From error visibility to structural similarity," *IEEE Trans. IMAGE Process.*, vol. 13, no. 4, pp. 600–612, 2004.

[67] A. Orsdemir, H. O. Altun, G. Sharma, and M. F. Bocko, "On the security and robustness of encryption via compressed sensing," in *Military Communications Conference*, 2008, pp. 1–7.

[68] N. Zhou, S. Pan, S. Cheng, and Z. Zhou, "Image compression-encryption scheme based on hyper-chaotic system and 2D compressive sensing," *Opt. Laser Technol.*, vol. 82, pp. 121–133, 2016.

[69] D. Ponnaian and K. Chandranbabu, "Crypt analysis of an image compression-encryption algorithm and a modified scheme using compressive sensing," *Opt. - Int. J. Light Electron Opt.*, vol. 147, pp. 263–276, 2017.

[70] J. Chen, Y. Zhang, L. Qi, C. Fu, and L. Xu, "Exploiting chaos-based compressed sensing and cryptographic algorithm for image encryption and compression," *Opt. Laser Technol.*, vol. 99, pp. 238–248, 2018.

[71] G. Hu, D. Xiao, Y. Wang, and T. Xiang, "An image coding scheme using parallel compressive sensing for simultaneous compression-encryption applications," *J. Vis. Commun. Image Represent.*, vol. 44, no. C, pp. 116–127, 2017.

[72] X. Chai, Z. Gan, K. Yang, Y. Chen, and X. Liu, "An image encryption algorithm based on the memristive hyperchaotic system, cellular automata and DNA sequence operations," *Signal Process.*

Image Commun., vol. 52, no. March 2017, pp. 6–19, 2017.

[73] X. Chai, X. Fu, Z. Gan, Y. Lu, and Y. Chen, "A color image cryptosystem based on dynamic DNA encryption and chaos," *Signal Processing*, vol. 155, pp. 44–62, 2019.

[74] J. Ahmad and S. Oun, "A secure image encryption scheme based on chaotic maps and affine transformation," *Multimed. Tools Appl.*, vol. 75, no. 21, pp. 13951–13976, 2016.