



Full length article

Exploiting chaos-based compressed sensing and cryptographic algorithm for image encryption and compression

Junxin Chen^a, Yu Zhang^a, Lin Qi^a, Chong Fu^b, Lisheng Xu^{a,*}^a Sino-Dutch Biomedical and Information Engineering School, Northeastern University, Shenyang 110169, China^b School of Computer Science and Engineering, Northeastern University, Shenyang 110169, China

ARTICLE INFO

Article history:

Received 17 April 2017

Received in revised form 16 August 2017

Accepted 7 September 2017

Available online 28 September 2017

Keywords:

Image encryption

Compressed sensing

Structurally random matrix

3-D cat map

ABSTRACT

This paper presents a solution for simultaneous image encryption and compression. The primary introduced techniques are compressed sensing (CS) using structurally random matrix (SRM), and permutation-diffusion type image encryption. The encryption performance originates from both the techniques, whereas the compression effect is achieved by CS. Three-dimensional (3-D) cat map is employed for key stream generation. The simultaneously produced three state variables of 3-D cat map are respectively used for the SRM generation, image permutation and diffusion. Numerical simulations and security analyses have been carried out, and the results demonstrate the effectiveness and security performance of the proposed system.

© 2017 Elsevier Ltd. All rights reserved.

1. Introduction

With the significant developments of communication technologies, digital image application and exchange over Internet have become much more prevalent than the past. Cryptographic and compression approaches are therefore critical for real-time secure image transmission and storage over public networks, with the first phase prevent the information leakage and the latter for reducing the volume of the plaintext. However, traditional block ciphers such as Data Encryption Standard (DES), Advanced Encryption Standard (AES) are originally designed for encrypting textual data, and have been found poorly suited for digital images characterized with some intrinsic features such as high pixel correlation and redundancy [1–3]. With long-term efforts, researchers have noticed that the fundamental features of chaotic systems can be considered analogous to some ideal cryptographic properties for image encryption [4,5]. The properties of ergodic and high sensitivity to initial conditions and control parameters can be employed into both permutation and diffusion processes with satisfied efficiency and security. In [6], Fridrich proposed a general architecture for chaos-based image cipher. This architecture composes of two stages: permutation and diffusion. In the first phase, pixel locations are shuffled with the gray values unchanged, whereas they are then modified sequentially in the diffusion procedure. The permutation-diffusion architecture has drawn worldwide atten-

tions and a variety of successive variants have been subsequently proposed for secure image transmission [7–18]. Besides the security performance, compression is another important issue for real-time image transmission, especially for the scenarios such as battlefield medical online transmission where the bandwidth resource is critically valuable. However, the above cryptographic achievements are not suitable for encrypting compressed images and their ciphertext cannot be compressed either, as the redundancy of the plaintext has been removed in the encryption procedure. Meanwhile, compressed sensing (CS) [19,20] that is originally proposed as a revolutionary data acquisition technique has paved a novel perspective for simultaneous compression and encryption of plaintext, as the measurement matrix can be regarded as the secret key. It has been found in [21,22] that the measurement matrix of CS can guarantee the computational secrecy, whereas it is shown to be vulnerable to chosen-plaintext attack [23]. Fewer achievements have been proposed for simultaneous secure encryption and compression of natural images [24], which will be an attractive topic of nowadays image processing research.

This paper presents a solution for the simultaneous image encryption and compression, which consists of two primary stages with the first is the CS phase and the second one is a typical permutation-diffusion procedure. The three-dimensional (3-D) cat map [25] is introduced for key stream generation. With the iterations of cat map, three state variables are simultaneously produced, and they will be applied in the CS, permutation and diffusion processes respectively. In the CS procedure, structurally random matrix (SRM) [26] is adopted as the measurement matrix

* Corresponding author.

E-mail address: xuls@bmie.neu.edu.cn (L. Xu).

for compressed sampling the plain image. As described in [26], SRM consists of a diagonal matrix of Bernoulli random variables (or a uniform random permutation matrix), an orthonormal matrix such as the Discrete Cosine Transform (DCT) or Walsh-Hadamard Transform (WHT), and a subsampling operator. For the cryptographic and quantization issues, we propose to use chaos-based SRM mechanism, i.e., the Bernoulli random variables of SRM is generated under the control of 3-D cat map. Such a design embeds cryptographic feature into the CS phase, which makes CS contributes both compression and encryption performances. With respect to the weak resistance of CS against chosen-plaintext attack [23], typical permutation-diffusion image encryption procedure is developed subsequently to the CS phase. Empirically, the measurements of CS are generally with non-square size. Regarding this, a permutation approach based on chaotic-sorting technique (PACT) is investigated for arbitrary shape image shuffling, and the pixel masking operations are carried out subsequently in the diffusion phase for modifying the pixel values. The primary innovations of the proposed cryptosystem can be summarized as: (a) secret compressed sensing is developed with a chaos-based generation mechanism for SRM; (b) making full use of the chaotic variables so as to promote the operation efficiency; (c) PACT is investigated for shuffling plaintexts with various sizes; (d) more robustness against various attacks using cascaded compressed sensing and permutation-diffusion framework. Numerical simulations and security analyses have been carried out, and the results well validate the effectiveness and security of the proposed scheme.

The remainder of this paper is organized as follows. Some preliminaries are presented in Section 2, while the proposed scheme is described in Section 3. Simulation results and security analyses are addressed in Section 4. Finally, conclusions will be drawn in the last section.

2. Preliminaries

2.1. The 3-D cat map

In the proposed scheme, 3-D cat map is employed for key stream generation. The so-called 3-D cat map is the extension of classical two-dimensional Arnold cat map, as given out in Eq. (1), where the notation $x \bmod 1$ is used for the fractional parts of a real number x by subtracting or adding an appropriate number.

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

The map is area-preserving, as the determinant of its linear transformation matrix is equal to 1. The Lyapunov exponents are the eigenvalues of the matrix of Eq. (1), described as

$$\sigma_1 = \frac{1}{2}(3 + \sqrt{5}) > 1, \sigma_2 = \frac{1}{2}(3 - \sqrt{5}) < 1,$$

which implies the chaotic feature of cat map. The typical cat map is always generalized by introducing two parameters to Eq. (1), as follows:

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{bmatrix} 1 & a \\ b & ab + 1 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} \bmod 1. \quad (2)$$

In [25], the map given by Eq. (2) is extended to three dimensional, as described in Eqs. (3) and (4). The map is also invertible and area-preserving as the determinant of A is equal to 1.

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \\ z_{n+1} \end{bmatrix} = A \begin{bmatrix} x_n \\ y_n \\ z_n \end{bmatrix} \bmod 1. \quad (3)$$

$$A = \begin{bmatrix} 1 + a_x a_z b_y & a_z & a_y + a_x a_z + a_x a_y a_z b_y \\ b_z + a_x b_y + a_x a_z b_y b_z & a_z b_z + 1 & a_y a_z + a_x a_y a_z b_y b_z + a_x a_z b_z + a_x a_y b_y + a_x \\ a_x b_x b_y + b_y & b_x & a_x a_y b_x b_y + a_x b_x + a_y b_y + 1 \end{bmatrix}. \quad (4)$$

As a special case which is adopted in our scheme, by simply setting $a_x = b_x = a_y = b_y = a_z = b_z = 1$, we can directly obtain the 3-D cat map, as described in Eq. (5).

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

As investigated in [25], the Lyapunov characteristic exponents of the 3-D cat map are

$$\sigma_1 = 7.1842 > 1, \sigma_2 = 0.2430 < 1, \sigma_3 = 0.5728 < 1.$$

The leading Lyapunov characteristic exponent is significantly larger than 1 and larger than that of 2-D cat map, which implies that 3-D cat map is more chaotic than its 2-D version and is more suitable for data mixing.

Different from the cases of [25,27] where the 3-D cat map is further discretized for pixel location shuffling, the standard version of 3-D cat map will be used in our scheme. With the iterations of 3-D cat map, three series of chaotic state variables are simultaneously produced, and they will be subsequently used in the CS and permutation-diffusion processes.

2.2. Compressed sensing

The CS renders a solution for recovering a length- N signal \mathbf{f} from its linear measurements $\mathbf{y} = \Phi \mathbf{f}$, where Φ is the measurement matrix with fewer rows than columns. Generally, this system of equations has infinitely many solutions, as the equation is underdetermined. Yet, the CS will give exact solution by exploiting the potential of sparse theory, under the assumption that \mathbf{f} can be expressed as Eq. (6), where Ψ denotes the transformation matrix and \mathbf{s} is the transform coefficients of \mathbf{f} in the Ψ domain.

$$\mathbf{f} = \Psi \mathbf{s}. \quad (6)$$

The signal \mathbf{f} is said to be K -sparse if there are at most K non-zero coefficients in the Ψ domain, i.e., \mathbf{s} has at most K non-zero values. Besides, it is said to be compressible if \mathbf{f} can be well approximated using only K larger coefficients. In this case, the measurement process can be rewritten as Eq. (7), where \mathbf{y} is the sampled vector with $M \ll N$ data points, Φ represents a $M \times N$ measurement matrix and Θ is the sensing matrix.

$$\mathbf{y} = \Phi \mathbf{f} = \Phi \Psi \mathbf{s} = \Theta \mathbf{s}. \quad (7)$$

The revolutionary finding of CS is that the signal \mathbf{f} can be faithfully recovered with overwhelming probability from only $M = O(K \log N)$ measurements if Θ satisfies the restricted isometry property (RIP) [19,20]. In this case, the recovery of \mathbf{f} can be achieved by solving the following convex optimization problem

$$\min \|\mathbf{s}\|_1 \quad \text{s.t. } \Theta \mathbf{s} = \mathbf{y}, \quad (8)$$

and hence to further reconstruct $\mathbf{f} = \Psi \mathbf{s}$. Convex optimization algorithms [19,20] or greedy pursuit method such as Orthogonal Matching Pursuit (OMP) [28] can be employed.

One of the critical issues of CS framework is the construction of a proper measurement matrix Φ satisfying: (1) optimal recovery performance; (2) universality with almost all sparsifying basis for RIP requirements; (3) low complexity; and (4) hardware/optics implementation friendliness. In [26], authors present a solution by developing the SRM framework, defined as

$$\Phi = \sqrt{N/M} \mathbf{D} \mathbf{F} \mathbf{R}, \quad (9)$$

where $\mathbf{R} \in \mathbb{R}^{N \times N}$ is either a uniform random permutation matrix or a diagonal random matrix whose diagonal entries \mathbf{R}_{ii} are Bernoulli random variables with identical distribution $P(\mathbf{R}_{ii} = \pm 1) = 1/2$. A uniformly random permutation matrix shuffles the signal's sample locations whereas the diagonal Bernoulli random variables flip the signal's sample signs. $\mathbf{F} \in \mathbb{R}^{N \times N}$ denotes an orthonormal matrix which is selected among popular fast computable transforms like DCT and WHT. $\mathbf{D} \in \mathbb{R}^{N \times N}$ represents a subsampling operator which selects a random subset of rows in the matrix \mathbf{FR} and the scale coefficient $\sqrt{N/M}$ is to normalize the transform so that the energy of the measurement vector is almost similar to that of the input signal vector.

Quantization is the subsequent essential step of CS for digitizing the measurements. Achievements have been proposed in [14] that, when SRM is adopted to image acquisition, the measurements behave like Gaussian random variables, most of the measurements fall within the range of $[-127.5, 127.5]$. Fig. 1(a) is the standard lena image with size 512×512 , Fig. 1(b) and (c) plot the histogram distributions of the CS measurements when the sample rate (SR) is 0.8. As can be seen, most of the measurements own values within $[-127.5, 127.5]$, which offers the opportunity to quantize the measurements using 8 bits, i.e., within the interval $[0, 255]$. As only fewer measurements are out of $[-127.5, 127.5]$, it is believable that the deviation of the quantization is weak and acceptable [14].

In the proposed scheme, we exploit the intrinsic cryptographic characteristic of SRM, as the uniform random permutation matrix or the diagonal random matrix can be produced in a secret way and then the seed of the production process acts as the secret key. For the quantization process, Lloyd quantizer [29] that is known as an optimal quantizer in the mean square error sense, is introduced for digitizing the measurements to 8 bits. The quantized bit stream is further encrypted in the subsequent permutation-diffusion procedure.

2.3. Permutation and diffusion

In 1998, Fridrich proposed a typical chaos-based image encryption architecture [6], the so-called permutation-diffusion scheme. As the name suggests, this scheme consists of the permutation and diffusion processes, as shown in Fig. 2.

In the permutation stage, image pixels are generally shuffled by a kind of two-dimensional area-preserving chaotic map, without any change of their values. Traditionally, three types of chaotic maps, cat map, baker map and standard map are always employed [9]. Throughout the previous achievements, we can draw the following flaws of traditional permutation techniques. The first one

is the operation efficiency. Generally, 3–5 rounds permutation is required in one overall encryption round to obtain a satisfactory confusion performance, which leads to considerable amount of computation load to the cryptosystems. The second flaw is the periodicity problem. The discretized chaotic maps may become periodic under certain circumstances, which will downgrade the security of the cryptosystem. For example, an image of size 256×256 with any parameters will get back to itself after 192 rounds cat map permutation [9]. The last one is the image size restriction. The cat map, baker map, standard map and most of the permutation achievements are originally designed for scrambling a square image. For non-square plain image, extra pixels have to be padded to firstly form a square image, and that would downgrade the efficiency of the whole cryptosystem.

In the proposed scheme, the input of permutation phase is the CS measurements. As always the cases in practice, the size of CS measurements is usually non-square and cannot be directly scrambled by traditional permutation ciphers. Regarding this, PACT is developed in the present paper. The input and ciphertext of PACT are both viewed as one-dimensional arrays, denoting the pixels as $P = P(1), P(2), \dots, P(MN)$ and $C = C(1), C(2), \dots, C(MN)$ from the upper-left corner to the lower-right corner, respectively. The key procedures of PACT are described as follows:

Step 1: Taking the anterior MN random variables of y series of the 3-D cat map, denoted as $Y = (y_{1,1}, y_{1,2}, \dots, y_{1,MN})$.

Step 2: Sorting the chaotic sequence in ascending order, if there exists $y_{1,i} = y_{1,j}$, ($i > j$), it is regarded as $y_{1,i} > y_{1,j}$, without loss of generality. A new set $Y_2 = \text{sort}(Y) = (y_{2,1}, y_{2,2}, \dots, y_{2,MN})$ is consequently obtained.

Step 3: Obtain the confusion vector, denoted as $R = (r_1, r_2, \dots, r_{MN})$, and r_m ($1 \leq m \leq MN$) is based on the deduction from Eq. (10).

$$y_{1,r_m} = y_{2,m}. \quad (10)$$

Step 4: Rearrange all of the input pixels according to the confusion vector R , that is $C(m) = P(r_m)$.

The decryption process is similar to that of the encryption, identical confusion vector has to be firstly produced with correct parameters, and the plain image can be recovered according to $P(r_m) = C(m)$. The permutation effect of PACT is shown in Fig. 3, where the plaintext is 515×512 lena image shown in Fig. 3(a), and its 1 round shuffled image is demonstrated in Fig. 3(b), the recovered image is plotted in Fig. 3(c). As illustrated, the shuffled image after 1 round PACT permutation is completely unrecognizable and

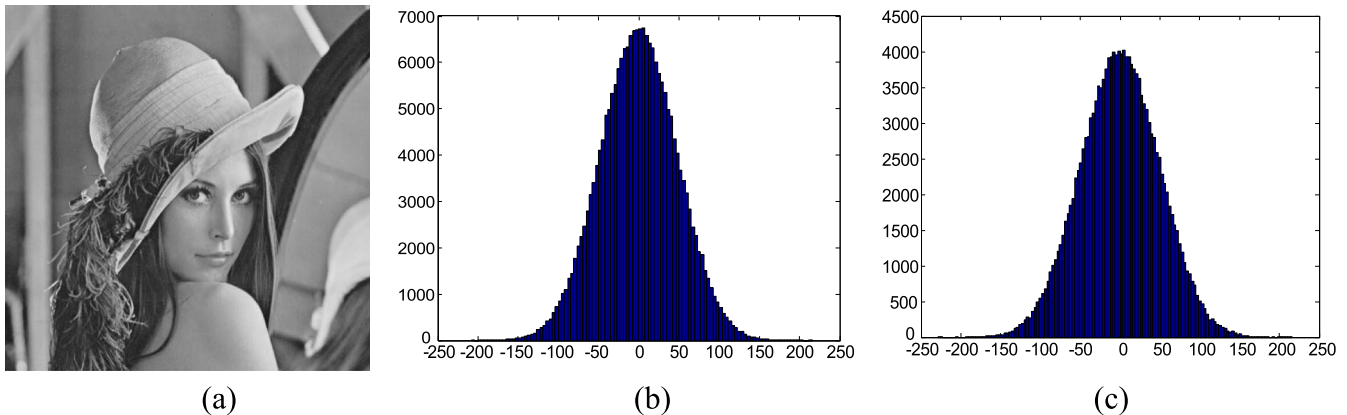


Fig. 1. Distribution histograms of the CS measurements when SR = 0.8: (a) Plaintext lena; histogram of the CS measurements when \mathbf{R} is a (b) uniform random permutation matrix; (c) diagonal Bernoulli random matrix.

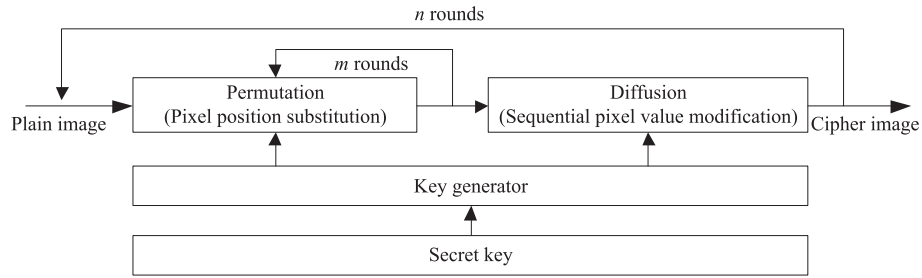


Fig. 2. Architecture of permutation-diffusion image cipher.

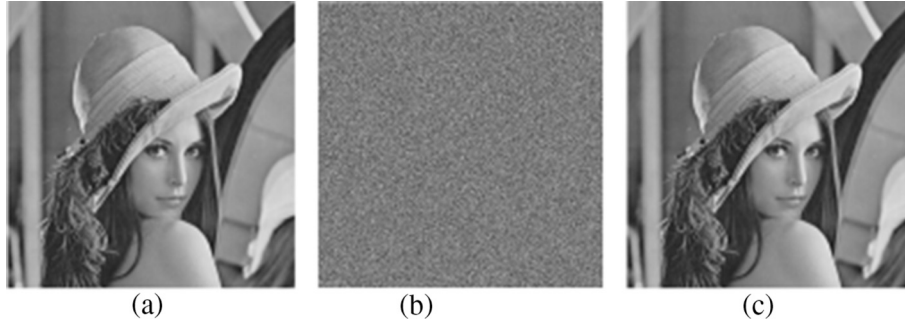


Fig. 3. The permutation effect of PACT: (a) lena image; (b) 1 round shuffled image; (c) the recovered image.

does not leak any useful information of the plaintext, which reveals that the plaintext has been successfully encrypted. Unlike multiple rounds of traditional permutation approaches, only 1 round is sufficient to scramble the plaintext when using PACT, the operation efficiency of PACT is therefore well demonstrated.

It is well known that the permutation module only shuffles the pixel coordinates without any modification of their values, and permutation-only ciphers have been proved to be vulnerable against various attacks [30,31]. To enhance the security of the cryptosystem, we introduce a diffusion procedure to collaborate with PACT and build a complete cryptosystem. The primary task of the diffusion procedure is to encrypt the pixel values, using the diffusion masks generated from the chaotic variables. In the proposed scheme, the diffusion mask $k(n)$ is produced from the z series of 3-D cat map according to Eq. (11), in which $z(n)$ is the current chaotic state variable and L is the gray-level of the plain image.

$$k(n) = \text{mod}[\text{floor}(z(n) \times 10^{15}), L]. \quad (11)$$

The pixel values are modified sequentially to according to

$$c(n) = k(n) \oplus p(n) \oplus c(n-1), \quad (12)$$

where $p(n)$, $k(n)$, $c(n)$, $c(n-1)$ are the current operated plain pixel, key stream element, output cipher-pixel, the previous cipher-pixel, respectively. To start up the diffusion process, a constant seed should be set for encrypting the first pixel.

3. The complete cryptosystem

The schematic of the proposed system is illustrated in Fig. 4. As can be seen, the proposed system consists of two primary procedures, with the first one is the CS using SRM, and the latter is the permutation-diffusion image cipher. All of the key stream elements are generated from a 3-D cat map, whose initial values serve as the secret key.

The operation procedures can be described as follows under the assumption that the plaintext is with size $M \times A$, the SR of CS is B/A , i.e., there are $M \times B$ measurements.

Step 1: Iterate the 3-D cat map with initial value (x_0, y_0, z_0) $M \times A$ times, three series of random state variables x, y, z are simultaneously produced, with all of the values distributed within $(0, 1)$.

Step 2: Choose proper orthonormal matrix and produce the diagonal random Bernoulli matrix of SRM, according to Eq. (13). The SRM is subsequently built, referring to Eq. (9).

$$R_{ii} = \begin{cases} 1 & \text{if } (x_i \geq 0.5) \\ 1 & \text{if } (x_i < 0.5) \end{cases} \quad 1 \leq i \leq M \times A. \quad (13)$$

Step 3: Stretch the plaintext into a vector with length $M \times A$, from the upper-left corner to the bottom-right point, and then obtain the CS measurements according to Eq. (7).

Step 4: Quantize the measurement data y to 8 bits through Lloyd quantizer.

Step 5: Scramble the quantized measurements using PACT, as described in Section 2.3.

Step 6: Mask the resultant data according to Eqs. (11) and (12).

Step 7: Repeat steps 5 and 6 to satisfy the security requirement.

4. Simulations and security analyses

In this section, simulation results and security analyses of the proposed scheme are given out for validation. Eight 256 gray-scale images with size of 512×512 pixels are introduced as plaintexts, with four of them are prevalent standard test images and the others are medical images, as shown in the first column of Fig. 5, i.e., the plaintexts are boats, couple, lena, peppers, X_Lungs, MR_Knee, MR_Prostate and CT_Abdomen. The orthonormal transform of SRM is DCT, the reconstruction algorithm for CS is the gradient projection for sparse reconstruction algorithm [32], and the sparsifying basis is 9–7 Daubechies wavelet transform domain. The compression ratio is

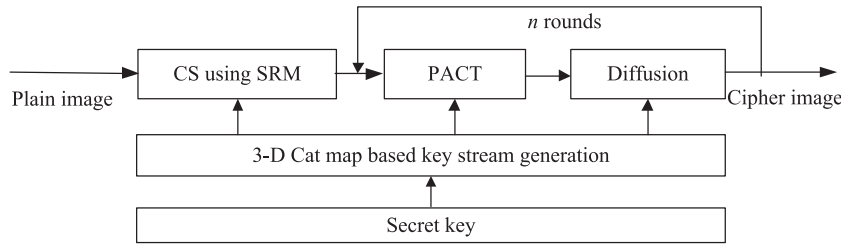


Fig. 4. The schematic of the proposed system.

0.5 for demonstration, which means $M = 512$, $A = 512$, $B = 256$. The algorithm is simulated in Matlab R2010a platform, and the secret key is randomly selected as $x_0 = 0.206429210808374$, $y_0 = 0.790662094577746$ and $z_0 = 0.401893863575571$ for 3-D cat map, the permutation-diffusion encryption is carried out 1 round.

4.1. Encryption and compression results

The results are demonstrated in Fig. 5, where the plain images and ciphertexts are shown in the first and third column respectively. It is obvious that the ciphertexts are all unrecognizable and cannot leak any visual perception of the corresponding plaintexts, and their volumes have been compressed half. We further verify the randomness of the ciphertexts from statistical perspective. The histograms of the corresponding plaintexts are plotted in the second column; meanwhile those of the ciphertexts are illustrated in the fourth column for comparison. As can be seen, the histograms of the ciphertexts are uniformly distributed, which indicate that the redundancy of the plain image has been successfully hidden and consequently does not provide any clue to launch statistical attacks. The encryption and compression performances have been well proved. The reconstructed images are plotted in the fifth column of Fig. 5, from which one can observe that the recovered images are of meaningful visual perception and there is no significant quality degradation in comparison with the plaintexts. We further compute the Peak Signal Noise Ratio (PSNR) as a numerical objective metric to evaluate the reconstruction quality. Under the case that SR is 0.5, the recovered images are with PSNRs of 33.5276 dB, 31.7482 dB, 33.8462 dB, 32.6173 dB, 39.0494 dB, 40.5567 dB, 38.3744 dB, 40.2114 dB, respectively. All of the PSNRs exceed 30 dB, which implies the acceptable reconstruction quality of the proposed scheme. Empirically, medical images always possess better reconstruction quality than natural images, as they have better sparsity (more zero pixels). Such superiority indicates the great potential of simultaneous encryption and compression of medical images, so as to meet the special requirements in the battlefield scene, etc., where the bandwidth resource is rare and precious. From 0.1 to 0.9, PSNRs under different compression ratios are plotted in Fig. 6, from which one can see that the PSNR can exceed 20 dB in the case that SR is greater than 0.1, and it can reach 30 dB when SR exceeds 0.4. In practical applications, there is a large scale for the compromise between compression ratio and recovery quality.

4.2. Key space analysis

The key space size is the total number of different keys that can be used in a cryptosystem. As suggested in [4], key space should be larger than 2^{100} to enhance the resistance against brute-force attack. In the proposed scheme, the secret key consists of the initial values of 3-D cat map, all of the three initial values are valid in $(-1, 1)$. According to the IEEE floating-point standard [33], the

computational precision of the 64-bit double-precision number is about 10^{-15} . The total key space of the proposed scheme is therefore

$$\text{Key} = 10^{15} \times 10^{15} \times 10^{15} = 10^{45} \approx 2^{149},$$

which satisfies the security requirement suggested in [4] and is large enough to resist brute-force attack.

4.3. Pixel correlation analysis

The correlation between adjacent pixels is always high for a meaningful image as their pixel values are usually close to each other. An effective image cryptosystem should produce an encrypted image with sufficiently low correlation between adjacent pixels. The following steps are performed to evaluate an image's correlation property. (1) 3000 pixels are randomly selected as samples; (2) the correlations between two adjacent pixels in horizontal, vertical and diagonal directions are calculated according to Eqs. (14)–(16), where x_i and y_i are gray-level values of the i th pair of the selected adjacent pixels, and N represents the sample counts.

$$r_{xy} = \frac{E(x - E(x))E(y - E(y))}{\sqrt{D(x)}\sqrt{D(y)}}, \quad (14)$$

$$E(x) = \frac{1}{N} \sum_{i=1}^N x_i, \quad (15)$$

$$D(x) = \frac{1}{N} \sum_{i=1}^N (x_i - E(x))^2. \quad (16)$$

Pixel correlation performances in each encryption stage have been analyzed. In other words, the pixel correlation coefficients of the compressed image after CS, resultant image after permutation and the ciphertext with complete encryption are comprehensively evaluated, as listed in Table 1, with the lowest coefficient shown in bold. The adjacent pixel dots are plotted in Fig. 7, where the first to fourth row severally represents the results of the plaintext, compressed image after CS, resultant image after permutation and the ciphertext with complete encryption, and the first to fourth column shows the image, correlation plots in horizontal, vertical and diagonal directions, respectively. One can observe that, the high adjacent pixel correlation in the plaintext has been dramatically reduced after the CS procedure, that is because CS essentially measures the plaintext with a random pattern. As mentioned above, the measurements of CS using SRM behave like Gaussian random variables, and the adjacent pixel dots are plotted in the second row of Fig. 7, where the pixels are relatively centred around the middle of the plots. The compressed image is subsequently permuted using PACT, and the adjacent pixel correlation coefficients are further decreased. However, as permutation merely shuffles the pixel positions without any modification of the pixel values, and hence the pixel dots are also relatively close

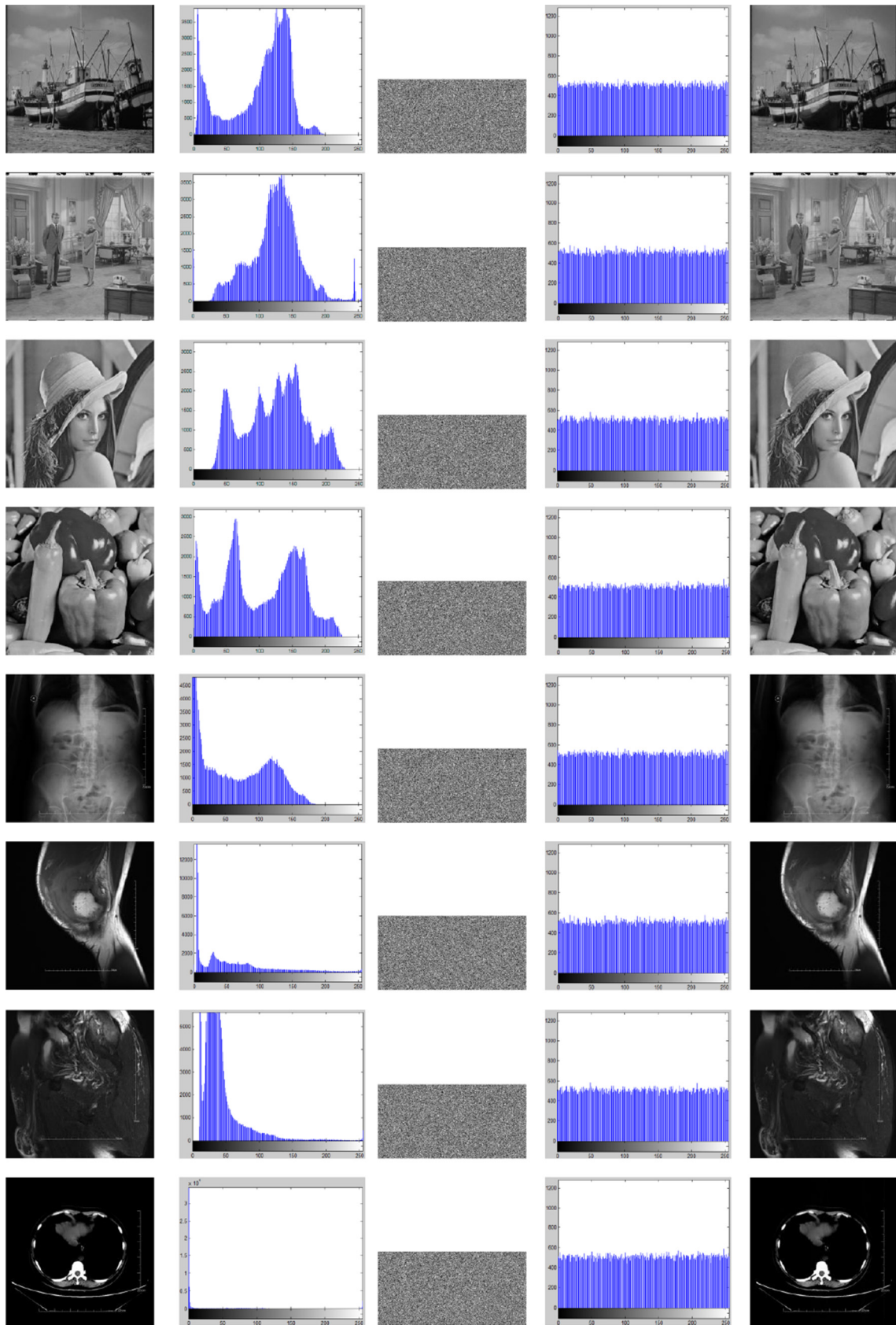


Fig. 5. Simulation results of the proposed scheme: from the first to the fifth column are plaintexts, histogram of the plaintexts, ciphertexts, histogram of the ciphertexts and the recovered images, respectively.

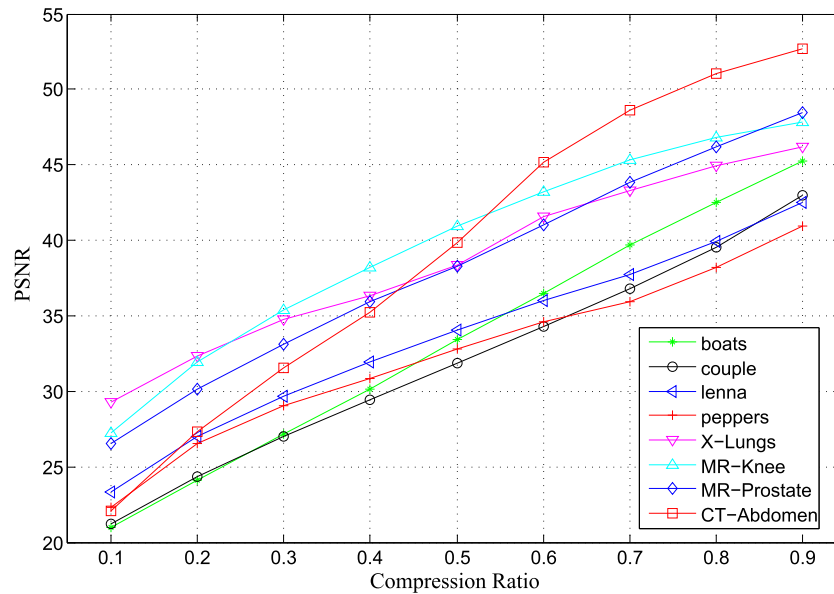


Fig. 6. PSNRs versus different compression ratios.

Table 1
Correlation coefficients of adjacent pixels.

Direction	Plain image	Compressed image	Image after permutation	Ciphertext with complete encryption
Horizontal	0.9849	0.0563	0.0202	0.0018
Vertical	0.9693	0.0210	0.0115	0.0014
Diagonal	0.9562	0.0219	0.0150	0.0034

to each other, as demonstrated in the third row of Fig. 7. The values of CS measurements will be masked in the diffusion procedure, and the produced pixels will be uniformly distributed. In the fourth row, it is obvious that the pixel dots have been scattered over the entire plane, which reveals the most satisfactory pixel correlation performance of the ciphertext, as listed in Table 1. Synthesizing the numerical results of Table 1 and the pixel plots in Fig. 7, one can draw the conclusion that the strong correlation among neighboring pixels of a plain image has been effectively de-correlated by the proposed cryptosystem, and therefore the ciphertext is more robust against statistical attack.

4.4. Key sensitivity analysis

Extreme key sensitivity is a critical feature of an effective cryptosystem, and can be observed in two aspects: (i) completely different ciphertexts should be produced when slightly different keys are applied to encrypt the same plain image; (ii) the cipher image cannot be correctly recovered even tiny difference exists between the encryption and decryption keys.

To evaluate the key sensitivity in the first case, the encryption is implemented 1 round at first to obtain a cipher image. Then a slight change 10^{-15} is introduced to one of the parameters with all others unchanged, and repeats the encryption. The corresponding cipher images and the differential images are shown in Fig. 8. The differences between the cipher images are computed and listed in Table 2. The results obviously illustrate that the ciphertexts exhibit no similarity one another and there is no significant relationship that could be deduced from the differential images.

In addition, decryption with slightly incorrect keys has also been implemented so as to evaluate the key sensitivity in the

decryption phase. All of the deciphering images are noise-like, as shown in Fig. 9. The differences between the incorrect deciphering images to the plain image are 99.6212%, 99.6212%, 99.6151%, respectively.

4.5. Information entropy

Entropy is a mathematical property that demonstrates the randomness and the unpredictability of an information source, it is first found in 1949 by Shannon [34]. The entropy $H(s)$ of a message source s is defined in Eq. (17), where s is the source, N is the number of bits to represent the symbol s_i , and $P(s_i)$ is the probability of the symbol s_i . For a truly random source consists of 2^N symbols, the entropy is N , and hence for the 256 gray image used in our experiments, the entropy should ideally be 8.

$$H(s) = - \sum_{i=0}^{2^N-1} P(s_i) \log_2 P(s_i). \quad (17)$$

The employed test images are encrypted and the information entropies are then calculated, as listed in Table 3. One can see that, the entropies of the cipher images are very close to the theoretical value of 8, which means that information leakage in the encryption procedure is negligible and the proposed algorithm is secure against entropy analysis.

Numerically, the entropies listed in Table 3 seem relatively low in comparison with other encryption-only algorithms (such as [16]). Yet, it should be emphasized that, the entropy difference essentially originates from the diverse sizes of the ciphertexts. According to the achievements proposed in [35], entropies of the ciphertexts own large volumes are always higher than those whose

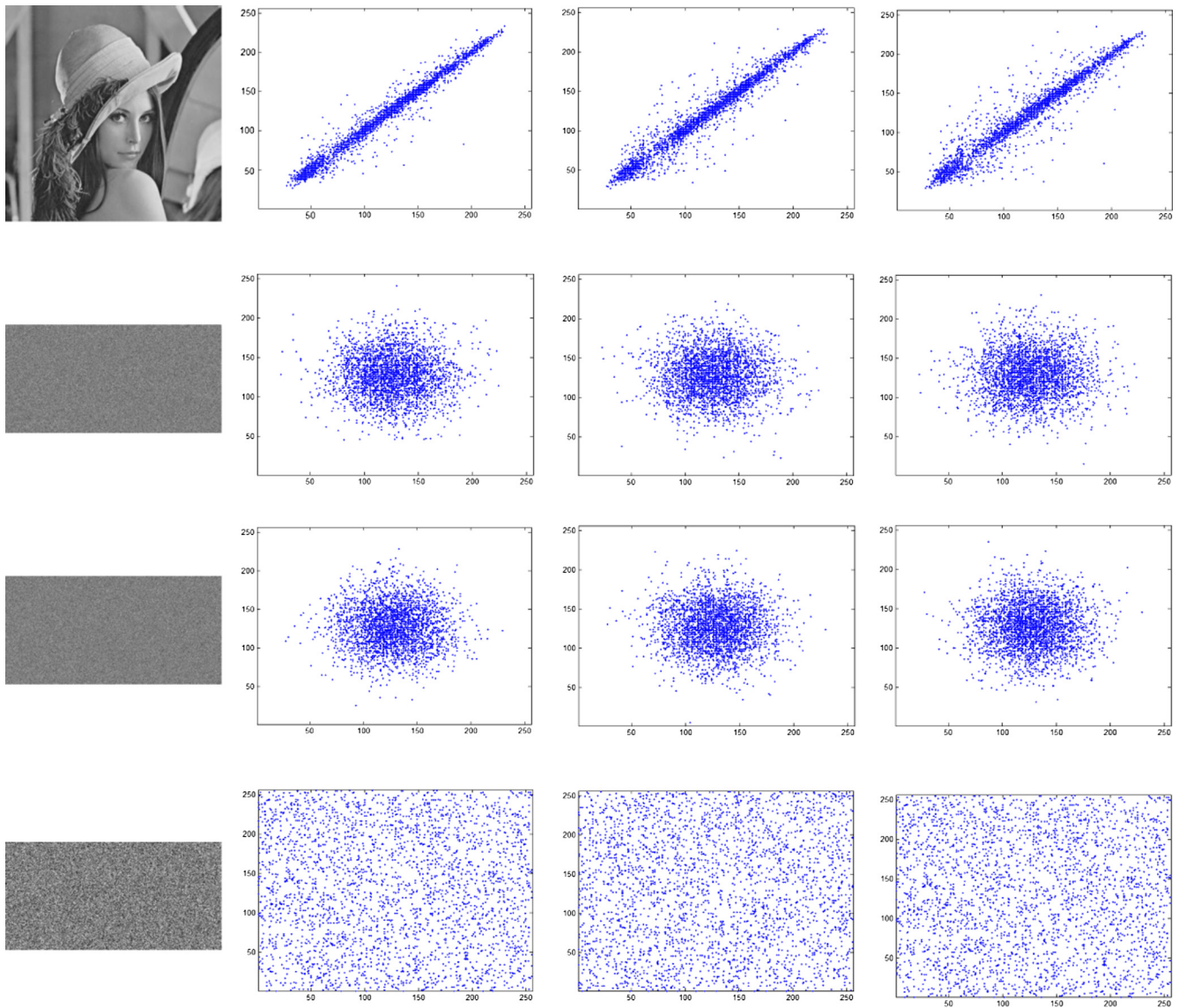


Fig. 7. Pixel correlation analysis: the first to fourth row is the plaintext, compressed image after CS, resultant image after permutation and the ciphertext with complete encryption; the first to fourth column shows the image, correlation plots in horizontal, vertical and diagonal directions, respectively.

sizes are relatively smaller, even though they are encrypted with the same cipher. Considering that the proposed cryptosystem can simultaneously encrypt and compress the plaintexts, the sizes of the produced ciphertexts are consequently smaller than those produced by encryption-only algorithms (such as [16]), and hence the entropies are relatively lower from numerical perspective. Compared with peer algorithms which are also encryption and compression systems using CS and chaotic map, our scheme owns advantageous, as described in Section 4.7. Synthesizing the other analyses proposed above, the security performance of the proposed cipher has been comprehensively evaluated.

4.6. Complexity analysis

The proposed cryptosystem consists of a CS projection module, and a permutation-diffusion type encryption procedure. Regarding the CS process of our scheme, SRM is employed as the measurement matrix instead of the widely-adopted random measurement matrix, such as Gaussian or Bernoulli matrices. In [26,36], researchers have investigated the computation complexity when

using SRM for signal sampling and reconstruction, as listed in Table 4. Assuming that there are N pixels in the plain image, the measuring complexity and reconstruction complexity of SRM are both $O(N \log N)$, which is more satisfactory than random measurement matrices in not only the measuring stage but also signal reconstruction process.

As pointed out in [37,38], the time-consumption of chaos-based image cryptosystem mainly derives from the workloads of chaotic map iteration and quantization in the encryption process. Consequently, the required chaotic variables and quantization counts for encrypting one pixel can be employed to evaluate the efficiency of permutation-diffusion type ciphers [39]. Referring to the encryption process in Section 3, one can conclude that it requires 1 chaotic variable for permutation and diffusion respectively, and 1 quantization for the generation of diffusion mask. Therefore, the complexity of the permutation-diffusion encryption of our scheme is $O(3N)$. It should be noted that, if the permutation-diffusion encryption is implemented multiple rounds, the permutation vector and diffusion mask in the subsequent encryption rounds are not required to regenerate. In other words, the required

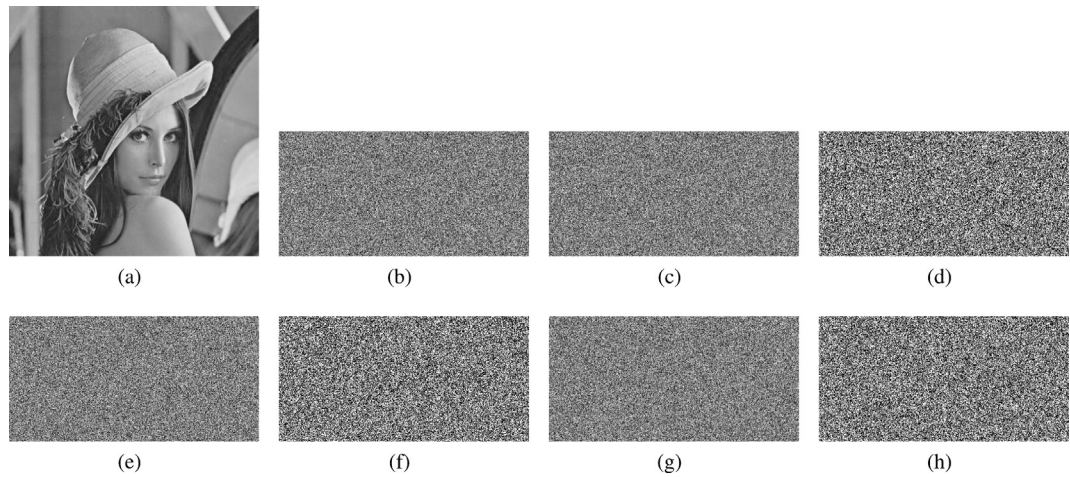


Fig. 8. Key sensitivity test in the first case: (a) plain image; (b) cipher image ($x_0 = 0.206429210808374$, $y_0 = 0.790662094577746$, $z_0 = 0.401893863575571$); (c) cipher image ($x_0 = 0.206429210808375$, $y_0 = 0.790662094577746$, $z_0 = 0.401893863575571$); (d) differential image between (b) and (c); (e) cipher image ($x_0 = 0.206429210808374$, $y_0 = 0.790662094577747$, $z_0 = 0.401893863575571$); (f) differential image between (b) and (e); (g) cipher image ($x_0 = 0.206429210808374$, $y_0 = 0.790662094577746$, $z_0 = 0.401893863575572$); (h) differential image between (b) and (g).

Table 2
Differences between cipher images produced by slightly different keys.

Figures	Encryption keys			Differences ratio between 8(b)
	x_0	y_0	z_0	
8(b)	0.206429210808374	0.790662094577746	0.401893863575571	–
8(c)	0.206429210808375	0.790662094577746	0.401893863575571	99.6185%
8(e)	0.206429210808374	0.790662094577747	0.401893863575571	99.5842%
8(g)	0.206429210808374	0.790662094577746	0.401893863575572	99.5842%

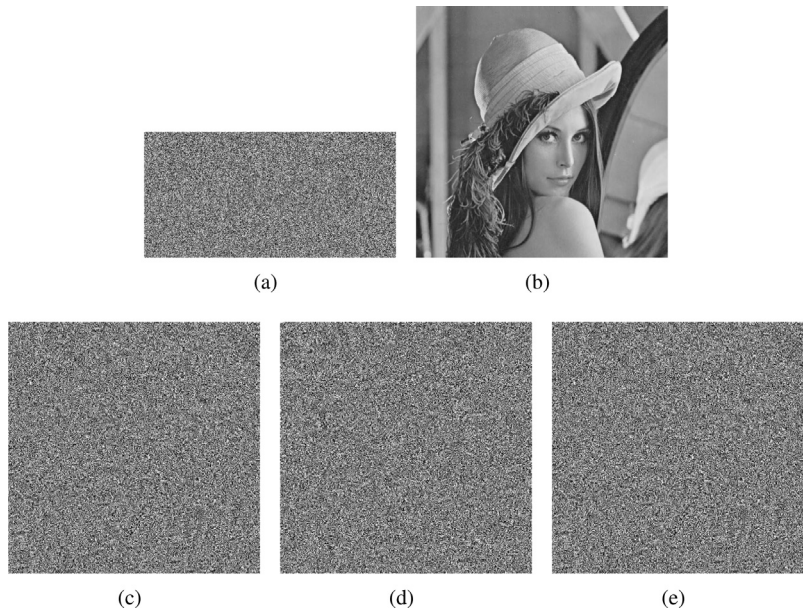


Fig. 9. Key sensitivity test in the second case: (a) cipher image ($x_0 = 0.206429210808374$, $y_0 = 0.790662094577746$, $z_0 = 0.401893863575571$); (b) decipher image with correct key; (c) decipher image with ($x_0 = 0.206429210808375$, $y_0 = 0.790662094577746$, $z_0 = 0.401893863575571$); (d) decipher image with ($x_0 = 0.206429210808374$, $y_0 = 0.790662094577747$, $z_0 = 0.401893863575571$); (e) decipher image with ($x_0 = 0.206429210808374$, $y_0 = 0.790662094577746$, $z_0 = 0.401893863575572$).

chaotic variables and quantization remain unchanged, though the permutation-diffusion encryption procedure may be performed many times. In this scenario, the increased workloads are merely the pixel swapping operation of permutation as well as the XOR arithmetic of the diffusion equation, which are very lower-cost than the chaotic iteration and quantization [38].

4.7. Performance comparison

In this subsection, the proposed cryptosystem is compared with some peer encryption-compression schemes [8–10,15]. Following fair comparisons principle adopted in [40], the performance record is directly cited from the source reports, and corresponding sys-

Table 3

Entropies of plain images and cipher images.

	Plain image	Cipher image
Boats	7.072868435	7.998380351
Couple	7.201008279	7.998584589
Lena	7.445567570	7.998613079
Peppers	7.571477564	7.998750708
X_Lungs	6.966385303	7.998412805
MR_Knee	5.384936963	7.998576529
MR_Prostate	6.241682696	7.998398284
CT_Abdomen	1.675035010	7.998320699

Table 4

Complexity comparison of various measurement matrix of CS.

Items	SRM	Random matrix
Required measurements	$O(K\log N)$	$O(K\log N)$
Measuring complexity	$O(N\log N)$	$O(KN\log N)$
Reconstruction complexity	$O(N\log N)$	$O(KN\log N)$
Hardware implementation	Easy	Difficult
Fast computability	Yes	No

tems will not be presented if there is no performance data in the original publication. The plaintext lena with size 512×512 is introduced as the sample, the default sample rate is set as 0.5. The comparison is carried out in terms of image reconstruction performance PSNR, pixel correlation coefficient, and the information entropy.

Table 5 lists the image reconstruction performance of the comparable schemes when $SR = 0.5$. The approximate PSNRs of the cryptosystems in [8–10] are deduced from the results presented in corresponding reports, as they didn't give exact value in this encryption scenario. As can be observed, when SR is 0.5, the PSNRs of the reconstructed images in [8,9] are less than 26 dB, and it is relatively more satisfactory as 32.5 dB in [10]. Under the same encryption-compression scenario, the PSNR of the recovered image in our scheme is 33.5276 dB, which indicates the highest reconstruction quality of the proposed scheme.

The comparison result of adjacent pixel correlation performance is listed in Table 6. As demonstrated in Fig. 7 and Tables 1 and 6, the adjacent pixels of the plaintext in horizontal, vertical and diagonal directions are tightly correlated and the correlation coefficients are all greater than 0.95. On the contrary, correlation coefficients of the ciphertexts are almost smaller than 0.02. In other words, all of the comparable cryptosystems can produce ciphertext with satisfactory adjacent pixel correlation, yet the proposed scheme owns superiority in horizontal and vertical directions.

Information entropy comparison is also conducted, and the result is listed in Table 7. As can be observed, information entropies of the encrypted images produced by the proposed method are very close to the ideal value 8, and is more satisfactory than peer algorithms in [9,10]. That is to say, the proposed cryptosystem can achieve better randomness, and hence is more robust against various attacks.

Table 5

Comparison of image reconstruction performance.

Algorithm	PSNR (dB)
Ref. [8]	<25.9997
Ref. [9]	<26
Ref. [10]	≈ 32.5
Proposed	33.5276

Table 6

Comparison of adjacent pixel correlation.

Algorithm	Horizontal	Vertical	Diagonal
Plaintext	0.9849	0.9693	0.9562
Ref. [8]	0.0042	−0.0043	0.0163
Ref. [9]	0.0036	0.0012	0.0005
Ref. [10]	0.0037	0.0018	0.0011
Ref. [15]	0.0029	0.0064	−0.0072
Proposed	0.0018	0.0014	0.0034

Table 7

Comparison of image reconstruction performance.

Algorithm	Entropy
Ref. [9]	7.995980
Ref. [10]	7.9219
Proposed	7.99861

4.8. Ciphertext and plaintext attacks

In cryptanalysis, plaintext and ciphertext attacks are always launched for evaluating the security of an encryption system. Particularity, ciphertext-only attack assumes that a set of ciphertexts are accessible to the opponents, a known-plaintext attack presumes that an adversary is able to obtain a set of plaintexts and their ciphertexts. Furthermore, a chosen-plaintext attack assumes that an adversary can get arbitrary plaintexts to be encrypted and access their corresponding ciphertexts [40]. As can be observed, chosen-plaintext attack provides the opponents most information about plaintexts and ciphertexts among three attack models, and hence if a cipher has satisfactory resistance against chosen-plaintext attack, it is also believed to be immune to ciphertext-only and known-plaintext attacks. Regarding the proposed scheme, the resistance against chosen-plaintext attack can be observed from the following aspects.

- The measurement matrix, permutation vector and diffusion masks are essentially equivalent key components of the proposed cryptosystem. If independently adopted for encrypting plaintexts, they are vulnerable against plaintext attack. For example, the CS based ciphers are vulnerable to chosen-plaintext attack, specially, the measurement matrix can be extracted by an identity input. Yet, when they are combined together as a cascaded system in our scheme, they will provide mutual protection to each other, and consequently the system is more secure.
- The well-known chosen-plaintext attack of CS based ciphers, i.e., extracting the measurement matrix using an identity matrix, will become infeasible in the proposed system. As can be observed from the encryption process, the CS output of an identity matrix is equal to the measurement matrix. Whereas, this output is not obtainable by the adversary, as it is intermediate variable produced in the encryption process. It will be unpreventable encrypted by the subsequent permutation-diffusion procedure, and hence the extraction of the measurement matrix can be avoided.
- Plaintext attack algorithms in [30,31] that are proposed for recovering the encryption matrix of a permutation-only cipher will lose efficacy either. In the proposed scheme, the first encryption procedure is CS, whose measurement matrix is generated by a chaotic serial. Originating from the unpredictable property of chaotic system, the measurement matrix is also unknown and unpredictable. Therefore, the adversary cannot

construct a plaintext whose CS measurements (also the inputs of the permutation phase) are known, the permutation procedure is consequently more secure.

- As can be deduced from Eq. (12), if the input and output of the diffusion procedure are all known to the adversary, the diffusion mask can be extracted. Yet, similar to the previous case, originating from the unpredictability of CS outputs and encryption effect of the permutation procedure, the input for diffusion (also the ciphertext after permutation) is also unknown and uncontrollable, and hence the diffusion mask is unobtainable even though its output (the final ciphertext) is known.

Consequently, the proposed cryptosystem also owns satisfactory resistance against ciphertext-only and known-plaintext attacks.

5. Conclusions

This paper reports a cryptosystem for simultaneous image encryption and compression, with the compression performance is achieved by CS while the security contribution originates from both the CS and permutation-diffusion procedures. The 3-D cat map is introduced for generating the measurement matrix of CS, as well as the permutation vector and diffusion masks of the subsequent encryption process. Security analyses have been carried out, and the image reconstruction, key space, histogram, key sensitivity and information entropy performances are comprehensively evaluated. The satisfactory compression and encryption performances renders the proposed scheme a suitable solution for secure image transmission and compression over public networks.

Conflicts of interest

The authors declare no conflict of interest.

Acknowledgements

This work was supported by the National Natural Science Foundation of China (Nos. 61773110 and 61374015), and the Fundamental Research Funds for the Central Universities (Nos. N161904002, N150402004 and N140404015).

References

- [1] S. Li, G. Chen, X. Zheng, Chaos-based encryption for digital image and video, *Multimedia Encrypt. Authentic. Tech. Appl.* (2006) 129.
- [2] Y.-Q. Zhang, X.-Y. Wang, A symmetric image encryption algorithm based on mixed linear–nonlinear coupled map lattice, *Inform. Sci.* 273 (2014) 329–351.
- [3] 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.
- [4] G. Alvarez, S. Li, Some basic cryptographic requirements for chaos-based cryptosystems, *Int. J. Bifurc. Chaos* 16 (08) (2006) 2129–2151.
- [5] Z. Hua, Y. Zhou, One-dimensional nonlinear model for producing chaos, *IEEE Trans. Circ. Syst. I: Regular Papers* (99) (2017) 1–12.
- [6] J. Fridrich, Symmetric ciphers based on two-dimensional chaotic maps, *Int. J. Bifurc. Chaos* 8 (06) (1998) 1259–1284.
- [7] Z. Tang, J. Song, X. Zhang, R. Sun, Multiple-image encryption with bit-plane decomposition and chaotic maps, *Opt. Lasers Eng.* 80 (2016) 1–11.
- [8] 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.
- [9] 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 (2017) 116–127.
- [10] T. Chen, M. Zhang, J. Wu, C. Yuen, Y. Tong, Image encryption and compression based on Kronecker compressed sensing and elementary cellular automata scrambling, *Opt. Laser Technol.* 84 (2016) 118–133.
- [11] X. Chai, Z. Gan, Y. Chen, Y. Zhang, A visually secure image encryption scheme based on compressive sensing, *Signal Process.* 134 (2017) 35–51.
- [12] J.-X. Chen, Z.-L. Zhu, C. Fu, L.-B. Zhang, Y. Zhang, Cryptanalysis and improvement of an optical image encryption scheme using a chaotic Baker map and double random phase encoding, *J. Opt.* 16 (12) (2014) 125403.
- [13] N. Zhou, A. Zhang, F. Zheng, L. Gong, Novel image compression-encryption hybrid algorithm based on key-controlled measurement matrix in compressive sensing, *Opt. Laser Technol.* 62 (2014) 152–160.
- [14] Z. Hua, Y. Zhou, Design of image cipher using block-based scrambling and image filtering, *Inform. Sci.* 396 (2017) 97–113.
- [15] J. Chen, Z.-L. Zhu, L.-B. Zhang, Z. Yushu, B.-Q. Yang, Exploiting self-adaptive permutation-diffusion and dna random encoding for secure and efficient image encryption, *Signal Process.* 142 (2018) 340–353.
- [16] D. Ravichandran, P. Praveenkumar, J.B.B. Rayappan, R. Amirtharajan, Chaos based crossover and mutation for securing DICOM image, *Comput. Biol. Med.* 72 (2016) 170–184.
- [17] H. Singh, A. Yadav, S. Vashisth, K. Singh, Fully phase image encryption using double random-structured phase masks in gyrator domain, *Appl. Opt.* 53 (28) (2014) 6472–6481.
- [18] A. Yadav, S. Vashisth, H. Singh, K. Singh, A phase-image watermarking scheme in gyrator domain using devil's vortex Fresnel lens as a phase mask, *Opt. Commun.* 344 (2015) 172–180.
- [19] E.J. Candès, J. Romberg, T. Tao, Robust uncertainty principles: exact signal reconstruction from highly incomplete frequency information, *IEEE Trans. Inform. Theory* 52 (2) (2006) 489–509.
- [20] D.L. Donoho, Compressed sensing, *IEEE Trans. Inform. Theory* 52 (4) (2006) 1289–1306.
- [21] E.J. Candès, T. Tao, Near-optimal signal recovery from random projections: universal encoding strategies?, *IEEE Trans. Inform. Theory* 52 (12) (2006) 5406–5425.
- [22] Y. Rachlin, D. Baron, The secrecy of compressed sensing measurements, in: 2008 46th Annual Allerton Conference on Communication, Control, and Computing, IEEE, 2008, pp. 813–817.
- [23] L.Y. Zhang, K.-W. Wong, Y. Zhang, J. Zhou, Bi-level protected compressive sampling, *IEEE Trans. Multimedia* 18 (9) (2016) 1720–1732.
- [24] Y. Zhang, D. Xiao, H. Liu, H. Nan, GLS coding based security solution to JPEG with the structure of aggregated compression and encryption, *Commun. Nonlinear Sci. Numer. Simul.* 19 (5) (2014) 1366–1374.
- [25] G. Chen, Y. Mao, C.K. Chui, A symmetric image encryption scheme based on 3D chaotic cat maps, *Chaos Solit. Fract.* 21 (3) (2004) 749–761.
- [26] T.T. Do, L. Gan, N.H. Nguyen, T.D. Tran, Fast and efficient compressive sensing using structurally random matrices, *IEEE Trans. Signal Process.* 60 (1) (2012) 139–154.
- [27] C. Fu, J.-B. Huang, N.-N. Wang, Q.-B. Hou, W.-M. Lei, A symmetric chaos-based image cipher with an improved bit-level permutation strategy, *Entropy* 16 (2) (2014) 770–788.
- [28] J.A. Tropp, A.C. Gilbert, Signal recovery from random measurements via orthogonal matching pursuit, *IEEE Trans. Inform. Theory* 53 (12) (2007) 4655–4666.
- [29] S. Lloyd, Least squares quantization in PCM, *IEEE Trans. Inform. Theory* 28 (2) (1982) 129–137.
- [30] S. Li, C. Li, G. Chen, N.G. Bourbakis, K.-T. Lo, A general quantitative cryptanalysis of permutation-only multimedia ciphers against plaintext attacks, *Signal Process.: Image Commun.* 23 (3) (2008) 212–223.
- [31] C. Li, K.-T. Lo, Optimal quantitative cryptanalysis of permutation-only multimedia ciphers against plaintext attacks, *Signal Process.* 91 (4) (2011) 949–954.
- [32] M.A. Figueiredo, R.D. Nowak, S.J. Wright, Gradient projection for sparse reconstruction: application to compressed sensing and other inverse problems, *IEEE J. Sel. Top. Signal Process.* 1 (4) (2007) 586–597.
- [33] A.N.S. Institute, IEEE Standard for Binary Floating Point Arithmetic: Approved March 21, 1985; Approved July 26, 1985, IEEE, 1985.
- [34] C.E. Shannon, Communication theory of secrecy systems, *Bell Labs Tech. J.* 28 (4) (1949) 656–715.
- [35] Y. Wu, Y. Zhou, G. Saveriades, S. Agaian, J.P. Noonan, P. Natarajan, Local Shannon entropy measure with statistical tests for image randomness, *Inform. Sci.* 222 (2013) 323–342.
- [36] D. Xiao, L. Wang, T. Xiang, Y. Wang, Multi-focus image fusion and robust encryption algorithm based on compressive sensing, *Opt. Laser Technol.* 91 (2017) 212–225.
- [37] G. Chen, Y. Mao, C.K. Chui, A symmetric image encryption scheme based on 3D chaotic cat maps, *Chaos Solit. Fract.* 21 (3) (2004) 749–761.
- [38] K.-W. Wong, B.S.-H. Kwok, C.-H. Yuen, An efficient diffusion approach for chaos-based image encryption, *Chaos Solit. Fract.* 41 (5) (2009) 2652–2663.
- [39] J.-X. Chen, Z.-L. Zhu, C. Fu, H. Yu, Y. Zhang, Reusing the permutation matrix dynamically for efficient image cryptographic algorithm, *Signal Process.* 111 (2015) 294–307.
- [40] Y. Wu, Y. Zhou, J.P. Noonan, S. Agaian, Design of image cipher using latin squares, *Inform. Sci.* 264 (2014) 317–339.