Optics & Laser Technology 82 (2016) 121–133

Contents lists available at ScienceDirect

Optics & Laser Technology

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

Full length article

Image compression–encryption scheme based on hyper-chaotic system and 2D compressive sensing

Nanrun Zhou [a,b,*], Shumin Pan [a], Shan Cheng [c], Zhihong Zhou [b]

[a] Department of Electronic Information Engineering, Nanchang University, Nanchang 330031, China
[b] Shanghai Key Laboratory of Integrate Administration Technologies for Information Security, Shanghai Jiao Tong University, Shanghai 200240, China
[c] Department of Electrical Engineering, Jiangxi Vocational College of Mechanical & Electrical Technology, Nanchang 330013, China

ARTICLE INFO

Article history:
Received 23 November 2015
Received in revised form
24 January 2016
Accepted 25 February 2016

Keywords:
Image compression–encryption
Compressive sensing
Hyper-chaotic system

ABSTRACT

Most image encryption algorithms based on low-dimensional chaos systems bear security risks and suffer encryption data expansion when adopting nonlinear transformation directly. To overcome these weaknesses and reduce the possible transmission burden, an efficient image compression–encryption scheme based on hyper-chaotic system and 2D compressive sensing is proposed. The original image is measured by the measurement matrices in two directions to achieve compression and encryption simultaneously, and then the resulting image is re-encrypted by the cycle shift operation controlled by a hyper-chaotic system. Cycle shift operation can change the values of the pixels efficiently. The proposed cryptosystem decreases the volume of data to be transmitted and simplifies the keys distribution simultaneously as a nonlinear encryption system. Simulation results verify the validity and the reliability of the proposed algorithm with acceptable compression and security performance.

1. Introduction

In recent years, chaos has been developed from low-dimensional into high-dimensional cases, and the performance of chaos is continually fashioned or improved. A variety of image encryption techniques based on chaos with good performance have been reported [1–10]. Chen et al. generalized the Arnold transformation into the 3D case to design a symmetric image encryption scheme [1]. Gao employed an image total shuffling matrix to shuffle the positions of image pixels and then used a hyper-chaotic system to confuse the relationship between the plain-image and the cipher-image [2]. Subsequently, Gao et al. proposed a new image authentication scheme based on cell neural network with hyper-chaos characteristics [3]. A novel image encryption–compression scheme using hyper-chaos and Chinese remainder theorem was designed [4], where the 2D hyper-chaos discrete nonlinear dynamic system was used to shuffle the plain image and then the Chinese remainder theorem was applied to diffuse and compress the shuffled image simultaneously. To solve the problem that chaos is degenerated in a limited computer precision and the key space of cat map is not large enough, an image encryption scheme based on a multiple chaotic map was constructed [5]. Chen et al. demonstrated an optical image encryption scheme using 3D chaotic map based on joint image scrambling and random encoding in the gyrator domain [8]. Ye presented an image scrambling encryption algorithm of pixel bit based on chaos map [9], which took advantage of the best features of chaos maps, such as their pseudorandom property, system parameters, sensitiveness dependent on initial conditions and nonperiodicity. Subsequently, Ye et al. proposed a chaotic image encryption algorithm based on a generalized Arnold map [10]. However, chaos cracking techniques also have been developed, and the chaos-based encryption algorithms are still under cracking [11–14]. Therefore, the hyper-chaotic systems were introduced to enhance the security of the image encryption algorithms [15–24]. According to Chen's chaos theory, Jia et al. put forward a four-dimensional hyper-chaotic system by adding a dimension into Chen's hyper-chaotic system [15]. Zhu improved the image encryption scheme based on hyper-chaotic sequence by encrypting different plain-text with different keys, which increases the length of the keys [22]. After that, another image encryption algorithm, which could resist chosen-plaintext attack, was devised based on an improved hyper-chaotic system by Ozkaynak [24]. To improve the security of image encryption further, the hyper-chaotic systems were naturally combined with other encryption algorithms [25–30]. Zhang et al. proposed a double-image encryption scheme based on discrete Chirikov standard map and chaos-based fractional random transform [26], where the discrete version of Chirikov standard map was employed to scramble the pixels of two images to improve the

* Corresponding author at: Department of Electronic Information Engineering, Nanchang University, Nanchang 330031, China.
E-mail addresses: nrzhou@ncu.edu.cn, znr21@163.com (N. Zhou).

http://dx.doi.org/10.1016/j.optlastec.2016.02.018
0030-3992/

security of the algorithm. A double-image encryption scheme [27] was proposed based on logistic map and discrete fractional random transform by Sui et al., where a chaotic confusion–diffusion process was used to disorder the plaintext images, which strengthens the nonlinearity in spatial domain and DFrRT domain. Khan provided an image encryption algorithm based on chaos and S-boxes [29], where the validity and the security were confirmed. To resist the chosen-plaintext attack, a parallel image encryption algorithm with DNA encoding was presented, where the bitwise exclusive OR operation was performed on the pixels of the plain image with the pseudorandom sequences produced by the spatiotemporal chaos system [30].

Most of the encryption algorithms mentioned above did not consider image compression or data compression, thus they cannot realize compression and encryption simultaneously. To solve this problem, compressive sensing [31,32] (CS) is utilized to construct new encryption systems. Orsdemir et al. proposed a cryptosystem [33] based on the selection of random measurement matrix, which keeps the robustness of the CS system to noise. Huang et al. designed a digital image compression–encryption method [34], which is robust against consecutive packet loss and malicious shear attack. A color image encryption scheme [35] was devised by combining CS with Arnold transform, where the compressed measurements were scrambled by Arnold transform. Random sensing matrix was usually used in CS-based encryption algorithms, Endra et al. improved the quality of the reconstructed image compared with random sensing matrix by using the optimized sensing matrix and introduced a new image compression–encryption algorithm [36]. Subsequently, an image encryption algorithm was improved by utilizing Arnold transform to scramble the pixels [37]. Most of the mentioned CS-based encryption algorithms treated the whole measurement matrix as the key, thereby rendering the key too large to distribute and store. To control the measure matrix with a shorter key, a novel image compression–encryption hybrid algorithm [38] was devised, where the measurement matrix was controlled by keys in two directions to achieve compression and encryption simultaneously. After that, Zhou et al. proposed a new hybrid image compression–encryption algorithm based on compressive sensing [39], which is very sensitive to the keys and could resist the chosen-plaintext attack as the measurement matrix was scrambled by a chaos sequence. An image compression–encryption algorithm [40] combining 2D CS with nonlinear fractional Mellin transform (FrMT) was provided, which naturally maintained the nonlinearity of FrMT to resist common attacks and the compression ability of compressive sensing. George et al. presented an image encryption approach [41] based on CS technique and linear feedback shift register, which was validated through different block-based CS techniques of images and provided better performance than its counterparts. Subsequently, a new system [42] for scrambling the CS audio data using two dimensional cellular automata was presented. After that, several optical encryption systems combining CS and optical encryption techniques were proposed. A new optical image compression–encryption algorithm [43] based on CS and chaos was introduced in the fractional Fourier domain, which could be implemented with a simple optoelectronic set-up to improve the encryption speed. An image encryption method [44] combining two-step-only quadrature phase-shifting digital holography with CS was devised in the fully optical domain.

An efficient image compression–encryption algorithm combining 2D CS with hyper-chaotic system is presented in this paper, which enhances the security by the improved Chen's chaos system and achieves fast encryption through 2D CS. To decrease the data volume of the encrypted image, the original image is measured by the measurement matrices, and then the pseudorandom matrix generated by the hyper-chaotic system performs cyclic shift operation with the compressed image. Generally, hyper-chaotic systems are used to generate chaotic sequences for image scrambling based on its randomness characteristic. The measurements are performed in two directions and the measurement matrices controlled by chaos index sequences with initial conditions are constructed as the partial Hadamard matrices. Therefore, the cyclic shift operation controlled by the hyper-chaotic system, which provides good security of this encryption algorithm due to its nonlinearity.

The rest of this paper is arranged as follows: In Section 2, the hyper-chaotic system and 2D CS are reviewed. The detailed description of this scheme is provided in Section 3. In Section 4, simulations and discussions are given. Finally, a brief conclusion is drawn in Section 5.

2. Fundamental knowledge

2.1. Hyper-chaotic system

The original definition of Chen's hyper-chaotic system is:

$$\begin{cases} \dot{x} = a(y - x) \\ \dot{y} = dx - xz + cy - h \\ \dot{z} = xy - bz \\ \dot{h} = x + k \end{cases} \tag{1}$$

where a, b, c, d, and k are the control parameters of the hyper-chaotic system. The system is in a hyperchaotic state if $a=36$, $b=3$, $c=28$, $d=-16$ and $-0.7 < k < 0.7$. If k is set as 0.2, the Lyapunov exponents of the hyper-chaotic system are 1.552, 0.023, 0 and -12.573, respectively. Since the hyper-chaotic system has two positive Lyapunov exponents, the prediction time of the hyper-chaotic system is shorter than the original chaotic system, and the encryption algorithm based on this hyper-chaotic system would have higher security than those based on the chaotic system. The equations are taken to obtain four chaotic sequences by the fourth order Runge–Kutta method. Considering this advantage of the hyper-chaotic system, we will use it to generate the keys in the diffusion stage of our image compression–encryption algorithm.

2.2. Compressive sensing

Interestingly, in CS theory, signal sampling and compressing could be achieved simultaneously. Generally, a one dimensional signal x in R^N with length N could be represented as:

$$x = \sum_{j=1}^{N} \alpha_j \Psi_j = \Psi\alpha \text{ or } \alpha = \Psi^{\mathrm{T}} x \tag{2}$$

where Ψ is an $N \times N$ matrix and $\alpha = [\alpha_1, \alpha_2, \ldots, \alpha_N]$ is the coefficient sequence of the one dimensional signal x. If there are only $K (K \ll N)$ coefficients nonzero in the coefficient vector α, the signal is compressible and sparse. Then, a condensed representation between x and a collection of test functions $\{\Phi_j\}_{j=1}^{M}$ could be directly acquired in $y_j = \left\langle x, \Phi_j^{\mathrm{T}} \right\rangle$ by an $M (M < N)$ dimension linear measurement. The compressed signal could be obtained by stacking y_j into an $M \times 1$ vector and an $M \times N$ matrix Φ could be constructed by gathering the rows Φ_j, i.e.,

$$y = \Phi x = \Phi\Psi\alpha = \Theta\alpha \tag{3}$$

where Φ is necessarily incoherent with the basis matrix Ψ. The sensor matrix $\Theta = \Phi\Psi$ should satisfy the restricted isometry property (RIP) [31]. To reconstruct x from y, the following optimal problem should be resolved inevitably.

$$\alpha = \text{argmin}\ \|\alpha\|_0 \text{ s. t. } y = \Phi x \tag{4}$$

where $\|\alpha\|_0$ means the number of nonzero components in α. Signal x could be rebuilt if $M \geq cK \log(N)$, where c is an arbitrarily small constant. Similarly, a 2D signal X with size $N \times N$ is transformed in the Ψ domain and measured with Φ_1. The 2D compressed–encrypted result Y is obtained by another measurement matrix Φ_2. Y is an $M \times M$ matrix, and $\beta = \Psi^T X^T \Psi$. Similarly, to reconstruct X from Y, the following optimal problem is supposed to be solved.

$$\beta = \arg\min \|\beta\|_0 \text{ s. t. } Y = \Phi_2 \beta \Phi_1^T \tag{5}$$

Smoothed l_0 Norm SL_0 [45] is effective to retrieve the original signal X from the encrypted result Y, which is usually chosen as one of the common reconstruction algorithms in CS theory. Subsequently, the hyperbolic tangent function is used to approximate the norm in the NSL_0 algorithm [46] and the modified Newton detection is used as a search party to reconstruct or rebuild the matrix. The hyperbolic tangent function is defined as:

$$f_\sigma(x_j) = \frac{e^{\frac{x_j^2}{2\sigma^2}} - e^{\frac{x_j^2}{-2\sigma^2}}}{e^{\frac{x_j^2}{2\sigma^2}} + e^{\frac{x_j^2}{-2\sigma^2}}} \tag{6}$$

It can be obtained from Eq. (6) that: $\lim_{\sigma\to 0} f_\sigma(x_j) = \begin{cases} 0, & x_j = 0 \\ 1, & x_j \neq 0 \end{cases}$, where x_j is the vector of the X. Similarly, $F_\sigma(X) = \sum_{j=1}^{N} f_\sigma(x_j)$, and the norm L_0 is :

$$\|X\|_0 = \lim_{\sigma\to 0} F_\sigma(X) \tag{7}$$

The two reconstruction algorithms were compared in [46], and the simulation results of the simulations show that the NSL_0 algorithm could improve the convergence speed and the signal-to-noise ratio apparently comparing with the SL_0 algorithm under the same experimental conditions.

3. Image compression–encryption combining hyper-chaos system with 2D compressive sensing

The proposed image compression–encryption scheme is illustrated in Fig. 1 and the encryption process is described as follows:

Step 1: The original image X is extended in the Ψ domain and then performed the projection measurement in Ψ_1 to obtain $\beta_1 = \Phi_1 \Psi^T x$, where Ψ_1 is the $M \times N$ measurement matrix and Ψ is the $N \times N$ orthogonal basis.

Step 2: Then β_1 is extended in the Ψ domain to obtain $\beta_2 = \Psi^T X^T \Psi \Phi_1^T$, where measurement result $\beta = \Psi^T X^T \Psi$, and $\beta = \Psi^T X^T \Psi$ is the transform in the 2D Ψ domain.

Step 3: The partial Hadamard matrices are exploited to construct the measurement matrices Φ_1 and Φ_2, which are respectively controlled by two different logistic maps. Take the construction of the measurement matrix Φ_1 for example, the steps are as follows:

(1) A sequence $\lambda = [\lambda_1, \lambda_2, \ldots, \lambda_{2N}]$ with length $2N$ is generated by logistic map with initial condition x_{01}. To obtain the index sequence $s = [s_1, s_2, \ldots, s_N]$, the preceding N elements of λ are abandoned.

(2) The nature sequence $n = [1, 2, \ldots, N]$ is sorted with the index sequence s and the sorted sequence is noted as $l = [l_1, l_2, \ldots, l_i, \ldots, l_N]$, where $l_i \in \{1, 2, \ldots, N\}$.

(3) The M row vectors $H(l_1, :), H(l_2, :), \ldots, H(l_i, :), \ldots, H(l_M, :)$ of the Hadamard matrix H of order N are used to group into the following measurement matrix Φ_1.

$$\Phi_1 = \left[H(l_1, :)\ H(l_2, :)\ \ldots\ H(l_i, :)\ \ldots\ H(l_M, :) \right]^T \tag{8}$$

where $H(l_i, :)$ denotes the l_i-th row vector of H.

With another initial condition x_{02}, the measurement matrix Φ_2 could be constructed in a same way.

Step 4: By considering $Y = \Phi_2 \beta \Phi_1^T$, the intermediate encryption result Y could be obtained by measuring β.

Step 5: Confirm the values of the initial conditions x_0, y_0, z_0, h_0, and iterate Chen's chaos system by the Runge–Kutta method to avoid the harmful effect of transient procedure. Four hyper-chaotic sequences $\{x_i\}$, $\{y_i\}$, $\{z_i\}$ and $\{h_i\}$ can be generated with a suitable step length in the Runge–Kutta method, respectively.

Step 6: Transform the four hyper-chaotic sequences $\{x_i\}$, $\{y_i\}$, $\{z_i\}$ and $\{h_i\}$ into integer sequences $\{t_i^*\}$, t can be replaced by x, y, z and h.

$$t_i^* = \left\| \left(t_i - \lfloor t_i \rfloor \right) \times 10^{14} \right\| \bmod 224 \tag{9}$$

where $\lfloor x \rfloor$ rounds x to the nearest integer towards zero.

Step 7: Construct a hyper-chaotic sequence $K = \{k_1, k_2, \ldots, k_{2^{2n}}\}$. If the result of h_i^* mod 3 equals to 0, 1, or 2, then one takes k_i as x_i^*, y_i^* or z_i^* correspondingly to perform the cycle shift operation. The integer k_i can be represented as a binary number $k_i = h_i^7 h_i^6 \ldots h_i^0$, $h_i^j \in \{0, 1\}$, $i = 1, 2, \ldots, 2^{2n}$, $j = 0, 1, \ldots, 7$.

Step 8: The pseudorandom sequence generated by the hyper-chaotic system is transformed as:

$$R_2 = \left\{ R_2 \middle| R_{2i} = \text{round}\left[\text{mod}\left(10000 y_i, 8 \right) \right] \right\},\ i = 1, 2, \ldots \tag{10}$$

Step 9: All pixels of Y are mapped into an integer range from 0 to 255.

$$C = \text{round}\left[255 \times \frac{Y}{\max Y} \right] \tag{11}$$

And then each pixel in C is decomposed into an 8 bits binary number.

$$a^t(i, j) = \begin{cases} 1, & a(i, j)/2^t \bmod 2 = 1; \\ 0, & \text{others.} \end{cases} \tag{12}$$

In Eq. (12), $a^t(i, j)$ is the t-th number after the conversion, $t = 0, 1, \ldots, 7$. The results are arranged in a row in turn, and the size of the transformed matrix $D_{8\times M^2}$ is $8M^2$.

Step 10: Disturb the pixel values of the matrix with the cycle shift operation and the pseudorandom sequence R_2:

$$C' = T\left(D_{8\times M^2}, R_2 \right) \tag{13}$$

Step 11: Deduce an $M \times M$ binary matrix from C' and obtain the encrypted image G.

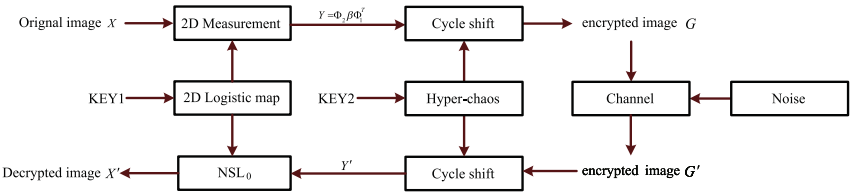


Fig. 1. Image compression–encryption based on hyper-chaos and 2D CS.

$$a(i,j) = \sum_{t=0}^{7} 2^t \times a^t(i,j) \tag{14}$$

$$G = \frac{C'}{255} \times \max Y \tag{15}$$

In the decryption process, the encrypted image is first performed by the inverse cycle shift operation, and then is retrieved with the NSL_0 algorithm.

4. Experimental results and analyses

A series of numerical simulations are carried out on a 64-bit computer with Matlab 2012(a) to demonstrate the performance of the proposed image compression–encryption scheme.

4.1. Encrypted image and decrypted image

The gray image "Lena", "Peppers" and "Lake" with 256×256 pixels, shown in Fig. 2(a), (d) and (g), serve as the test images of

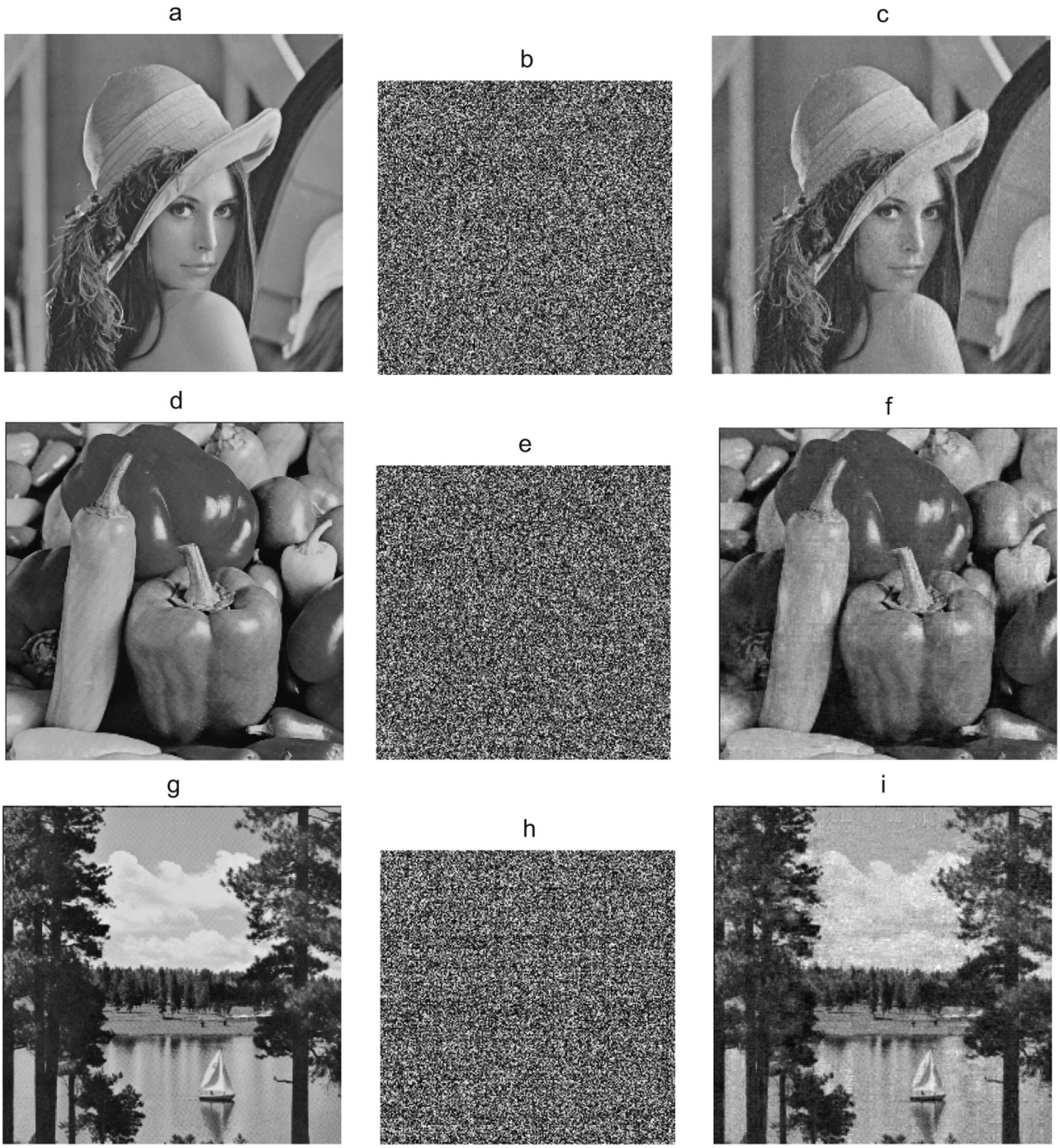


Fig. 2. Results of test images: (a) "Lena", (b) encrypted "Lena", (c) decrypted "Lena", (d) "Peppers", (e) encrypted "Peppers", (f) decrypted "Peppers", (g) "Lake", (h) encrypted "Lake", and (i) decrypted "Lake".

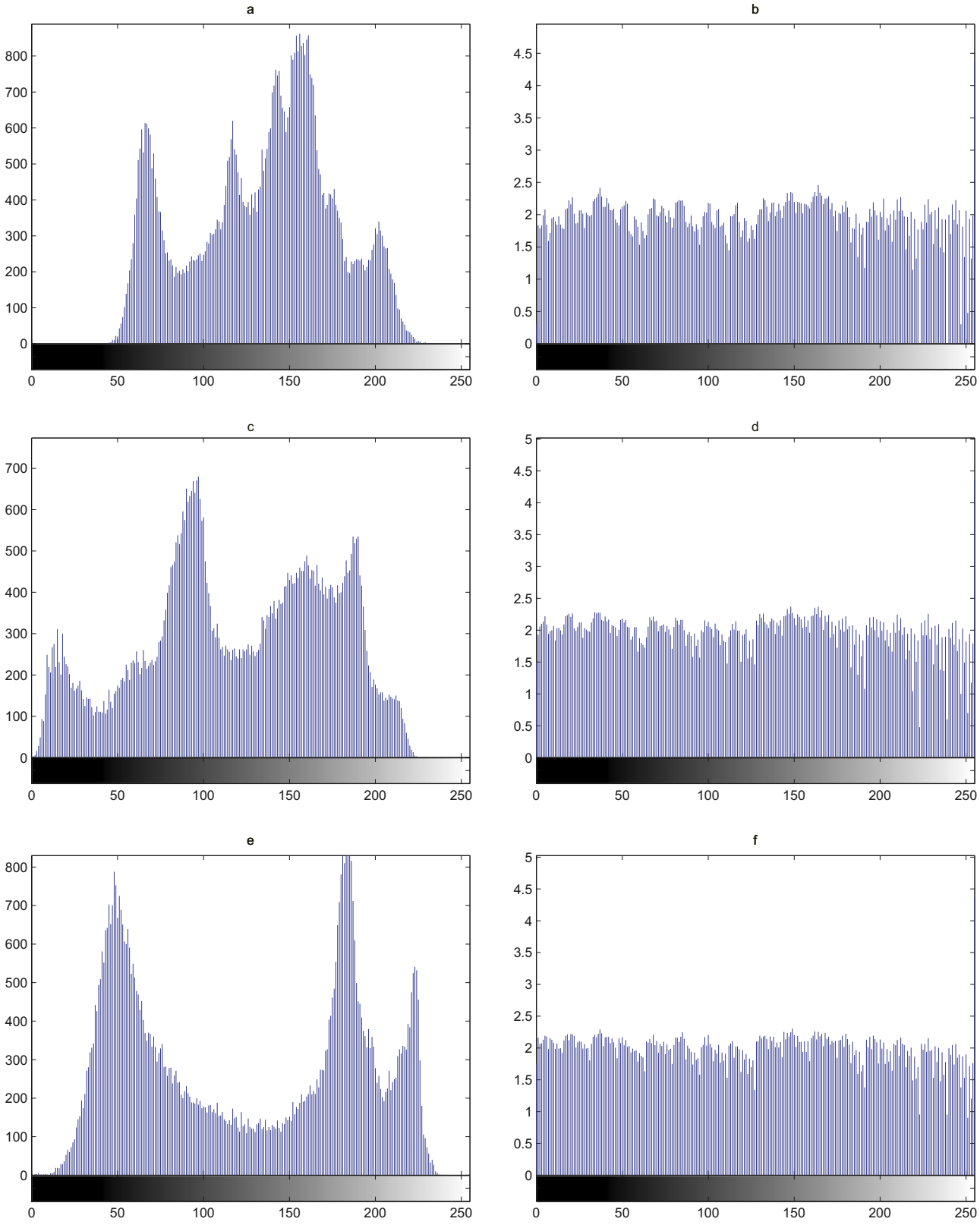


Fig. 3. Histograms: (a) "Lena", (b) encrypted "Lena" (c) "Peppers", (d) encrypted "Peppers", (e) "Lake", (f) encrypted "Lake".

the image compression–encryption algorithm based on hyper-chaos and 2D compressive sensing. The parameters in 2D CS are taken as: $x_{01} = 0.13$, $x_{02} = 0.25$, $\mu = 3.99$. The size of the ciphered image is 224×224. The four initial values of the hyper-chaotic system are set as: $x_0 = 0.3$, $y_0 = 0.4$, $z_0 = 0.5$ and $h_0 = 0.6$. The encrypted "Lena", "Peppers" and "Lake" are shown in Fig. 2(b), (e) and (h). The decrypted images with the correct keys are shown in Fig. 2(c), (f) and (i).

4.2. Histograms

Fig. 3(a), (c), and (e) are the histograms of "Lena", "Peppers" and "Lake", respectively, while Fig. 3(b), (d), and (f) show the histograms of their corresponding encrypted images, respectively. The histograms of the encrypted images are similar and almost equally distributed although the histograms of the original images are apparently different from each other. Generally speaking, a secure and effective image encryption algorithm should make the encrypted images corresponding to different original images have similar histograms. Therefore, the proposed algorithm can frustrate the basic statistical analysis attack due to the similar histograms of different encrypted images.

4.3. Correlation of adjacent pixels

It is better for a good image encryption algorithm that the correlation coefficient of the encrypted image should be much weaker than that of the original image. The correlation coefficient between adjacent pixels of an image can be obtained as:

$$C = \frac{\sum_{i=1}^{N}\left(x_i - \bar{x}\right)\left(y_i - \bar{y}\right)}{\sqrt{\sum_{i=1}^{N}(x_i - \bar{x})^2 \times \sum_{i=1}^{N}(y_i - \bar{y})^2}} \tag{16}$$

where $\bar{x} = \frac{1}{N}\sum_{i=1}^{N} x_i$ and $\bar{y} = \frac{1}{N}\sum_{i=1}^{N} y_i$. The correlation coefficients of the proposed algorithm and the algorithms in [33] and [37] are compiled in Table 1, which shows that the proposed algorithm has better performance than them. The adjacent pixels of the original images in the horizontal, vertical and diagonal directions are tightly correlated and the correlation coefficients are all greater than 0.9 in each direction. Contrary to the cipher images, the correlation coefficients are almost smaller than 0.05. Fig. 4 gives the correlation distribution between two horizontally adjacent pixels in three different original images and the corresponding encrypted images. From Fig. 4, the correlation distributions between adjacent pixels in the original images are similar to a linear-like area in the horizontal direction, and the pixel statistical correlations of the final encrypted images are much weaker as expected. It is indicated that the proposed image compression–encryption algorithm can resist statistical attack with this negligible correlation. And it is impossible for the attackers to restore valuable information from the correlation of adjacent pixels.

4.4. Compression performance

One of the most prominent advantages of the proposed image compression–encryption algorithm is that it could compress and encrypt the image simultaneously. To evaluate the quality of the decrypted digital images versus different compression ratios, the peak-to-peak signal-to-noise ratio (PSNR) [44] is employed.

$$\mathrm{PSNR} = 20\log 255 - 10\log\left(1/N^2\right)\sum_{i=1}^{N}\sum_{j=1}^{N}\left[R(i,j) - I(i,j)\right]^2 \tag{17}$$

where $R(i, j)$ and $I(i, j)$ are the reconstructed image and the original one, respectively. Table 2 lists the PSNR values for different compression ratios. The compression ratio β=25% means that the compressed image is 25% as large as the original image. From Table 2, the quality of the decrypted image remains acceptable to some degree with the different compression ratios, which means the compression ability of the proposed method is great enough and helpful for transmission and storage.

Table 1
Correlation coefficients of adjacent pixels.

Algorithm	Image	Horizontal	Vertical	Diagonal
	Lena	0.9569	0.9236	0.9019
Proposed algorithm	Encrypted Lena	0.0042	−0.0043	0.0163
Ref. [33]	Encrypted Lena	0.0442	0.0382	0.0631
Ref. [37]	Encrypted Lena	−0.0071	−0.0045	0.0229
	Peppers	0.9544	0.9471	0.9200
Proposed algorithm	Encrypted Peppers	−0.0005	−0.0062	0.0036
Ref. [33]	Encrypted Peppers	0.0387	0.0182	0.0473
Ref. [37]	Encrypted Peppers	−0.0080	−0.0005	0.0153
	Lake	0.9377	0.9403	0.9100
Proposed algorithm	Encrypted Lake	0.0231	0.0140	0.0097
Ref. [33]	Encrypted Lake	0.0239	0.0134	0.0448
Ref. [37]	Encrypted Lake	−0.0306	−0.0101	0.0081

4.5. Key sensitivity analysis

The mean square error (MSE) between decrypted image and original image is an important factor to evaluate the key sensitivity of an image encryption algorithm:

$$\mathrm{MSE} = \frac{\sum_{x=1}^{M}\sum_{y=1}^{N}\left[f(x,y) - \bar{f}(x,y)\right]^2}{M \times N} \tag{18}$$

where $f(x, y)$ and $\bar{f}(x, y)$ mean the pixel values at point (x, y) of original image and decrypted image, respectively. $M \times N$ denotes the image size. Fig. 5 shows the MSE curves for x_{01}, x_{02}, x_0, y_0, z_0 and h_0, respectively. The MSE is very large with a little deviation to the correct keys and the MSE is very small only when the main keys are correct. Thus the decrypted image can be recognized if and only if the keys are correct.

The sensitivity can be also rated with the wrong keys deviated only a little from the correct keys. Fig. 6 shows the decrypted "Lena" with the incorrect keys deviated 10^{-16} from x_{01} or x_{02}, 10^{-15} from x_0 or z_0, and -10^{-15} from y_0 or h_0, respectively. The PSNR values are listed in Table 3. It is obvious that the decrypted images are distorted greatly and with low PSNR values. They show no information about the original image visually any more, which means that a little change to the key would cause a direct and great distortion in the decrypted image visually. It is indicated that the presented image compression–encryption algorithm is sensitive to the keys, which ensures a larger key space and makes the attacker difficult to exhaust the correct keys.

4.6. Key space

As is known, the size of key space reflects the difficulty and the complexity in attacking a cryptosystem successfully, thus an effective image compression–encryption scheme should have a large enough key space S to resist the brute-force attack. In the proposed scheme, the parameters x_{01}, x_{02}, x_0, y_0, z_0 and h_0 are regarded as the main keys for their large key subspace. The total key space S can be expressed as

$$S = S_1S_2S_3S_4S_5S_6 \tag{19}$$

where S_i is the key subspace of the i-th key, i = 1, 2, …, 6. To estimate the size of the key space, two different sequences x and $\bar{x}$ are generated with the initial values x_{01} and $x_{01} + \Delta$ (Δ is the deviation of the key), and both sequences are of length N. The mean absolute error (MAE) between two sequences is:

$$\mathrm{MAE}(\mu, \bar{\mu}) = \frac{1}{N}\sum_{i=1}^{N}|\mu_i - \bar{\mu}| \tag{20}$$

The key space of x_{01} is equal to $1/\Delta$, where Δ is the right value subject to $\mathrm{MAE}(\mu, \bar{\mu}) = 0$. The simulation results show that the space of x_{01} or x_{02} is 10^{16}. Similarly, the subspace of x_0, y_0, z_0 and h_0

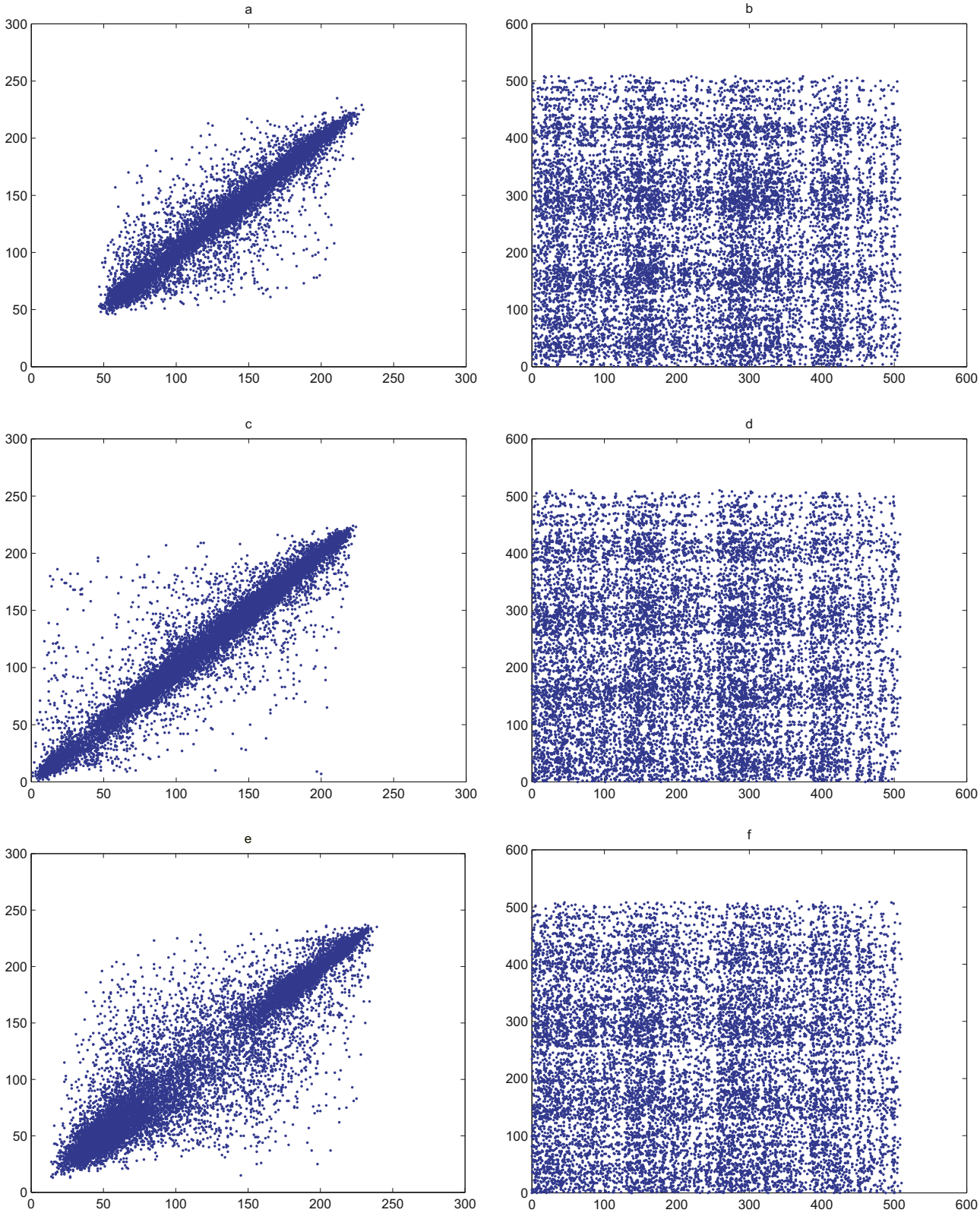
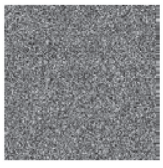
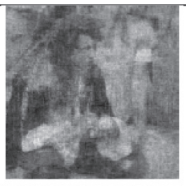


Fig. 4. Correlation distribution of two horizontally adjacent pixels: (a) original "Lena", (b) encrypted "Lena", (c) original "Peppers", (d) encrypted "Peppers", (e) original "Lake"; and (f) encrypted "Lake".

is about 10^{15}. The key subspace S_1 or S_2 is 10^{16} while the key subspace S_3, S_4, S_5 or S_6 is 10^{15}, thus the total key space is as large as 10^{92}, which is greater than 2^{276}. That is to say, the attacker has to calculate more than 2^{276} times if she attempts to construct the correct matrixes by exhausting the keys. Table 4 gives the key space of different schemes. From the results given in Table 4, it is obvious that the proposed image compression–encryption algorithm is secure enough against the brute-force attack due to the

Table 2
PSNR values for different compression ratios.

Original image	Compression ration	Compressed and encrypted image	Decrypted image	PSNR(dB)
	25%			17.4172
	56.25%			25.9997
	76.5625%			30.6881
	25%			15.1139
	56.25%			22.4933
	76.5625%			26.3460

multiple initial parameters of the Chen's hyper-chaotic system.

4.7. Known plaintext attack

Known-plaintext attack is one of the most common attacks for a multimedia cryptosystem. As for a linear measurement process, the correct decrypted image could be reconstructed if the attacker attempts to obtain the measurement matrix by choosing a unit matrix as the input. However, in our proposed image compression–encryption scheme, we assume that Ψ is known and set β as a unit matrix. Therefore, the measurement result $Y = \Phi_2\Phi_1^T$ can be obtained. The measurement matrix Φ_1 is

$$\Phi_k = \left[\delta_{k1}^{\mathrm{T}}, \quad \delta_{k2}^{\mathrm{T}}, \quad \ldots, \quad \delta_{kM}^{\mathrm{T}}\right], k = 1, 2 \tag{21}$$

where δ_{kj} is one of the row vectors of Hadamard matrix of order N. The measurement matrices are constructed as partial Hadamard matrices,

$$Y = \begin{bmatrix} \delta_{21}\delta_{11}^{\mathrm{T}} & \delta_{21}\delta_{12}^{\mathrm{T}} & \cdots & \delta_{21}\delta_{1M}^{\mathrm{T}} \\ \delta_{22}\delta_{11}^{\mathrm{T}} & \delta_{22}\delta_{12}^{\mathrm{T}} & \cdots & \delta_{22}\delta_{1M}^{\mathrm{T}} \\ \vdots & \vdots & \ddots & \vdots \\ \delta_{2M}\delta_{11}^{\mathrm{T}} & \delta_{2M}\delta_{12}^{\mathrm{T}} & \cdots & \delta_{2M}\delta_{1M}^{\mathrm{T}} \end{bmatrix} \tag{22}$$

Since both δ_{1a} and δ_{2a} are one of the row vectors of the Hadamard matrix of order N,

$$\delta_{2k}\delta_{1j}^{\mathrm{T}} = \begin{cases} 0, & \delta_{2k} \neq \delta_{1j}; \\ N, & \delta_{2k} \neq \delta_{1j}. \end{cases} \tag{23}$$

According to Eq. (23), the attacker could not obtain the measurement matrices Φ_1 and Φ_2. Therefore, the proposed system is robust or invulnerable to the known-plaintext attack.

4.8. Noise attack

The images in the transform process are easily affected by different kinds of noises more or less due to the uncoordinated

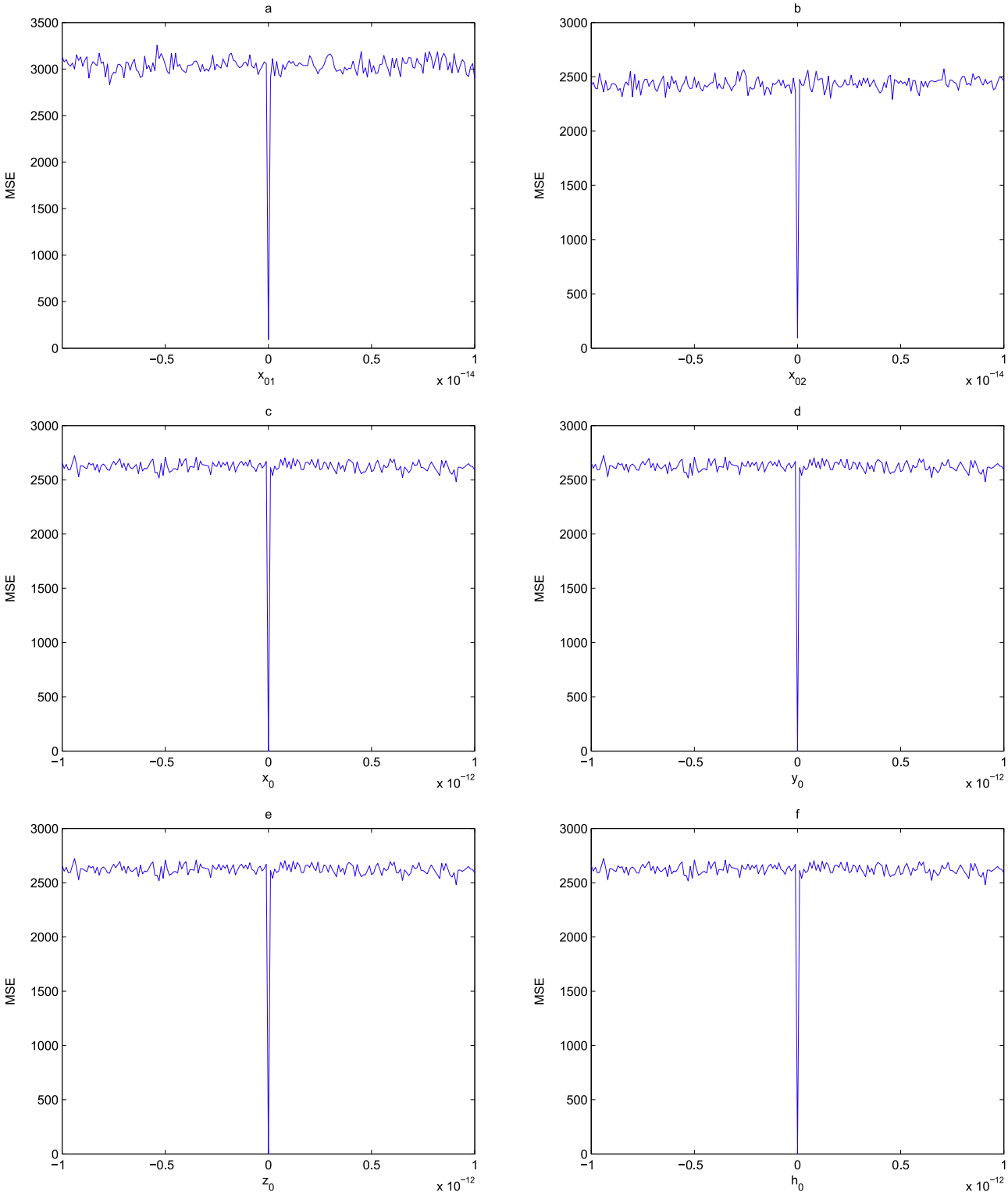


Fig. 5. MSE curves: (a) x_{01}, (b) x_{02}, (c) x_0, (d) y_0, (e) z_0 and (f) h_0.

transmission medium, imperfect recording equipment or something else. To crown it all, the noises would have a significant impact on the quality of the decrypted images, thus the schemes insensitive to noise are necessary to evaluate. Suppose the noise is added into the encrypted image as:

$$G' = G + cW \tag{24}$$

where G and G' are the encrypted and the noisy encrypted images, respectively, c is a coefficient related to the noise strength, and W represents the Gaussian random data with zero-mean and unit standard deviation. The Gaussian noises with different noise intensities are added into the encrypted image, and the deviation of MSE versus noise intensity c is illustrated in Fig. 7(a). The decrypted images when c equals to 1, 5, 10, 15, 20, 15 are shown in

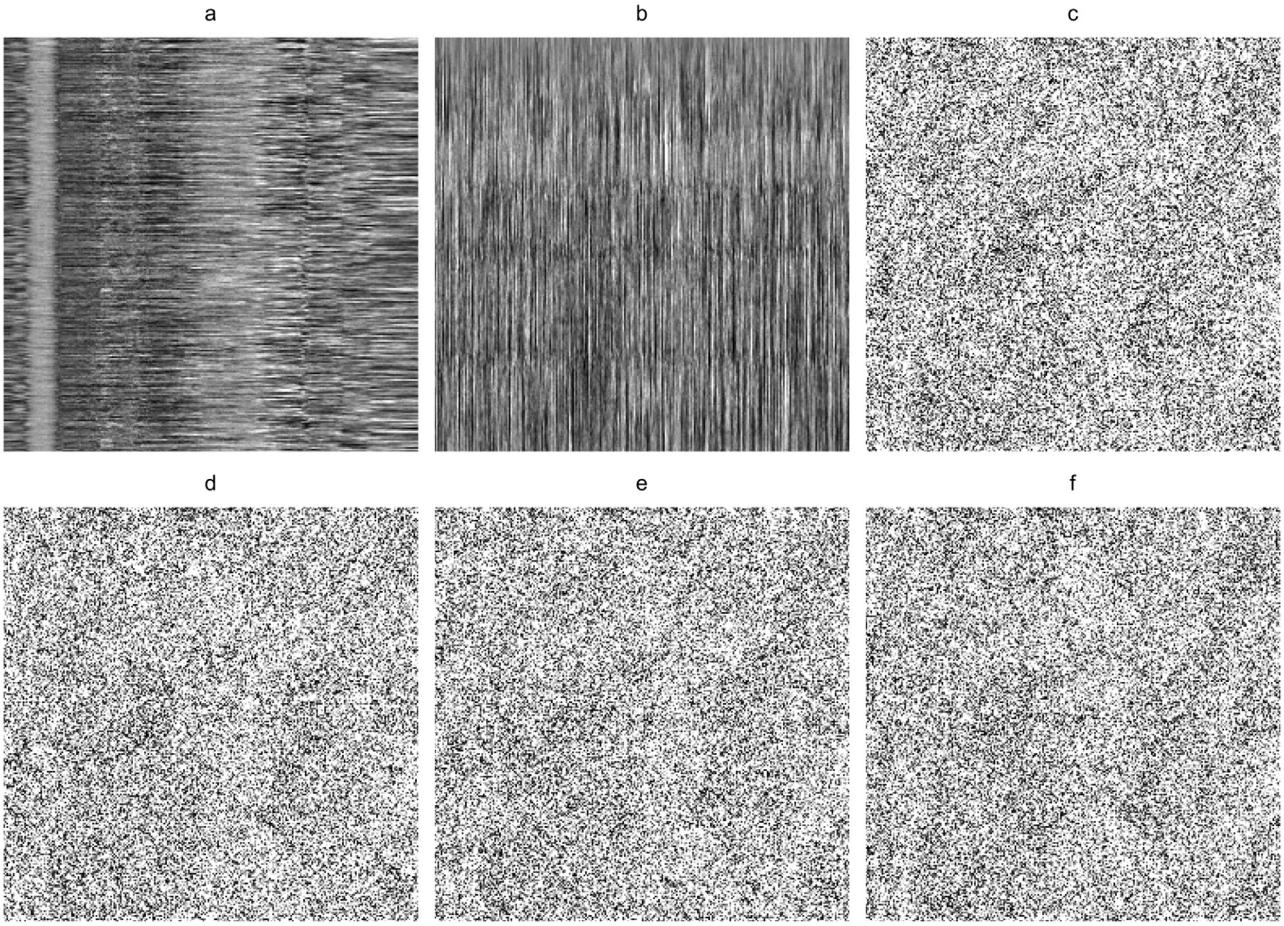


Fig. 6. Decrypted "Lena" with incorrect keys: (a) $x_{01} = 0.11 + 10^{-16}$, (b) $x_{02} = 0.24 + 10^{-16}$, (c) $x_0 = 0.3 + 10^{-15}$, (d) $y_0 = 0.4 - 10^{-15}$, (e) $z_0 = 0.5 + 10^{-15}$ and (f) $h_0 = 0.6 - 10^{-15}$.

Fig. 7(b), (c), (d), (e), (f), (g), respectively. Table 5 lists the PSNR values of the decrypted images with different noise intensities. The results demonstrate that the decrypted images can be still recognized within a certain range of noises. Although the decrypted images would become fuzzier with the increase of noise intensity, the major information of the image can be still figured out. Therefore the proposed scheme could resist against the noise attack to a certain degree.

4.9. Robustness

During the process of image transmission, network failure and network congestion will take place sometimes, thus the encrypted image information may be lost partially or even totally in the worst case. Therefore, it is necessary to evaluate the robust performance of the proposed image compression–encryption algorithm. Fig. 8 (a) gives the encrypted image with triangle pixels cropped (1/8 occlusion), (b) shows the encrypted image with four-corner pixels cropped (1/8 occlusion), (c) is the encrypted image with center pixels cropped (1/4 occlusion) and (d) displays the encrypted image with top pixels cropped (1/2 occlusion). The corresponding decrypted images are shown in Fig. 8(e)–(h), respectively.

From the results, the main information of the original plain

Table 4
Comparison of key space.

Algorithm	Proposed algorithm	Ref. [33]	Ref. [34]	Ref. [41]	Ref. [42]
Key space	2^{276}	2^{16}	2^{128}	2^{78}	2^{96}

Table 3
Key sensitivity test.

Figures	Decryption keys						PNSR (dB)
	x_{01}	x_{02}	x_0	y_0	z_0	h_0	
6(a)	$0.11 + 10^{-16}$	0.24	0.3	0.4	0.5	0.6	12.3575
6(b)	0.11	$0.24 + 10^{-16}$	0.3	0.4	0.5	0.6	12.1604
6(c)	0.11	0.24	$0.3 + 10^{-15}$	0.4	0.5	0.6	2.9838
6(d)	0.11	0.24	0.3	$0.4 - 10^{-15}$	0.5	0.6	2.9152
6(e)	0.11	0.24	0.3	0.4	$0.5 + 10^{-15}$	0.6	2.9374
6(f)	0.11	0.24	0.3	0.4	0.5	$0.6 - 10^{-15}$	2.9746

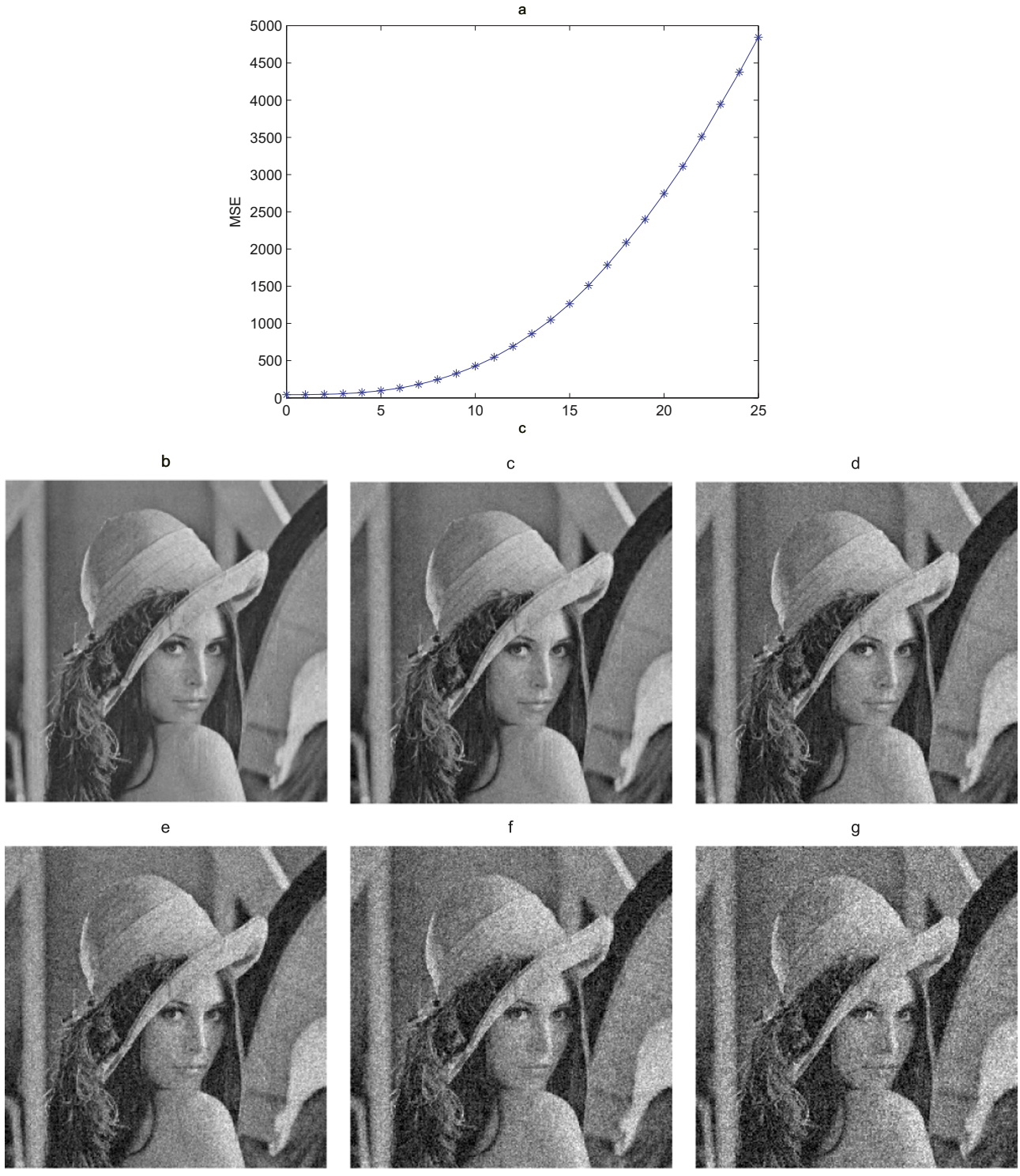


Fig. 7. The results of noise attack with different noise intensities: (a) MSE curve, (b) $c=1$, (c) $c=5$, (d) $c=10$, (e) $c=15$, (f) $c=20$ and (f) $c=25$.

Table 5
PSNR values for different noise intensities.

Noise intensity	1	5	10	15	20	25
PSNR(dB)	30.5884	28.5532	25.3264	22.7359	20.5801	18.9111

image can be still recognizable with correct keys from the decrypted images. The quality of the decrypted images is still acceptable even if the cipher-text is partially missed, which indicates that the original image information is fully diffused in the encryption process and the proposed image compression–encryption scheme is able to defend the shearing attack.

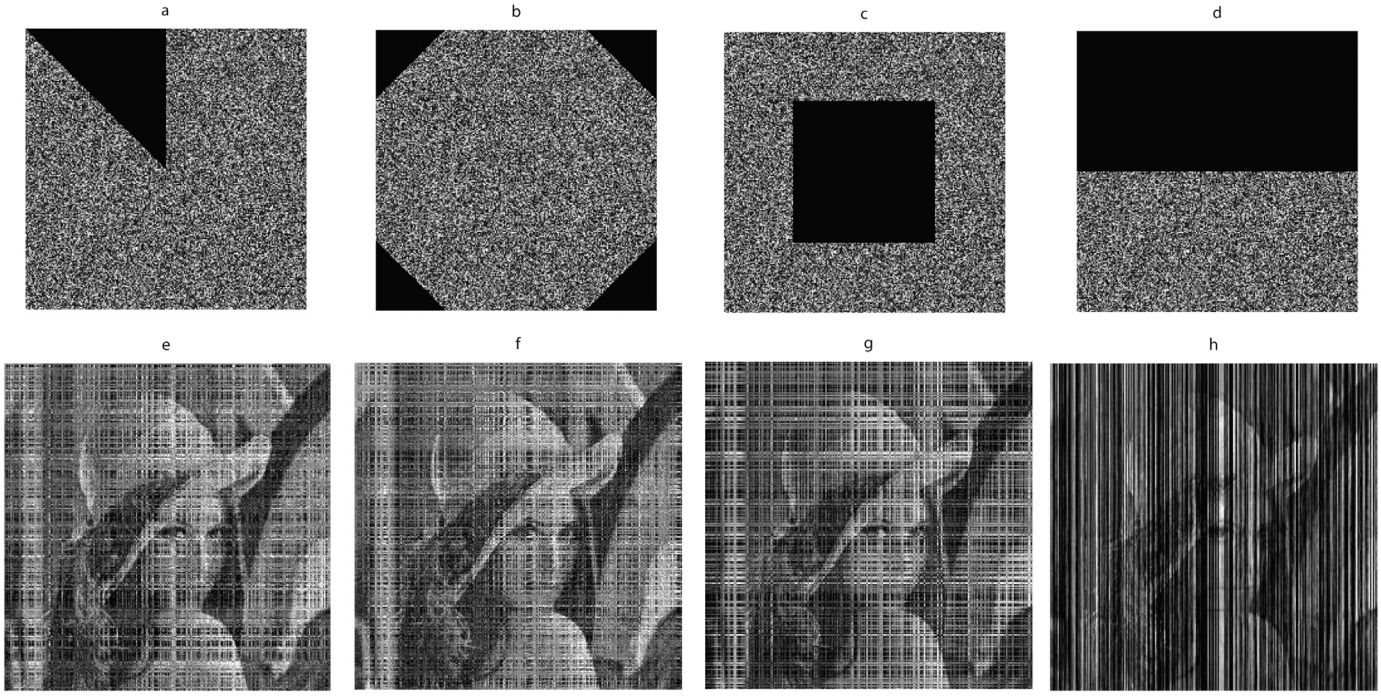


Fig. 8. Robustness of the encryption algorithm. Encrypted images: (a) with triangle pixels cropped (1/8 occlusion), (b) with four corners pixels cropped (1/8 occlusion), (c) with center pixels cropped (1/4 occlusion) and (d) with top pixels cropped (1/2 occlusion). Decrypted images: (e)–(h) are the corresponding decrypted images of (a)–(d), respectively.

4.10. Computation complexity

The computation complexity of the proposed image compression–encryption algorithm was analyzed from the aspect of time complexity of the cyclic shift operation. Assume that the original image x is of size $n \times n$, and the number of the pixels is n^2. The gray-scale information for each pixel of the compressed image is decomposed into an 8 bits binary number in a row in turn to perform the cyclic shift operation. If the compression ratio is 100%, the size of the compressed image is $n \times n$, and the plain adder includes n^2 carry operation. If the compression ratio is $(n-m)(n-m)/n^2$, the elementary gates are $(n-m)(n-m)$. Therefore, the time complexity for the operations is $O(n^2)$ and the computation complexity of the hyper-chaotic system and logistic map both are $O(n)$. However, the computation complexity of the image compression–encryption algorithm is $O(n^2)$. By analyzing the corresponding classical image encryption algorithm, the computation complexity of the generalized Arnold transform is $O(2^{2n})$. The classical random-phase encoding is realized by using 2^{2n} multiplication operations. The computation complexity of the classical Fourier transform is $O(n2^{2n})$. Therefore, the proposed image compression–encryption algorithm takes advantage over its classical counterparts in terms of computation complexity.

5. Conclusion

Based on hyper-chaotic system and 2D compressive sensing, an efficient image compression–encryption scheme is investigated, which possesses the compression ability of the compressive sensing and accomplishes both image compression and image encryption simultaneously. The compression feature of CS theory is employed to cut down the size of the original image proportionally, and then the compressed–encrypted image is re-encrypted by taking the cycle shift operation controlled by the hyper-chaotic system. By utilizing the circulant matrices, the measurement matrices in compressive sensing are constructed as the partial Hadamard matrices controlled by chaos sequences. The decryption process includes the inverse process of the cycle shift operation and the reconstruction process with the NSL_0 algorithm. Simulation results indicate that the proposed image compression–encryption scheme is effective, robust and secure with good compression performance and is also able to stand against statistical analysis, brute force attack and noise attack due to its considerably large key space. In some cases, such as massive monitoring image information in public or private areas, the quality of the decrypted images can be relatively lower while the compression performance is more important, the proposed algorithm could be useful to cut down the costs for storage with acceptable security.

Acknowledgments

This work was supported by the National Natural Science Foundation of China (Grant nos. 61262084 and 61462061), the Foundation for Young Scientists of Jiangxi Province (Jinggang Star) (Grant no. 20122BCB23002), the Opening Project of Shanghai Key Laboratory of Integrate Administration Technologies for Information Security (Grant no. AGK2014004), and the Innovation Project of Jiangxi Graduate Education (Grant nos. YC2015-S036 and YC2014-S070).

References

[1] G.R. Chen, Y.B. Mao, C.K. Chui, A symmetric image encryption scheme based on 3D chaotic cat maps, Chaos Soliton Fractal 21 (2004) 749–761.
[2] T.G. Gao, Z.Q. Chen, A new image encryption algorithm based on hyper-chaos, Phy. Lett. A 372 (2008) 394–400.
[3] T.G. Gao, Q.L. Gu, S.B. Emmanuel, A novel image authentication scheme based on hyper-chaotic cell neural network, Chaos Soliton Fractal 42 (2009) 548–553.
[4] H.G. Zhu, C. Zhao, X.D. Zhang, A novel image encryption-compression scheme using hyper-chaos and chinese remainder theorem, Signal Process-Image 28 (2013) 670–680.

[5] X.J. Tong, Design of an image encryption scheme based on a multiple chaotic map, Commun. Nonlinear Sci. 18 (2013) 1725–1733.
[6] L.F. Chen, J.Y. Liu, J.S. Wen, X. Gao, H.D. Mao, X.Y. Shi, Q.L. Qu, A new optical image encryption method based on multi-beams interference and vector composition, Opt. Laser Technol. 69 (2015) 80–86.
[7] L.F. Chen, J.Y. Liu, J.S. Wen, H.D. Mao, F. Ge, D.M. Zhao, Pseudo color image encryption based on three-beams interference principle and common vector composition, Opt. Commun. 338 (2015) 110–116.
[8] J.X. Chen, Z.L. Zhu, C. Fu, Optical image encryption scheme using 3-D chaotic map based joint image scrambling and random encoding in gyrator domains, Opt. Commun. 341 (2015) 263–270.
[9] G.D. Ye, Image scrambling encryption algorithm of pixel bit based on chaos map, Pattern Recognit. Lett. 31 (2010) 347–354.
[10] G.D. Ye, K.W. Wong, An efficient chaotic image encryption algorithm based on a generalized arnold map, Nonlinear Dyn. 69 (2012) 2079–2087.
[11] G.D. Ye, K.W. Wong, An image encryption scheme based on time-delay and hyperchatic system, Nonlinear Dyn. 71 (2013) 259–267.
[12] C.X. Zhu, C.L. Liao, Breaking and improving an image encryption scheme based on total shuffling scheme, Nonlinear Dyn. 71 (2013) 25–34.
[13] H. Liu, Y.B. Liu, Cryptanalyzing an image encryption scheme based on hybrid chaotic system and cyclic elliptic curve, Opt. Laser Technol. 56 (2014) 15–19.
[14] X.Y. Wang, L.T. Liu, Cryptanalyzing of a parallel sub-image encryption method with high-dimensional chaos, Nonlinear Dyn. 73 (2013) 795–800.
[15] X.Y. Wang, D.P. Luan, X.M. Bao, Cryptanalysis of an image encryption algorithm using Chebyshev generator, Digit. Signal Process. 25 (2014) 244–247.
[16] L.X. Jia, H. Dai, M. Hui, A new four-dimensional hyperchaotic Chen system and its generalized synchronization, Chin. Phys. B 19 (2010) 125–135.
[17] H. Hermassi, R. Rhouma, S. Belghith, Improvement of an image encryption based on hyper-chaos, Telecommun. Syst. 52 (2013) 539–549.
[18] X.J. Tong, Y. Liu, M. Zhang, H. Xu, Z. Wang, An image encryption scheme based on hyperchaotic rabinovich and exponential chaos map, Entropy 17 (2015) 181–196.
[19] R. Boriga, A.C. Dascalescu, I. Priescu, A new hyperchaotic map and its application in an image encryption scheme, Signal Process-Image 29 (2014) 887–901.
[20] H.J. Liu, X.Y. Wang, A. Kadir, Color image encryption using Choquet fuzzy integral and hyperchaotic system, Optik 124 (2013) 3527–3533.
[21] H.G. Zhu, C. Zhao, X.D. Zhang, A novel image encryption-compression scheme using hyper-chaos and chinese remainder theorem, Signal Process-Image 28 (2013) 670–680.
[22] C.X. Zhu, A novel image encryption scheme based on improved hyperchaotic sequences, Opt. Commun. 285 (2012) 29–37.
[23] Y.S. Zhang, D. Xiao, Self-adaptive permutation and combined global diffusion for chaotic color image encryption, AEU-Int. J. Electron. C 4 (2014) 361–368.
[24] F. Ozkaynak, A.B. Ozer, S. Yavuz, Cryptanalysis of a novel image encryption scheme based on improved hyperchaotic sequences, Opt. Commun. 285 (2012) 4946–4948.
[25] A.A. Abdo, S.G. Lian, I.A. Ismail, M. Amin, H. Diab, A cryptosystem based on elementary cellular automata, Commun. Nonlinear Sci. 18 (2013) 136–147.
[26] Y.S. Zhang, D. Xiao, Double optical image encryption using discrete Chirikov standard map and chaos-based fractional random transform, Opt. Lasers Eng. 51 (2013) 472–480.
[27] L.S. Sui, H.W. Lu, Z.M. Wang, Q.D. Sun, Double-image encryption using discrete fractional random transform and logistic maps, Opt. Lasers Eng. 56 (2014) 1–12.
[28] L.S. Sui, K.K. Duan, J.L. Liang, Z.Q. Zhang, H.N. Meng, Asymmetric multiple-image encryption based on coupled logistic maps in fractional fourier transform domain, Opt. Lasers Eng. 62 (2014) 139–152.
[29] M. Khan, T. Shah, A novel image encryption technique based on Hnon chaotic map and S8 symmetric group, Neural Comput. Appl. 25 (2014) 1717–1722.
[30] X.Y. Wang, Y.Q. Zhang, X.M. Bao, A novel chaotic image encryption scheme using DNA sequence operations, Opt. Lasers Eng. 73 (2015) 53–61.
[31] D.L. Donoho, Compressed sensing, IEEE Trans. Inf. Theory 52 (2006) 1289–1306.
[32] E.J. Cands, Compressive sampling, Marta Sanz Sol (2006) 1433–1452.
[33] A. Orsdemir, H.O. Altun, G. Sharma, M.F. Bocko, On the security and robustness of encryption via compressed sensing, in: IEEE Military Communications Conference, 2008 (MILCOM 2008), IEEE, Rochester, 2008, pp. 1–7.
[34] R. Huang, K Sakurai. A robust and compression-combined digital image encryption method based on compressive sensing, in: 2011 7th International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIHMSP), 2011, pp. 105–108.
[35] A.D. Zhang, N.R. Zhou, L.H. Gong, Color image encryption algorithm based on compressive sensing with arnold transform, J. Comput. 8 (2013) 2857–2863.
[36] Endra, R. Susanto. Compressive sensing-based image encryption with optimized sensing Matrix, in: IEEE International Conference on Computational Intelligence and Cybernetics (IEEE Cybernetics Com), 2013, pp. 122–125.
[37] X.Y. Liu, Y.P. Cao, P. Lu, X. Lu, Y. Li, Optical image encryption technique based on compressed sensing and arnold transformation, Optik 124 (2013) 6590–6593.
[38] N.R. Zhou, A.D. Zhang, F. Zheng, L.H. Gong, Novel image compression-encryption hybrid algorithm based on key-controlled measurement matrix in compressive sensing, Opt. Laser Technol. 62 (2014) 152–160.
[39] N.R. Zhou, A.D. Zhang, J.H. Wu, D.J. Pei, Y.X. Yang, Novel hybrid image compression-encryption algorithm based on compressive sensing, Optik 125 (2014) 5075–5080.
[40] N.R. Zhou, H.L. Li, D. Wang, S.M. Pan, Z.H. Zhou, Image compression and encryption scheme based on 2D compressive sensing and fractional Mellin transform, Opt. Commun. 343 (2015) 10–21.
[41] S.N. George, D.P. Pattathil, A secure LFSR based random measurement matrix for compressive sensing, Sens. Imaging: Int. J. 15 (2014) 1–29.
[42] S.N. George, N. Augustine, D.P. Pattathil, Audio security through compressive sampling and cellular automata, Multimed. Tools Appl. 74 (2015) 10393–10417.
[43] X.B. Liu, W.B. Mei, H.Q. Du, Optical image encryption based on compressive sensing and chaos in the fractional fourier domain, J. Mod. Opt. 61 (2014) 1570–1577.
[44] J. Li, H.B. Li, J.S. Li, Y.Y. Pan, R. Li, Compressive optical image encryption with two-step-only quadrature phase-shifting digital holography, Opt. Commun. 344 (2015) 166–171.
[45] H. Mohimani, Z.M. Babaie, C. Jutten, A fast approach for overcomplete sparse decomposition based on smoothed norm, IEEE Trans. Signal Process. 57 (2009) 289–301.
[46] W.J. Lin, R.Z. Zhao, H. Li, The NSL0 algorithm for compressive sensing signal reconstruction, New Ind. 7 (2011) 78–84.