



Full length article

Image compression-encryption algorithms by combining hyper-chaotic system with discrete fractional random transform

Lihua Gong^{a,b,c}, Chengzhi Deng^a, Shumin Pan^b, Nanrun Zhou^{b,*}^aJiangxi Province Key Laboratory of Water Information Cooperative Sensing and Intelligent Processing, Nanchang 330099, China^bDepartment of Electronic Information Engineering, Nanchang University, Nanchang 330031, China^cDepartment of Electrical and Computer Engineering, University of Pittsburgh, Pittsburgh 15261, USA

ARTICLE INFO

Article history:

Received 2 July 2017

Accepted 4 January 2018

Keywords:

Hyper-chaotic system

Discrete cosine transform

Discrete fractional random transform

Zigzag scanning

Image compression

Image encryption

ABSTRACT

Based on hyper-chaotic system and discrete fractional random transform, an image compression-encryption algorithm is designed. The original image is first transformed into a spectrum by the discrete cosine transform and the resulting spectrum is compressed according to the method of spectrum cutting. The random matrix of the discrete fractional random transform is controlled by a chaotic sequence originated from the high dimensional hyper-chaotic system. Then the compressed spectrum is encrypted by the discrete fractional random transform. The order of DFrRT and the parameters of the hyper-chaotic system are the main keys of this image compression and encryption algorithm. The proposed algorithm can compress and encrypt image signal, especially can encrypt multiple images once. To achieve the compression of multiple images, the images are transformed into spectra by the discrete cosine transform, and then the spectra are incised and spliced into a composite spectrum by Zigzag scanning. Simulation results demonstrate that the proposed image compression and encryption algorithm is of high security and good compression performance.

© 2018 Elsevier Ltd. All rights reserved.

1. Introduction

More and more image information is conveying over network. The security of important images attracts a number of researchers to investigate image encryption algorithms [1–10]. Chen et al. presented a new iterative phase retrieval algorithm for optical image encryption in three-dimensional space by considering the two-dimensional plaintext as a series of particles distribution in 3D space [1]. Later, they proposed a new optical image encryption method based on multiple-region plaintext and phase retrieval algorithm in 3D space [2], where the plaintext was divided into multiple regions and each region was encrypted into one phase-only mask. An optical image encryption scheme based on coherent diffractive imaging with multiple wavelengths was proposed [3]. He et al. analyzed the collision property of the optical image encryption technique based on interference and found that various distinct pairs of phase-only masks could yield almost the same outputs by a modified phase retrieval algorithm [4]. Sui et al. proposed a multiple-image encryption scheme based on the phase retrieval process and phase mask multiplexing in the fractional Fourier transform domain, where each original image was encoded

into a phase-only function and then all the obtained phase functions were modulated into an interim [5]. Lu et al. presented a novel optical image encryption method based on a modified radial shearing interferometer, in which the plaintext image was first encoded into a phase-only mask and then was modulated by a random phase mask [6]. Yuan et al. devised an optical multi-user authentication way based on interference image hiding system and phase-only correlation, where some predefined complex images with different amplitudes and the same phase were respectively encoded into two phase-only masks according to the interference principle [7]. A flexible multiple-image encryption algorithm based on log-polar transform and double random phase encoding technique was proposed [8]. A color image encryption algorithm was designed with the affine transform in the Gyrator transform domain, where the RGB components of the color image were converted into real part and imaginary one of a complex function [9]. Liu et al. proposed a double image encryption scheme by combining random phase encoding with pixel exchanging in the Gyrator transform domain [10]. Rachlin and Baron demonstrated that the linear encryption scheme based on compressive sensing cannot achieve perfect security [11]. To solve these problems, Zhou et al. presented a novel image compression-encryption hybrid algorithm based on compressive sensing, in which the

* Corresponding author.

E-mail addresses: nrzhou@ncu.edu.cn, znr21@163.com (N. Zhou).

measurement matrix is controlled by keys easy to distribute, store or memorize [12].

The well-known double random phase encoding (DRPE) scheme was proposed to encrypt an image into stationary white noise data by multiplying a random phase in mask (RPM) in the spatial plane while another in the frequency plane [13]. The optical encryption schemes based on Fresnel transform (FrT) [14–16], fractional Fourier transform (FrFT) [17–21], Gyration transform (GT) [22,23] have been investigated. Li cryptanalyzed a class of image encryption schemes based on Chinese Remainder Theorem [24]. To make the image encryption scheme more practical, fractional angular transform with minimum kernel matrix was proposed by Liu et al. [25]. Subsequently, double image encryption schemes based on fractional angular transform was designed with high encryption efficiency [26,27]. An efficient image compression-encryption scheme based on hyper-chaotic system and 2D compressive sensing was designed [28].

DRPE-based image encryption schemes are vulnerable to the chosen-plaintext attack and the known-plaintext attack. He et al. proposed a hybrid two-step attack scheme combining the chosen-plaintext attack and the known-plaintext attack algorithm to acquire the secret keys of the optical cryptosystem based on double random phase-amplitude encoding technique [29]. Subsequently, an asymmetric double-image encryption algorithm was devised by Wang et al., where the encryption keys are different from the decryption ones [30]. A novel technique for multiple-image optical encryption is presented by Zhou et al., where the plaintexts extracted mode is extended from peer-to-peer to peer-to-multiplepeer [31]. To overcome the security risk of image encryption systems based on linear transforms, the nonlinear fractional Mellin transform was introduced into the field of image encryption [32]. To overcome the shortcomings of low-dimensional chaotic system, an image compression-encryption algorithm based on hyper-chaotic system and discrete fractional random transform is designed.

The rest of this paper is arranged as follows. In Section 2, the DFrRT is reviewed. The detailed description of the proposed image

compression-encryption algorithm is provided in Section 3. In Section 4, simulations and discussions are performed. Finally, a brief conclusion is drawn in Section 5.

2. Discrete fractional random transform

The discrete fractional random transform of a two dimensional signal I is

$$\mathbf{E}_R = \mathbf{H}^\alpha I (\mathbf{H}^\alpha)^T \tag{1}$$

where \mathbf{E}_R is the kernel transform of the DFrRT, $(\mathbf{H}^\alpha)^T$ is the transpose of \mathbf{H}^α , α is the fractional order. The kernel transform \mathbf{H}^α is defined as:

$$\mathbf{H}^\alpha = \mathbf{\Gamma} \mathbf{D}^\alpha \mathbf{\Gamma}^t \tag{2}$$

where $\mathbf{\Gamma}$ is the eigenvector basis, $\mathbf{\Gamma}^T$ is the transpose of $\mathbf{\Gamma}$ and $\mathbf{\Gamma} \mathbf{\Gamma}^T = \mathbf{I}$. \mathbf{D}^α is an $N \times N$ diagonal matrix.

$$\mathbf{D}^\alpha = \text{diag} \left\{ 1, \exp \left(-\frac{i2\pi\alpha}{T} \right), \exp \left(-\frac{i4\pi\alpha}{T} \right), \dots, \exp \left[-\frac{i2(N-1)\pi\alpha}{T} \right] \right\} \tag{3}$$

where positive number T is the period of DFrRT.

$$\mathbf{E} = \frac{\mathbf{P} + \mathbf{P}^t}{2} \tag{4}$$

The transform kernel of DFrRT is random which results from the randomness of matrix \mathbf{I} .

3. Image compression-encryption algorithm based on hyper-chaotic system and DFrRT

Fig. 1 shows the order of Zigzag operation. The proposed image compression and encryption algorithm is illustrated in Fig. 2 and the compression and encryption process is as follows.

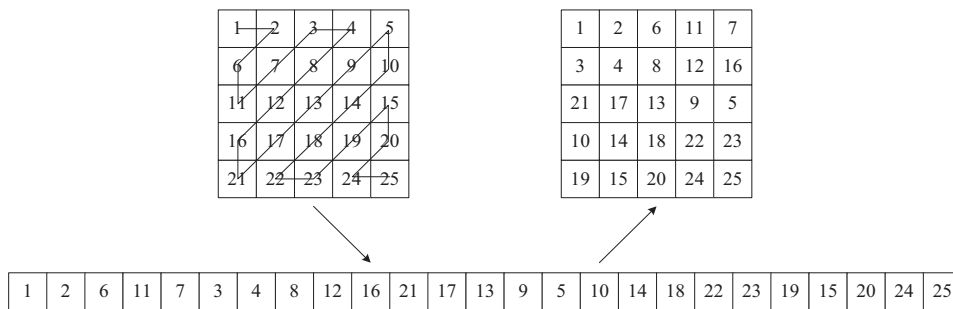


Fig. 1. The order of Zigzag operation.

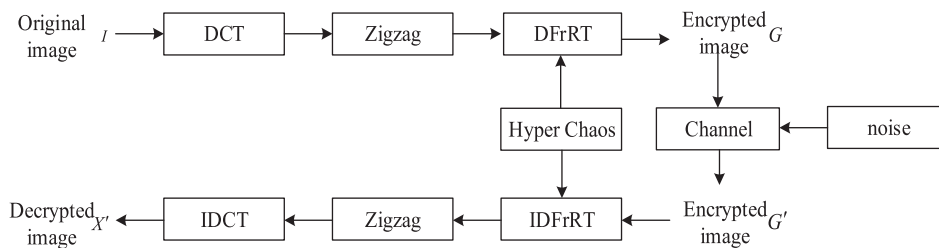


Fig. 2. Image compression-encryption algorithm based on hyper-chaos and DFrRT.

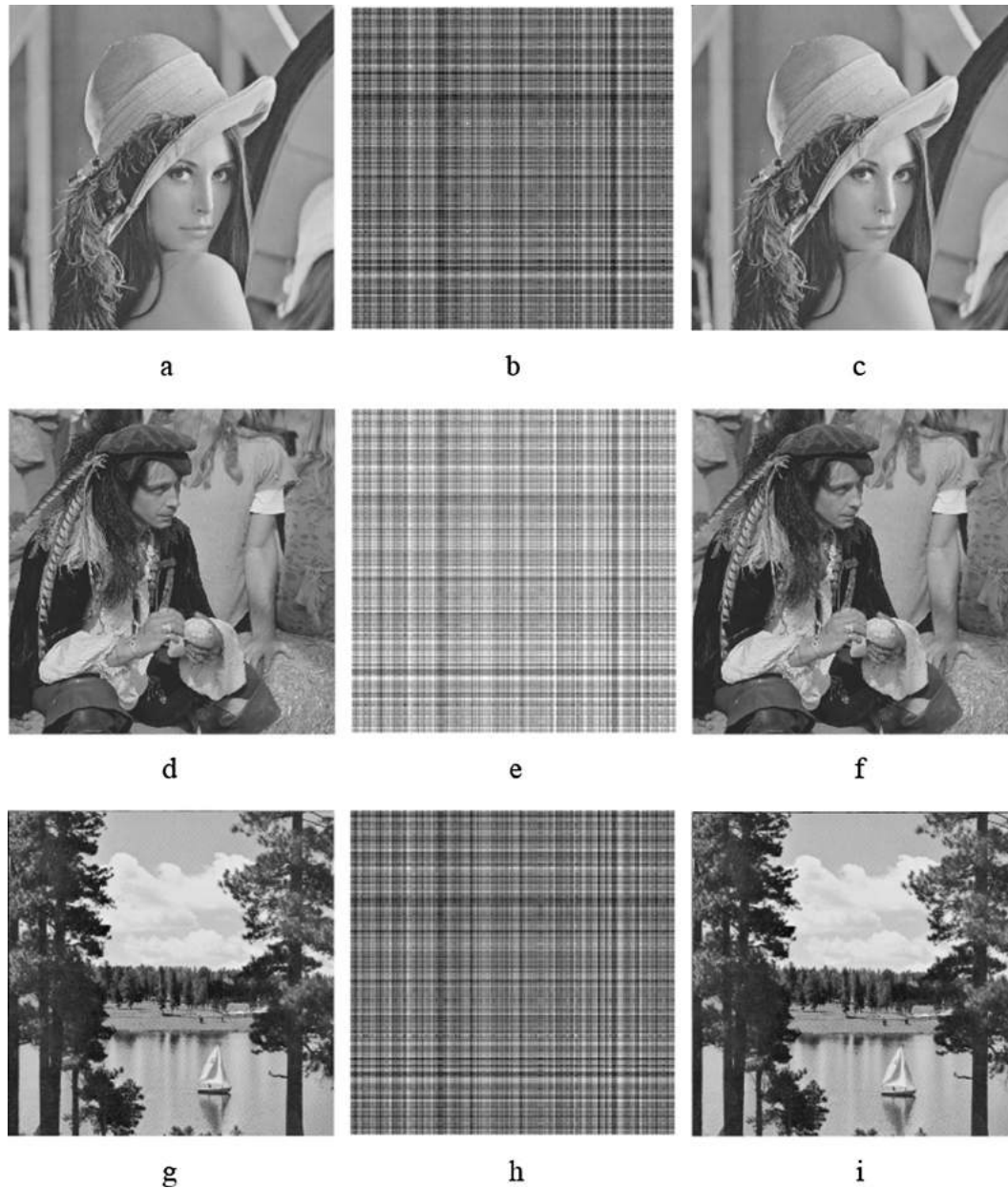


Fig. 3. Encryption and decryption results: (a) Original “Lena”, (b) Encrypted image of (a), (c) Decrypted image of (b); (d) Original “Man”, (e) Encrypted image of (d), (f) Decrypted image of (e); (g) Original “Lake”, (h) Encrypted image of (g), (i) Decrypted image of (h).

Step 1 To compress image, the original image I is transformed into spectrum by the fractional cosine transform.

Step 2 Scanning the matrix by Zigzag operation respectively to form the one-dimensional matrix I_1 .

Step 3 Intercepting the $M \times M$ previous sections of the one-dimensional matrix as I_2 . The front part of the elements implies the main information to be encrypted is contained in the DC component, i.e., the low frequency part of the image.

Step 4 By confirming the value of the initial conditions x_0, y_0, z_0, h_0 , and iterating the Chen’s chaos system by the Runge–Kutta method to avoid the harmful effect of transient procedure, the four hyper-chaotic sequences $\{x_i\}, \{y_i\}, \{z_i\}$ and $\{h_i\}$ ($1 \leq i \leq n_0$) can be generated with the following Chen’s hyper-chaotic system.

$$\begin{cases} \dot{x} = a(y - x) \\ \dot{y} = dx - xz + cy - h \\ \dot{z} = xy - bz \\ \dot{h} = x + k \end{cases} \quad (5)$$

where a, b, c, d and k are the parameters of the hyper-chaotic system.

Step 5 The four hyper-chaotic sequences $\{x_i\}, \{y_i\}, \{z_i\}$ and $\{h_i\}$ are transformed into integer sequences $\{t_i^*\}$, where t can be considered as any one of x, y, z and h .

$$t_i^* = \lfloor (t_i - \lfloor t_i \rfloor) \times 10^{14} \rfloor \bmod 224 \quad (6)$$

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

Step 6 A hyper-chaotic sequence $K = \{k_1, k_2, \dots, k_{2n}\}$ is constructed. If $h_i^* \bmod 3 = 0$, then k_i will take x_i^* as the random

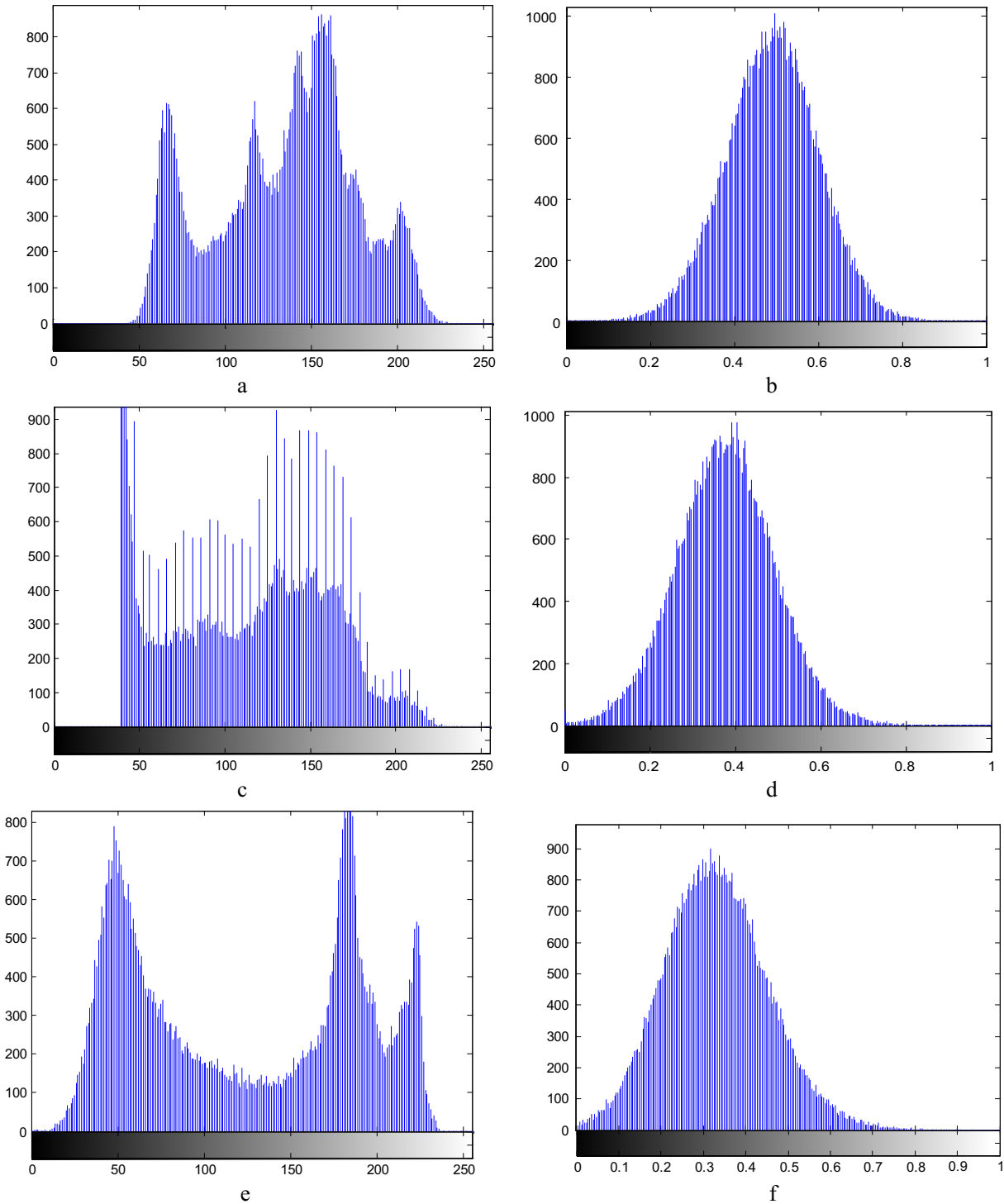


Fig. 4. Histograms: (a) “Lena”, (b) encrypted “Lena” (c) “Man”, (d) encrypted “Man”, (e) “Lake”, (f) encrypted “Lake”.

matrix of DFrRT. If $h_i^* \bmod 3 = 1$, then k_i will take y_i^* as the random matrix of DFrRT. Otherwise, k_i will take z_i^* as the random matrix of DFrRT. The integer k_i can be represented as a binary number $k_i = h_i^7 h_i^6 \dots h_i^0$, $h_i^j \in \{0, 1\}$, $i = 1, 2, \dots, 2^{2n}$, $j = 0, 1, \dots, 7$.

Step 7 The final encryption image I_2 can be obtained by performing discrete fractional random transform on $\mathbf{R}^\alpha(I_2)$, where the fractional order α is the only key of DFrRT.

4. Simulation experiment and analysis

Simulations and analysis on various grayscale images have been performed on a Matlab 7.11.0 (R2010b) platform. For conciseness and simplicity, the calculation formulae of the image correlation coefficient, peak-to-peak signal-to-noise ratio (PSNR) and mean squared error (MSE) [43] are not repeated here. Three plain-images “Lena”, “Man” and “Lake” of size 256×256 are designated

Table 1
Correlation coefficients of adjacent pixels.

Correlation coefficient	Horizontal direction	Vertical direction	Diagonal direction
"Lena"	0.9569	0.9236	0.9019
Encrypted "Lena" with proposed algorithm	0.4968	0.4938	0.0480
Encrypted "Lena" with algorithm in [25]	0.6661	0.6407	0.3452
"Man"	0.9544	0.9471	0.9200
Encrypted "Man" with proposed algorithm	0.5017	0.5220	0.0454
Encrypted "Man" with algorithm in [25]	0.6920	0.6850	0.4361
"Lake"	0.9377	0.9403	0.9100
Encrypted "Lake" with proposed algorithm	0.4996	0.5029	0.0647
Encrypted "Lake" with algorithm in [25]	0.6887	0.6435	0.4873

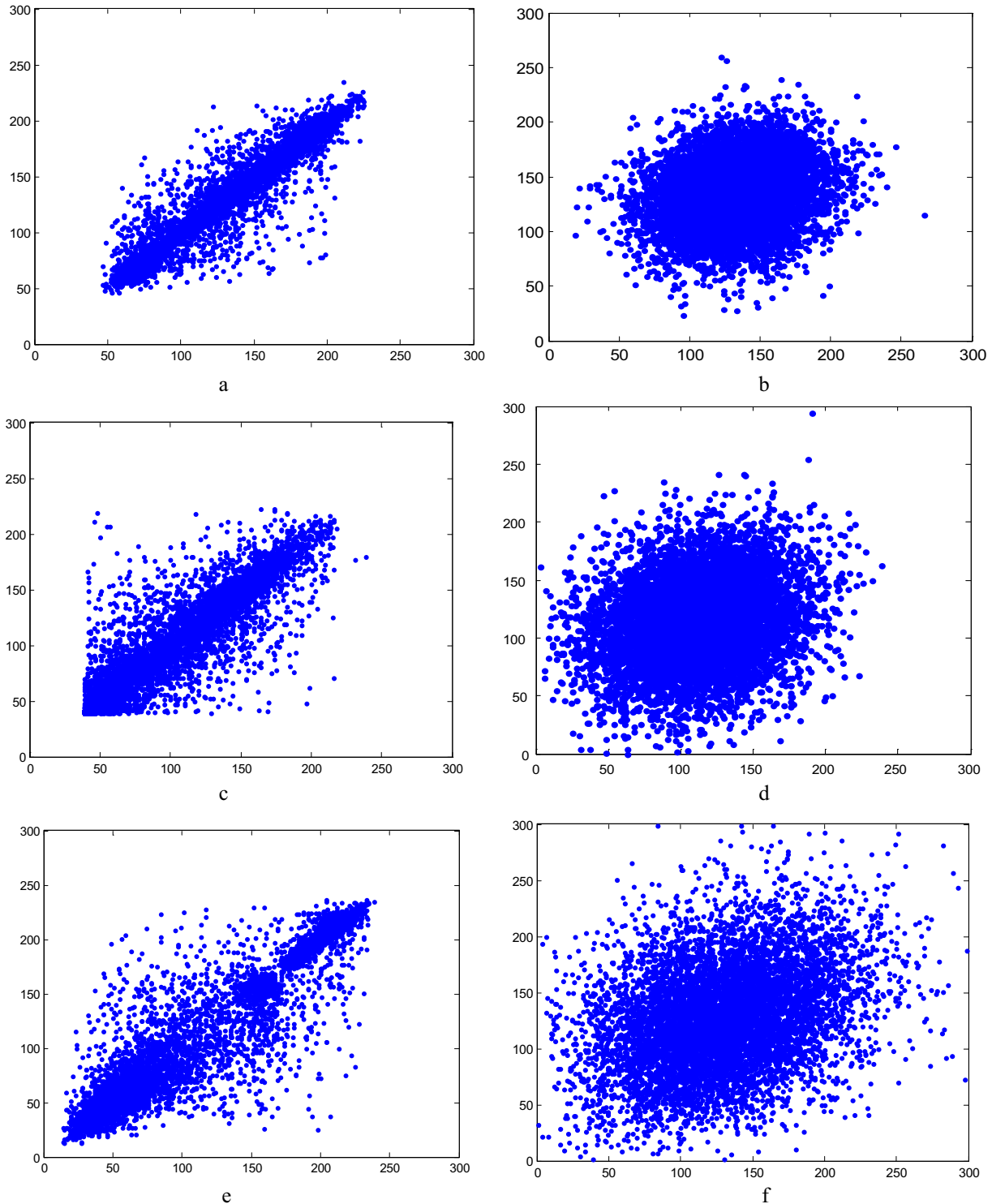

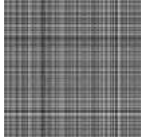

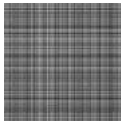




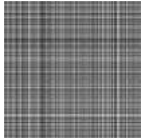

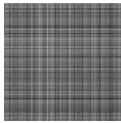





Fig. 5. Correlation distribution: (a) original "Lena", (b) encrypted "Lena", (c) original "Man", (d) encrypted "Man", (e) original "Lake"; and (f) encrypted "Lake".

Table 2
PSNR values for different compression ratios.

Original image	Compression ration (%)	Compressed-encrypted image	Recovered image
	76.5625		
	56.25		
	25		
	76.5625		
	56.25		
	25		

as the test images. The four initial parameters x_0, y_0, z_0, h_0 of hyper-chaotic system and the fractional order α of the discrete fractional random transform are taken as 0.3, 0.4, 0.5, 0.6 and 0.2, respectively. The step length of the Runge-Kutta method is set as 0.001. The encrypted images “Lena”, “Man” and “Lake” are shown in Fig. 3(b), (e), (h). The corresponding ideal decrypted images with correct keys are shown in Fig. 3(c), (f), (i).

4.1. Histogram and correlation of adjacent pixels

Histogram is an important statistical feature of an image, which is often used to analyze the performance of image encryption algorithms. Fig. 4(a), (c) and (e) are the corresponding histograms of the original images, while Fig. 4(b), (d) and (f) are the corresponding histograms of the encrypted images, respectively. Obviously, the histograms of different encryption images show a similar Gaussian-like distribution, though the histograms of different original images are apparently different. So as for resisting the statistical analysis attacks by histogram, the proposed image compression-encryption algorithm is secure.

In order to verify the security of the proposed algorithm, we test the correlation of adjacent pixels and joint distribution analysis. (1) 10,000 pairs of adjacent pixels in horizontal, vertical, and diagonal

directions are randomly selected from the original images and corresponding encrypted images as samples; (2) the correlations between two adjacent pixels are calculated for each direction. Table 1 shows the correlation of adjacent pixels of original images and encrypted images with different methods. The values of the correlation coefficients between two adjacent pixels in the encrypted images are much weaker than those in their corresponding original images. The correlation coefficients between two adjacent pixels in the encrypted images with the proposed algorithm are also smaller than those with the algorithm in [25]. It indicates that the proposed algorithm has a certain ability to resist correlation attack (see Fig. 5.).

4.2. Compression performance

The proposed algorithm can compress and encrypt the images simultaneously. To evaluate the quality of the decrypted digital images versus different compression ratios, peak-to-peak signal-to-noise ratio is employed.

Table 2 lists the PSNR values for different compression ratios. While the size of the compressed image is 25% as large as the original image, the quality of the decrypted image is acceptable in some degree, which means the compression ability of the proposed method is great and helpful for transmission.

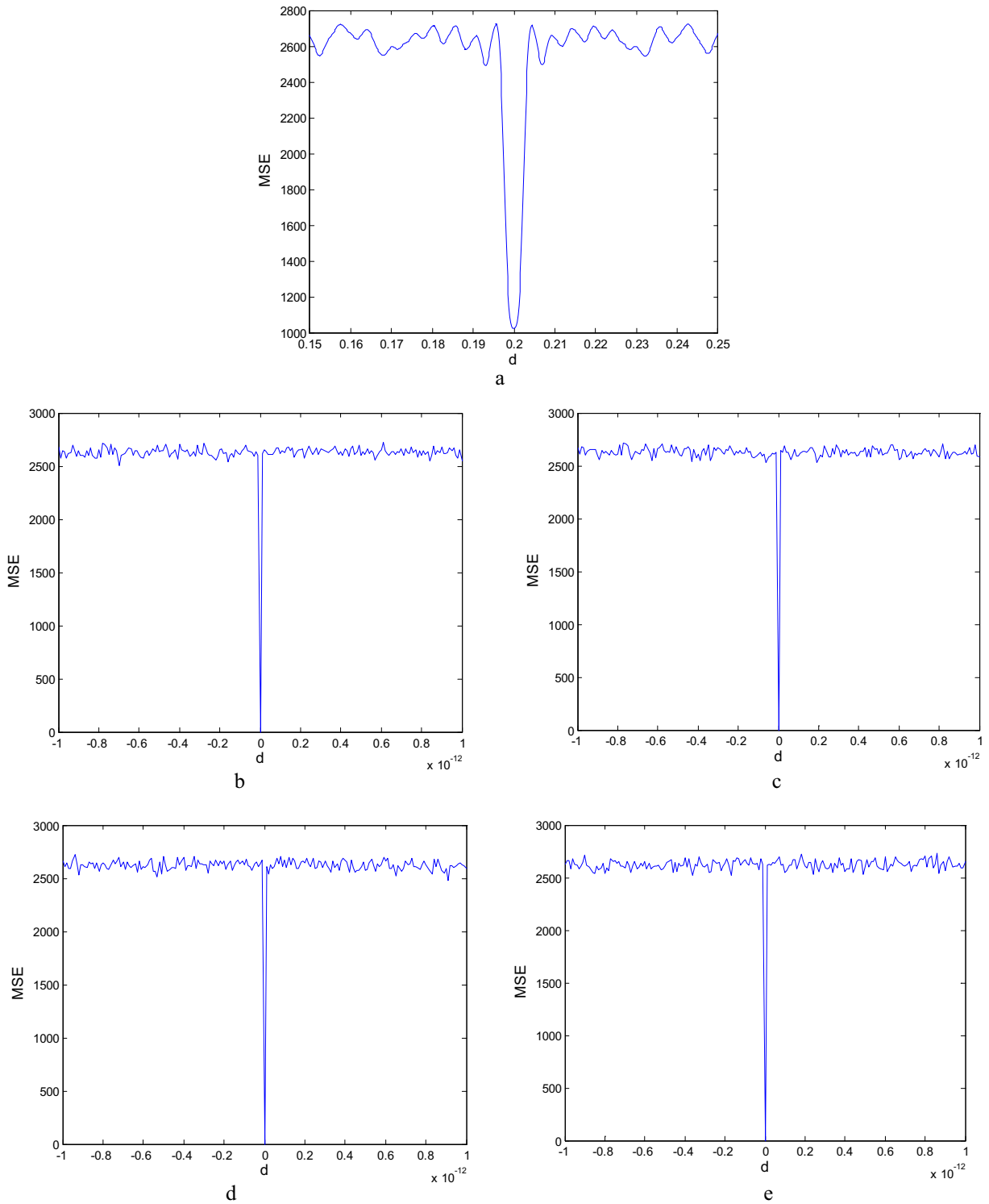


Fig. 6. MSE curves: (a) α , (c) x_0 , (d) y_0 , (e) z_0 , and (f) h_0 .

4.3. Key sensitivity and key space

MSE is an important factor to evaluate key sensitivity in image encryption algorithm, and PSNR is widely used to evaluate the quality of the decrypted image. Fig. 6 shows the MSE curves of “Lena” for x_0, y_0, z_0, h_0 and α , respectively. From Fig. 6, the MSE values change apparently when a little deviation from the correct keys exists. Therefore the encrypted image can be decrypted when

all the secret keys are exactly correct. Fig. 7 exhibits the decrypted image “Lena” with only one incorrect secret key while other secret keys are correct.

The size of key space reflects the difficulty and the complexity in attacking a cryptosystem successfully, thus a large enough key space is necessary to resist the brute-force attack. In the proposed algorithm, α, x_0, y_0, z_0 , and h_0 are main keys. The key space S can be determined by the key subspace S_i of the i th key, $i = 1, 2, \dots, 5$.

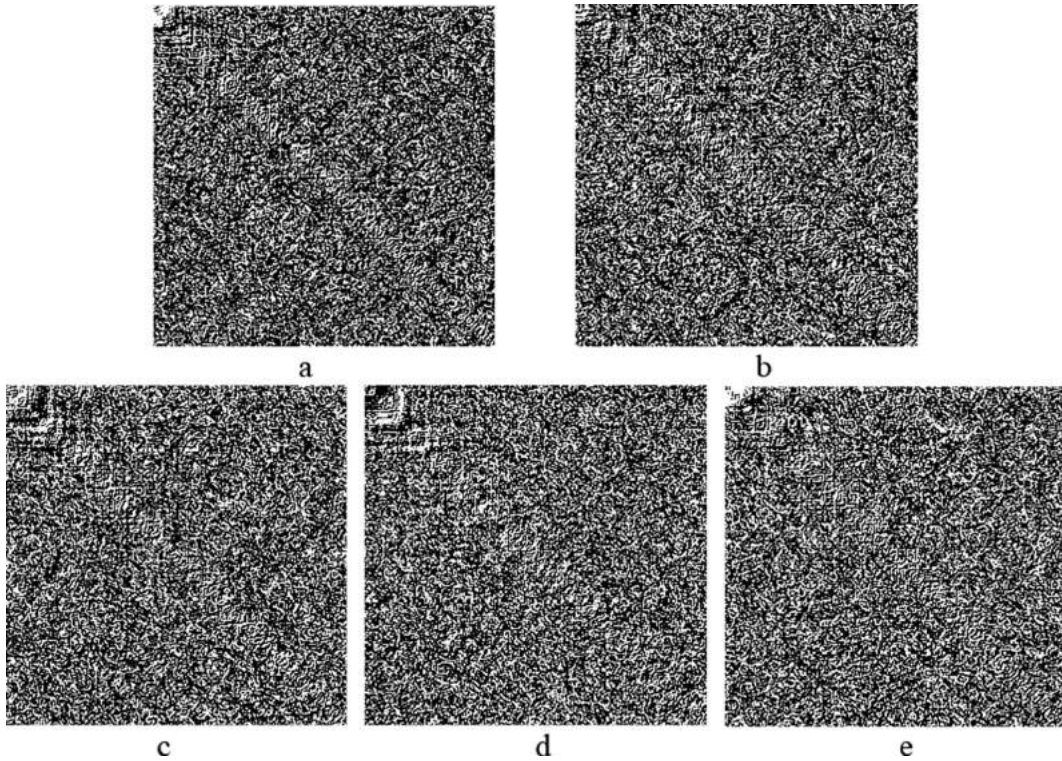


Fig. 7. Decrypted “Lena” with incorrect keys: (a) $a = 0.195$, (c) $x_0 = 0.3 + 10^{-15}$, (d) $y_0 = 0.4 - 10^{-15}$, (e) $z_0 = 0.5 + 10^{-15}$ and (f) $h_0 = 0.6 - 10^{-15}$.

Table 3
Key space of different algorithms.

Algorithm	Proposed algorithm	Algorithm in [33]	Algorithm in [34]	Algorithm in [35]
Key space	2^{187}	2^{16}	2^{128}	2^{186}

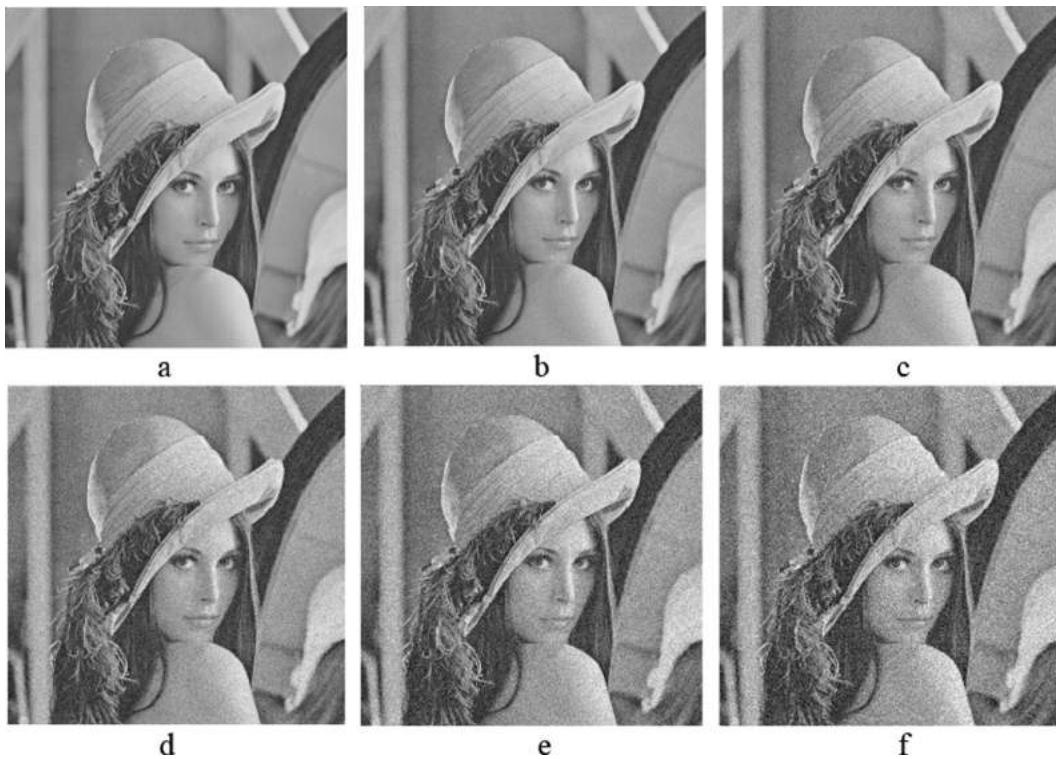


Fig. 8. The results of attacks with different noise intensities of which (a)–(f) are added Gaussian noise $k = 1$, (b) $k = 5$, (c) $k = 10$, (d) $k = 15$, (e) $k = 20$, (f) $k = 25$.

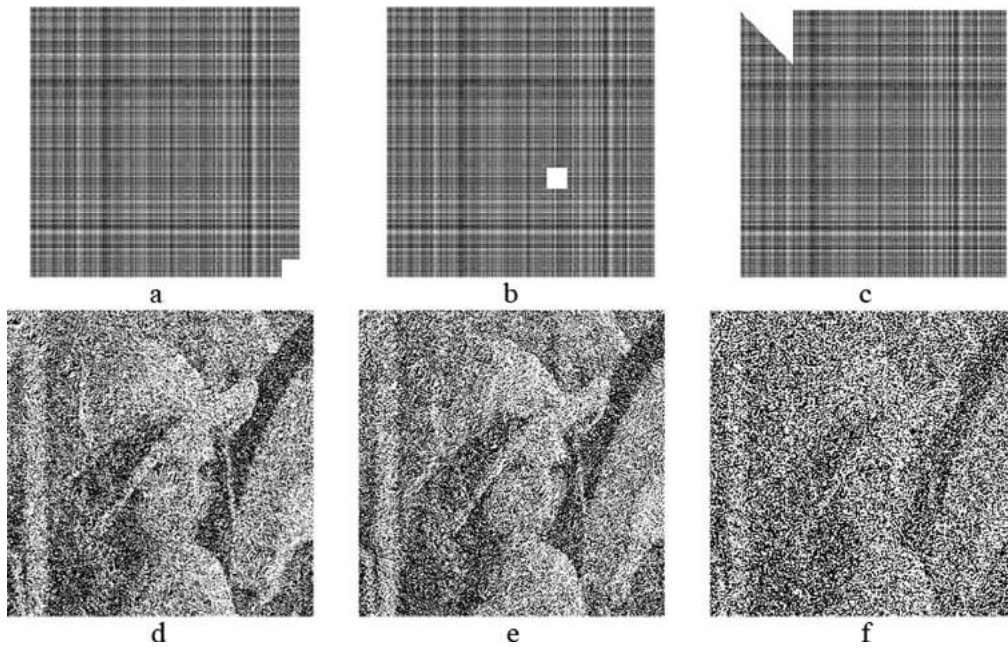


Fig. 9. Results of attacks with different occlusion sizes.

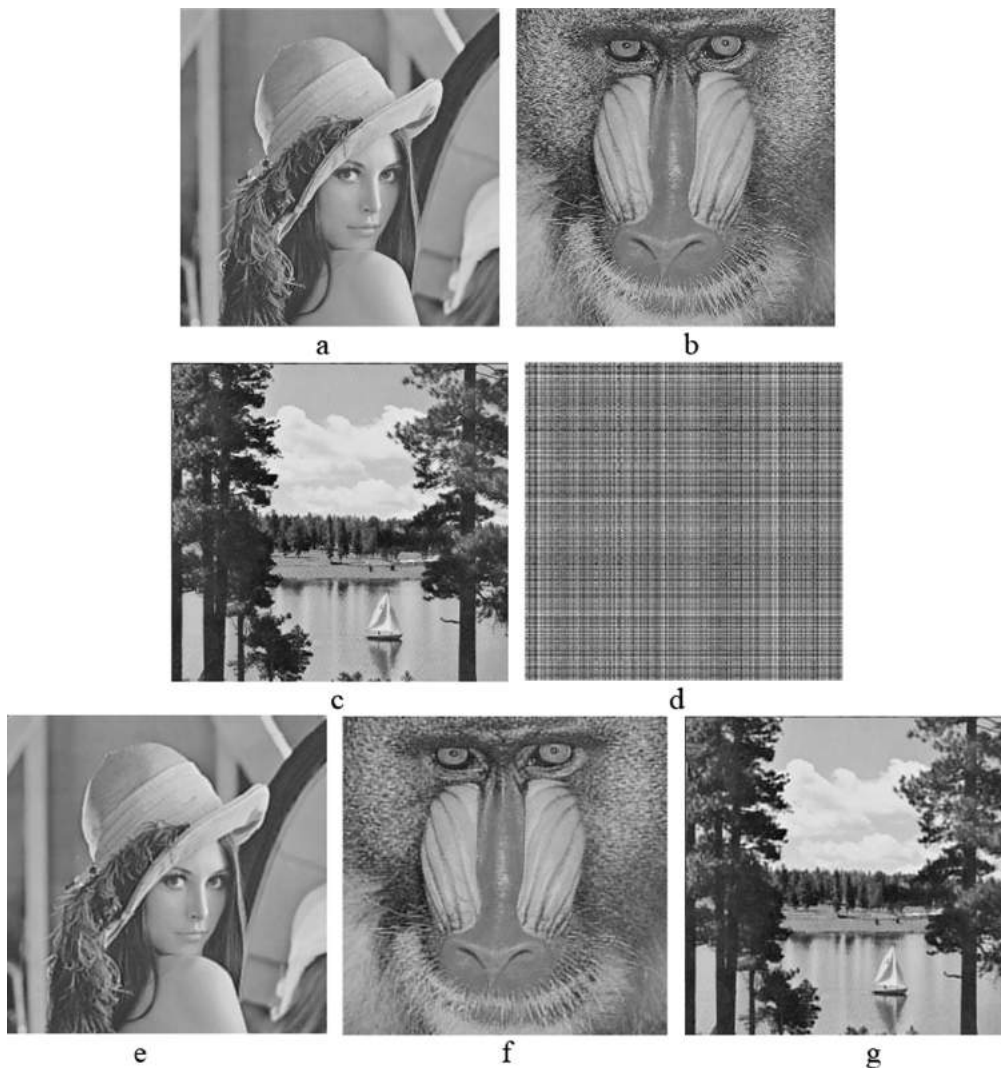


Fig. 10. Results of the test images. (a)–(c) original images, (d) encrypted image, (e)–(g) decrypted images.

Simulation results show that the space of α is about 200. Similarly, each key space of x_0 , y_0 , z_0 , and h_0 is up to 10^{15} as shown in Fig. 7, respectively. The total key space S is greater than 2^{187} , which is large enough to resist the brute-force attack and better than those in [33–35] (see Table 3.).

4.4. Robustness analysis

When the encrypted images are affected inevitably by noise and occlusion in the transform process, they are expected to be recovered correctly though the robustness against noise and occlusion is contradicted with security. In this simulation, the Gaussian noises are added into the ideal encrypted image, respectively. Suppose the Gaussian noise is expressed as:

$$E' = E + kW \quad (7)$$

where E' and E are the noisy encrypted images and the pure encrypted images, respectively, k is the coefficient related to noise intensities, and W is the white Gaussian random data with zero-mean and unit standard deviation. Fig. 8 shows the decrypted images of “Lena”, which are added Gaussian noise with different intensities. From Fig. 8, the decrypted images are recognized in general almost within a certain range of noise, and the major information of the decrypted images is still obtained. The results show that the proposed scheme can resist noise attacks to some extent. Another important robustness analysis is the occlusion, and the results of “Lena” are exhibited in Fig. 9. Although the decrypted images become fuzzier with the increase of occlusion size, the major content of the image can be recognized. Therefore, it can be considered that the proposed scheme has a high robustness against noise and occlusion attacks.

4.5. Three images encryption

Beside compressing and encrypting single image, the proposed algorithm can also compress and encrypt multiple images simultaneously. To achieve the compression of multiple images, the original images are transformed into spectra by the discrete cosine transform, and then the spectra are incised and spliced by Zigzag scanning into a composite spectrum. Three images are chosen to test the effectiveness and the encryption capacity. The original test images are shown in Fig. 10(a)–(c), the ideal decrypted images with correct keys are shown in Fig. 10(e)–(g). The simulation results show that the presented algorithm can compress and encrypt multi-image flexibly.

5. Conclusion

An image compression-encryption algorithm based on hyper-chaotic system, discrete cosine transform and discrete fractional random transform is designed. The chaotic sequence originated from the high dimensional hyper-chaotic system is used to control the random matrix of the discrete fractional random transform, and then the compressed spectrum is encrypted by the discrete fractional random transform. The main keys of this image encryption scheme include the order of DFRT and the parameters of the hyper-chaotic system. The algorithm not only could compress and encrypt single image, but also could compress and encrypt multiple images simultaneously. Simulation results indicate that the proposed scheme is effective, secure and robust to compress-encrypt and decompress-decrypt images, which could resist statistical analysis attack, brute-force attack and noise attack.

Acknowledgments

This work is supported by the National Natural Science Foundation of China (Grant Nos. 61462061 and 61262084), the China Scholarship Council (Grant No. 201606825042), the Department of Human Resources and Social security of Jiangxi Province, the Major Academic Discipline and Technical Leader of Jiangxi Province (Grant No. 20162BCB22011), the Natural Science Foundation of Jiangxi Province, China (Grant No. 20171BAB202002) and the Opening Project of Jiangxi Province Key Laboratory of Water Information Cooperative Sensing and Intelligent Processing (Grant No. 2016WICSIP001).

References

- [1] W. Chen, X.D. Chen, C.J.R. Sheppard, Optical image encryption based on phase retrieval combined with three-dimensional particle-like distribution, *J. Opt.* 14 (7) (2012) 07542.
- [2] W. Chen, X.D. Chen, Optical image encryption based on multiple-region plaintext and phase retrieval in three-dimensional space, *Opt. Lasers Eng.* 51 (2) (2013) 128–133.
- [3] W. Chen, X. Chen, C.J.R. Sheppard, Optical image encryption based on coherent diffractive imaging using multiple wavelengths, *Opt. Commun.* 285 (3) (2012) 225–228.
- [4] W.Q. He, X. Peng, X.F. Meng, et al., Collision in optical image encryption based on interference and a method for avoiding this security leak, *Opt. Laser Technol.* 47 (47) (2013) 31–36.
- [5] L.S. Sui, M.T. Xin, A.L. Tian, Multiple-image encryption based on phase mask multiplexing in fractional Fourier transform domain, *Opt. Lett.* 38 (11) (2013) 1996–1998.
- [6] D.J. Lu, W.Q. He, X. Peng, Optical image encryption based on a radial shearing interferometer, *J. Opt.* 15 (10) (2013) 105405.
- [7] S. Yuan, T. Zhang, X. Zhou, et al., Optical authentication technique based on interference image hiding system and phase-only correlation, *Opt. Commun.* 304 (1) (2013) 129–135.
- [8] L.H. Gong, X.B. Liu, F. Zheng, N.R. Zhou, Flexible multiple-image encryption algorithm based on log-polar transform and double random phase encoding technique, *J. Mod. Opt.* 60 (13) (2013) 1074–1082.
- [9] H. Chen, X.P. Du, Z.J. Liu, C.W. Yang, Color image encryption based on affine transform and Gyrator transform, *Opt. Lasers Eng.* 51 (6) (2013) 768–775.
- [10] Z. Liu, Y. Zhang, S. Li, W. Liu, W. Liu, Y. Wang, S. Liu, Double image encryption scheme by using random phase encoding and pixel exchanging in the Gyrator transform domains, *Opt. Laser Technol.* 47 (2013) 152–158.
- [11] Y. Rachlin, D. Baron, The secrecy of compressed sensing measurements, in: 2008 46th Annual Allerton Conference on Communication, Control, and Computing, IEEE, Urbana-Champaign, 2008, pp. 813–817.
- [12] N.R. Zhou, A.D. Zhang, F. Zheng, et al., Novel image compression-encryption hybrid algorithm based on key-controlled measurement matrix in compressive sensing, *Opt. Laser Technol.* 62 (2014) 152–160.
- [13] B. Javidi, P. Refregier, Optical image encryption based on input plane and Fourier plane random encoding, *Opt. Lett.* 20 (7) (1995) 767–769.
- [14] P.W.M. Tsang, T.C. Poon, K.W.K. Cheung, Fast numerical generation and encryption of computer-generated Fresnel holograms, *Appl. Opt.* 50 (7) (2011) B46–B52.
- [15] S.K. Rajput, N.K. Nishchal, Known-plaintext attack-based optical cryptosystem using phase-truncated Fresnel transform, *Appl. Opt.* 52 (4) (2013) 871–878.
- [16] X.J. Shen, S.F. Dou, M. Lei, Y.D. Chen, Optical image encryption based on a joint Fresnel transform correlator with double optical wedges, *Appl. Opt.* 55 (30) (2016) 8513–8522.
- [17] S.E. Azoug, S. Bouguezal, A non-linear preprocessing for opto-digital image encryption using multiple-parameter discrete fractional Fourier transform, *Opt. Commun.* 359 (2016) 85–94.
- [18] S.K. Rajput, N.K. Nishchal, Image encryption based on interference that uses fractional Fourier domain asymmetric keys, *Appl. Opt.* 51 (10) (2012) 1446–1452.
- [19] L. Yuan, Q.W. Ran, T.Y. Zhao, Image authentication based on double-image encryption and partial phase decryption in nonseparable fractional Fourier domain, *Opt. Laser Technol.* 88 (2017) 111–120.
- [20] Z. Zhong, H.T. Qin, L. Liu, Y.B. Zhang, M.G. Shan, Silhouette-free image encryption using interference in the multiple-parameter fractional Fourier transform domain, *Opt. Express* 25 (6) (2017) 6974–6982.
- [21] D. Kong, X. Shen, Q. Xu, et al., Multiple-image encryption scheme based on cascaded fractional Fourier transform, *Appl. Opt.* 52 (12) (2013) 2619–2625.
- [22] M.R. Abuturab, Color image security system using double random-structured phase encoding in Gyrator transform domain, *Appl. Opt.* 51 (15) (2012) 3006–3016.
- [23] J.X. Chen, Z.L. Zhu, Z.J. Liu, et al., A novel double-image encryption scheme based on cross-image pixel scrambling in Gyrator domains, *Opt. Express* 22 (6) (2014) 7349–7361.

- [24] C.Q. Li, Y.S. Liu, L.Y. Zhang, et al., Cryptanalyzing a class of image encryption schemes based on Chinese remainder theorem, *Signal Process. Image Commun.* 29 (8) (2014) 914–920.
- [25] Z.J. Liu, A.A. Muhammad, S.T. Liu, A discrete fractional angular transform, *Opt. Commun.* 281 (6) (2008) 1424–1429.
- [26] Z.J. Liu, M. Gong, Y.K. Dou, et al., Double image encryption by using Arnold transform and discrete fractional angular transform, *Opt. Lasers Eng.* 50 (2) (2012) 248–255.
- [27] L.S. Sui, K.K. Duan, J.L. Liang, Double-image encryption based on discrete multiple-parameter fractional angular transform and two-coupled logistic maps, *Opt. Commun.* 343 (2015) 140–149.
- [28] N.R. Zhou, S.M. Pan, S. Cheng, Z.H. Zhou, Efficient image compression-encryption scheme based on hyper-chaotic system and 2D compressive sensing, *Opt. Laser Technol.* 82 (2016) 121–133.
- [29] W.Q. He, X. Peng, X.F. Meng, A hybrid strategy for cryptanalysis of optical encryption based on double-random phase-amplitude encoding, *Opt. Laser Technol.* 44 (5) (2012) 1203–1206.
- [30] X.G. Wang, D.M. Zhao, Double images encryption method with resistance against the specific attack based on an asymmetric algorithm, *Opt. Express* 20 (11) (2012) 11994–12003.
- [31] Y.L. Xiao, X. Zhou, S. Yuan, et al., Multiple-image parallel optical encryption, *Opt. Commun.* 283 (14) (2010) 2789–2793.
- [32] N.R. Zhou, Y.X. Wang, L.H. Gong, Novel optical image encryption scheme based on fractional Mellin transform, *Opt. Commun.* 284 (13) (2011) 3234–3242.
- [33] A. Orsdemir, H.O. Altun, G. Sharma, et al., On the security and robustness of encryption via compressed sensing, in: *Proceedings of IEEE Military Communications Conference, San Diego CA, 2008*, pp. 1040–1046.
- [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)*, IEEE Computer Society, 2011, pp. 105–108.
- [35] X.J. Tong, M. Zhang, Z. Wang, et al., A joint color image encryption and compression scheme based on hyper-chaotic system, *Nonlinear Dyn.* 84 (4) (2016) 2333–2356.