Optica Applicata, Vol. XLVII, No. 1, 2017
DOI: 10.5277/oa170113

Image encryption algorithm by using the logistic map and discrete fractional angular transform

JING YU[1], YUAN LI[2], XINWEN XIE[3], NANRUN ZHOU[3, 4*], ZHIHONG ZHOU[4]

[1] Department of Computer Science and Technology, Nanchang University,
Nanchang 330031, China

[2] Department of Electrical Engineering and Automation, Nanchang University,
Nanchang 330031, China

[3] Department of Electronic Information Engineering, Nanchang University,
Nanchang 330031, China

[4] Shanghai Key Laboratory of Integrate Administration Technologies for Information Security,
Shanghai Jiao Tong University, Shanghai 200240, China

*Corresponding author: nrzhou@ncu.edu.cn

A new image encryption scheme based on logistic map and discrete fractional angular transform has been proposed. In the proposed scheme, the original image is encrypted with the random sequence generated by the logistic map, and the encrypted image is subsequently processed by the discrete fractional angular transform, which produces the ciphertext after double encryptions. The parameters of the logistic map and the order of the discrete fractional angular transform serve as the main keys of the image encryption algorithm. Simulation results show that the proposed image encryption algorithm can effectively resist the attacks of statistical analysis, and has acceptable encryption effect and security.

Keywords: image encryption, logistic map, discrete fractional angular transform.

1. Introduction

Nowadays more and more digital data including interesting and meaningful images are distributed through Internet frequently. Therefore, the secure transmission of confidential or private image data over public channels has become a hot issue. Recently, with the development of chaos theory, chaos-based image encryption technologies have been gradually developing. In the pure digital image encryption, chaotic sequence and logistic operation can be utilized to construct an encryption scheme [1]. A new chaotic image encryption scheme was presented by changing the positions and the gray values of image pixels [2]. XINGYUAN WANG *et al.* proposed an image encryption algorithm by combining the cycle shift with the chaotic system [3]. Since the cat map [4, 5] is periodic and it can be easily cracked by the chosen plaintext attack, XINGYUAN WANG *et al.* also proposed a new block image encryption scheme to eliminate the cyclical phenomenon and resist the chosen plaintext attack [6]. GUODONG YE presented an image encryption algorithm with multi-generalized logistic maps [7]. AKHSHANI *et al.* introduced an image encryption scheme based on the logistic map [8]. Furthermore, some image encryption schemes with good encryption effects have been investigated [9–12]. A chaos-based image encryption algorithm using a hybrid genetic algorithm and a DNA sequence was discussed [13]. And some typical chaos-based image encryption algorithms were also proposed [14–18], and some of them were analyzed [17, 18].

Some random operations and transforms have been introduced into the design of the image encryption algorithm, such as the fractional Fourier transform (FrFT) [9, 16, 17, 19, 20], fractional Mellin transform [21, 22], gyrator transform [23, 24] and generalized Arnold transform [25], most of which are the generalization of the Fourier transform (FT) with additional parameters as private keys. Additionally, ZHENGJUN LIU *et al.* presented a new discrete fractional transform defined by two parameters (angle and fractional order) and all eigenvectors of the transform are obtained by an angle with recursion, which was named as the discrete fractional angular transform (DFAT) [26]. The discrete fractional transform can be defined with only two parameters, the fractional order α and the angle β. Unlike the discrete fractional Fourier transform (DFrFT) [27], this transform can generate its eigenvectors by simple recurrences and hence the computation speed can be greatly enhanced. The computational load of the kernel matrix of the DFAT is minimal among all the fractional order transforms. This characteristic has very important practical applications in the field of signal and image processing. It has been proved that the DFAT is faster than DFrFT and the discrete fractional random transform (DFRNT) [28] in calculations and keeps the symmetry for even and odd signals. ZHENGJUN LIU *et al.* also proposed a new double image encryption scheme based on Arnold's transform and discrete fractional angular transform, where two original images are regarded as the amplitude and the phase of a complex function [29]. LIANSHENG SUI *et al.* designed an image encryption based on the discrete fractional angular transform, which has high resistance against the potential attacks, such as the chosen plaintext attack [30]. In the paper, a new image encryption algorithm is designed by using the logistic map and discrete fractional angular transform to achieve better security.

The rest of this paper is arranged as follows. The fundamental knowledge of the logistic map and the discrete fractional angular transform is reviewed in Section 2. The proposed image encryption scheme by using the logistic map and discrete fractional angular transform is described in detail in Section 3. Simulations and discussions are provided in Section 4 and a brief conclusion is drawn in Section 5.

2. Fundamental knowledge

2.1. Discrete fractional angular transform

The discrete fractional angular transform (DFAT) is derived based on the discrete fractional Fourier transform (DFrFT) and the discrete fractional random transform (DFRNT), in which the eigenvectors have been redefined by a series of vectors generated from an initial angle with recurrence [26]. Mathematically, a discrete transform can be expressed by the matrix multiplications, *i.e.*, [26]

$$T = VDV^{\tau} \tag{1}$$

where V and D represent the eigenvector matrix and the eigenvalue matrix of the transform, respectively; V^{τ} denotes the transpose of the matrix V. Similarly, the kernel matrix $A_N^{\alpha,\beta}$ of DFAT can also be expressed as [26]

$$A_N^{\alpha,\beta} = V_N^{\beta} D_N^{\alpha} (V_N^{\beta})^{\tau} \tag{2}$$

where α and β denote the fractional order and the angle of the kernel matrix $A_N^{\alpha,\beta}$, respectively. In addition, the eigenvectors of DFAT are mainly changed by the angle β. The DFAT on a one-dimensional signal χ with N points is

$$X_{\alpha,\beta} = A_N^{\alpha,\beta}\chi \tag{3}$$

As for a two-dimensional signal γ of size $M \times N$, the DFAT can be defined as

$$Y_{\alpha,\beta} = A_M^{\alpha,\beta}\gamma A_N^{\alpha,\beta} \tag{4}$$

If V_N is an orthonormal matrix $(E = V_N V_N^{\tau})$, then the orthonormal matrices will be:

$$V_{2N} = \frac{1}{\sqrt{2}}\begin{bmatrix} V_N & V_N \\ -V_N^Z & V_N^Z \end{bmatrix} \tag{5}$$

$$V_{2N+1} = \frac{1}{\sqrt{2}}\begin{bmatrix} V_N & V_N & V_0^{\tau} \\ V_0 & V_0 & \sqrt{2} \\ -V_N^Z & V_N^Z & V_0^{\tau} \end{bmatrix} \tag{6}$$

where the matrix V_N^Z is obtained by flipping the matrix V_N in up-down direction, and V_0 is a $1 \times N$ zero vector. An orthonormal matrix can be served as the eigenvectors matrix of the discrete fractional random transform. Therefore, the matrices V_N and V_{2N}

(or V_{2N+1}) can be used to construct the eigenvectors matrix of the DFAT. By taking N as 2 or 3, the eigenvector matrices V_2^β or V_3^β will turn out to be:

$$V_2^\beta = \begin{bmatrix} \cos(\beta) & \sin(\beta) \\ -\sin(\beta) & \cos(\beta) \end{bmatrix} \tag{7}$$

$$V_3^\beta = \begin{bmatrix} \cos(\beta) & \sin(\beta) & 0 \\ 0 & 0 & 1 \\ -\sin(\beta) & \cos(\beta) & 0 \end{bmatrix} \tag{8}$$

where V_2^β and V_3^β are the orthonormal matrices. The construction of V_2^β and V_3^β is similar to V_{2N}^β and V_{2N+1}^β, respectively. For other cases, the eigenvector matrix V_N^β for $N > 3$ can be calculated with a recursion process. The column vectors of the orthonormal matrix V_N^β can be regarded as the eigenvectors of the transform. All elements of the matrix V_N^β can be collected into the set S_N

$$S_N = \left\{ \left(\frac{1}{\sqrt{2}} \right)^\mu \left[0,\ 1,\ \pm\sin(\beta),\ \pm\cos(\beta) \right] \right\} \tag{9}$$

where μ represents the number of recurrences. For $N = 2^n$, Eq. (9) will be

$$S_{2^n} = \left\{ \left(\frac{1}{\sqrt{2}} \right)^{n-1} \left[\pm\sin(\beta),\ \pm\cos(\beta) \right] \right\} \tag{10}$$

and S_{2^n} can be considered as a subset of S_N. Since the eigenvectors are obtained by a simple matrix with recurrence, the eigenvalues of the DFrFT and the DFRNT are similar to the eigenvalues λ_N^α of the DFAT

$$\lambda_N^\alpha = \left[1,\ \exp(-i2\pi\alpha),\ \exp(-i4\pi\alpha),\ ...,\ \exp(-i2(N-1)\pi\alpha) \right] \tag{11}$$

The diagonal matrix D_N^α is defined as

$$D_N^\alpha = \mathrm{diag}(\lambda_N^\alpha) \tag{12}$$

2.2. Logistic map

Logistic map, as a one-dimensional chaotic function, is defined as

$$f(\chi) = P\chi(1-\chi) \tag{13}$$

The logistic map is sometimes called an iterated map function, since it maps one value of χ in the range (0, 1) into another value in the same range if P is in the range [0, 4]. The iterative form of the logistic map is usually denoted as

$$\chi_{n+1} = P\chi_n(1-\chi_n) \tag{14}$$

where P is a system parameter between 0 and 4, χ_n is a map variable between 0 and 1, χ_0 is the initial value of the logistic map and n is the number of iterations used to generate the iterative values. Thus, given an initial value χ_0 and a parameter P, the sequence can be computed.

As P becomes greater than 3.5699456, this logistic map is in the chaotic state, and the sequence sensitive to the initial value χ_0 is non-periodical and non-convergent, which is suitable for image encryption.

3. Image encryption algorithm based on logistic map and DFAT

For a given original image of size $M \times N$, the proposed image encryption and decryption algorithm shown in Fig. 1 by combining the logistic map with the discrete fractional angular transform is described as follows.

1) By giving the parameter P and initial value χ_0 of the logistic map in Eq. (14), a random sequence $G = \{G_{ij} \mid i, j = 0, 1, 2, ..., N-1\}$ is generated. The resulting image could be obtained by XORing the original image with the random sequence generated by the logistic map.

2) The DFAT of fractional order α and angle β is performed on the transformed image according to Eqs. (9)–(11), that is to say, the transformed image will be converted by the discrete fractional angular transform $A_N^{\alpha,\beta}$, and we denote the resulting encrypted image with E.

In this algorithm, the parameter χ_0 of the logistic map, fractional order α and angle β of the DFAT can be used as the keys. The decryption process is depicted in Fig. 1, which is similar to the encrypted process with a reversed order. The inverse transform of the discrete fractional angular transform $A_N^{\alpha,\beta}$ can be obtained by taking a negative fractional order to generate the corresponding kernel matrix, *i.e.*, $A_N^{-\alpha,\beta}$.

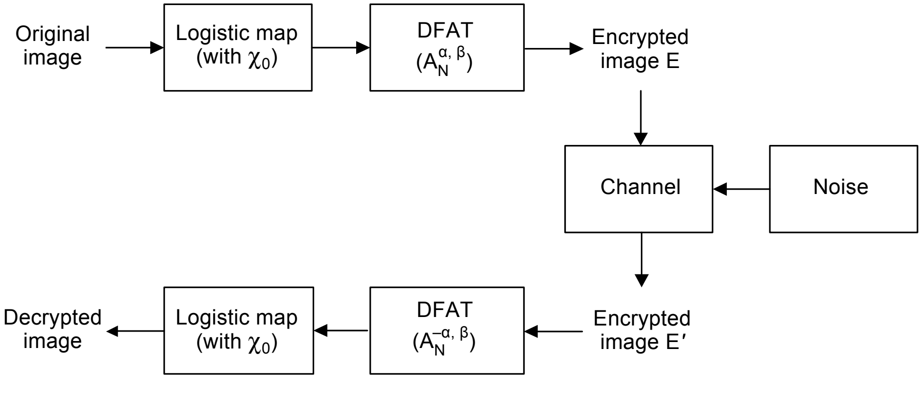
Original image
Logistic map (with χ_0)
DFAT ($A_N^{\alpha,\beta}$)
Encrypted image E
Channel
Noise
Encrypted image E′
DFAT ($A_N^{-\alpha,\beta}$)
Logistic map (with χ_0)
Decrypted image

Fig. 1. Encryption and decryption scheme.

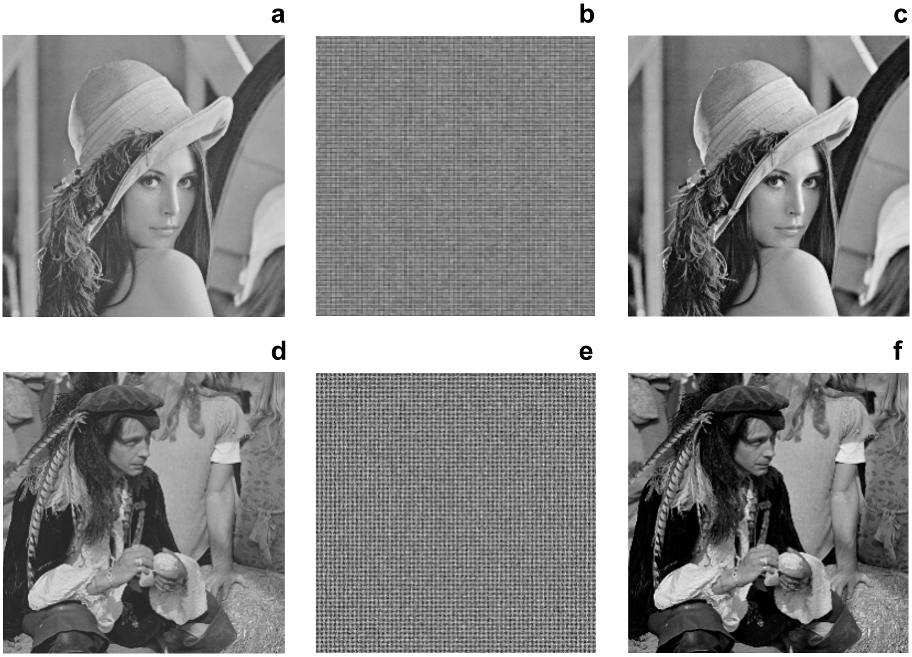

Fig. 2. Results of the test images: original (**a**), encrypted (**b**), and decrypted (**c**) image of *Lena*; original (**d**), encrypted (**e**), and decrypted (**f**) image of *Man*.

The inverse transform $A_N^{-\alpha,\,\beta}$ will be utilized to decrypt the ciphertext in this image encryption algorithm.

4. Simulation and discussion

To verify the feasibility and the effectiveness of the proposed image encryption scheme based on the logistic map and discrete fractional angular transform, simulations are performed with the plaintext image *Lena* shown in Fig. 2**a**. The initial value χ_0 of the logistic map is set as 0.2. As for the DFAT, the fractional order α and the angle β are taken as 0.1992 and 1.5, respectively. Figures 2**b** and 2**e** display the ciphertext images of *Lena* and *Man*, respectively. Figures 2**c** and 2**f** are the decrypted images of *Lena* and *Man* with correct keys, respectively, from which the differences between the plaintext image and the decrypted one cannot be distinguished.

4.1. Histogram

It is normal for us to analyze the performance of the image encryption scheme with the image histogram. As for a good image encryption scheme, the histograms of the encrypted images are fairly uniformed or similar in distribution. Figures 3**a** and 3**b** are the histograms of *Lena* and *Man*, respectively. Figures 3**c** and 3**d** show the histograms of the corresponding encrypted images. From Fig. 3, the histograms of the original

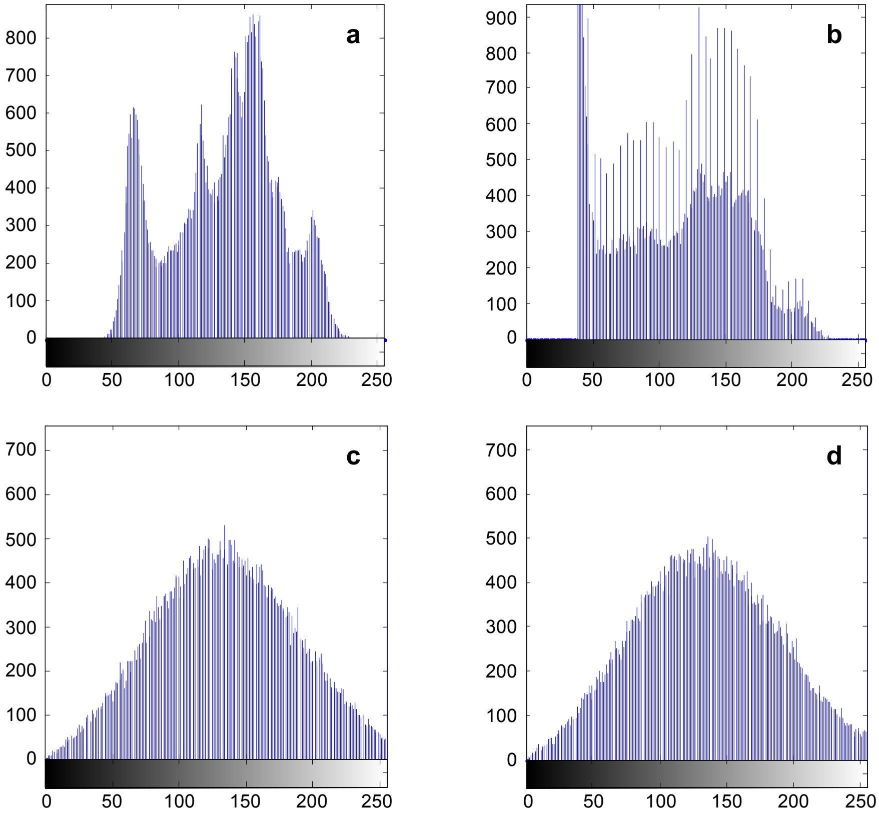

Fig. 3. Histograms: *Lena* (**a**), *Man* (**b**), encrypted image of *Lena* (**c**), and encrypted image of *Man* (**d**).

images are apparently different from each other, while the encrypted images exhibit similar statistical properties. The histograms of the encrypted image are subject to approximate normal distribution. Thus, it does not provide any useful information for the opponent to perform histogram attack on the image encryption algorithm.

4.2. Correlation analysis

Usually, the adjacent pixels in a natural, meaningful and practical image in the horizontal, vertical and diagonal directions may be tightly correlated. The correlation coefficient between adjacent pixels of any original image can be expressed as

$$C = \frac{\sum_{j=1}^{N}(x_j - \overline{x})(y_j - \overline{y})}{\sqrt{\sum_{j=1}^{N}(x_j - \overline{x})^2 \sum_{j=1}^{N}(y_j - \overline{y})^2}} \tag{15}$$

where $\overline{x} = \frac{1}{N}\sum_{j=1}^{N} x_j$ and $\overline{y} = \frac{1}{N}\sum_{j=1}^{N} y_j$.

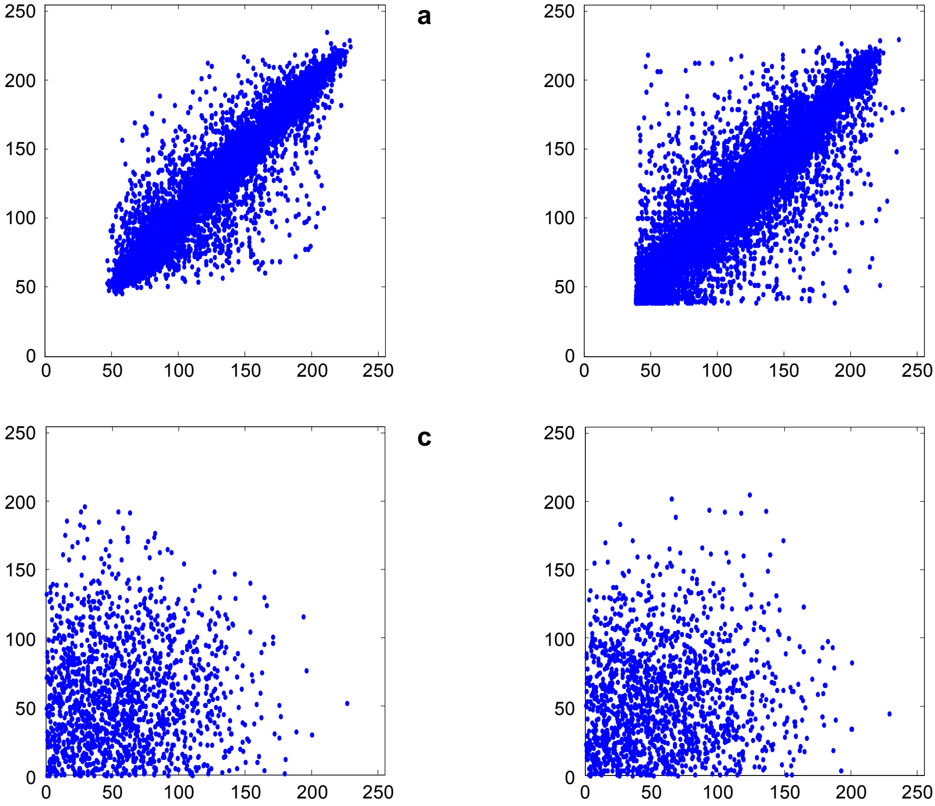

Fig. 4. Correlation distributions of two horizontally adjacent pixels in *Lena* (**a**), *Man* (**b**), encrypted image of *Lena* (**c**), and encrypted image of *Man* (**d**).

Figure 4 gives the correlation distribution between two horizontally adjacent pixels in the two original images and their corresponding encrypted images. The correlation coefficients are collected in the Table, which shows that the proposed image encryption algorithm has better performance from the aspect of correlation. In [26], ZHENGJUN

Table. Correlation coefficient of adjacent pixels.

Algorithm	Image	Horizontal direction	Vertical direction	Diagonal direction
	Lena	0.9543	0.9293	0.8981
Proposed algorithm	Encrypted *Lena*	0.1068	0.0766	0.0182
Reference [26]	Encrypted *Lena*	0.6661	0.6407	0.3452
	Man	0.9297	0.9139	0.8837
Proposed algorithm	Encrypted *Man*	0.1047	0.0876	–0.0113
Reference [26]	Encrypted *Man*	0.6920	0.6850	0.4361

Liu *et al.* mainly aimed to propose a new DFAT and did not combine it with other algorithms, thus the correlation coefficients are relatively high. The adjacent pixels of the original images in the horizontal, vertical and diagonal directions are tightly correlated and the correlation coefficients are all close to 0.9 in each direction. However, in the cipher images of the proposed algorithm, the correlation coefficients are smaller than those before encryption. Thus the image encryption scheme can reduce the correlation of the encrypted image greatly. This further confirms that our scheme has a strong ability to resist the statistical analysis attack.

4.3. Key sensitivity analysis

The following relative mean square error (RMSE) function is usually employed to express the difference between the decrypted images and the original ones quantitatively

$$\mathrm{RMSE} = \log \frac{\sum_{x=1}^{M} \sum_{y=1}^{N} \left[f(x, y) - \overline{f}(x, y) \right]^2}{M \times N} \tag{16}$$

where $f(x, y)$ and $\overline{f}(x, y)$ mean the pixel values of the original image and the decrypted one, respectively; $M \times N$ denotes the image size.

The sensitivity also can be tested by observing the changes of the decryption images with the correct keys changing slightly. Figures 5**a** and 5**b** are the MSE of the initial value of the logistic map and the RMSE of the DFAT order, respectively. From the decryption results, the order α is more sensitive than the angle β. Therefore, it is not necessary to discuss the angle β since the security contribution of the angle β is relatively little and neglectable. The correct decrypted images are shown in Figs. 6**b** and 6**f**.

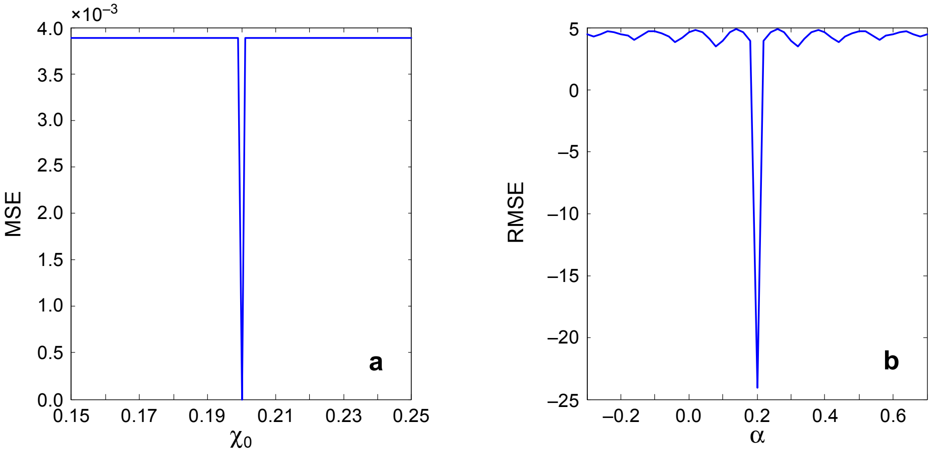

Fig. 5. MSE curves. RMSE of χ_0 (**a**), and RMSE of α (**b**).

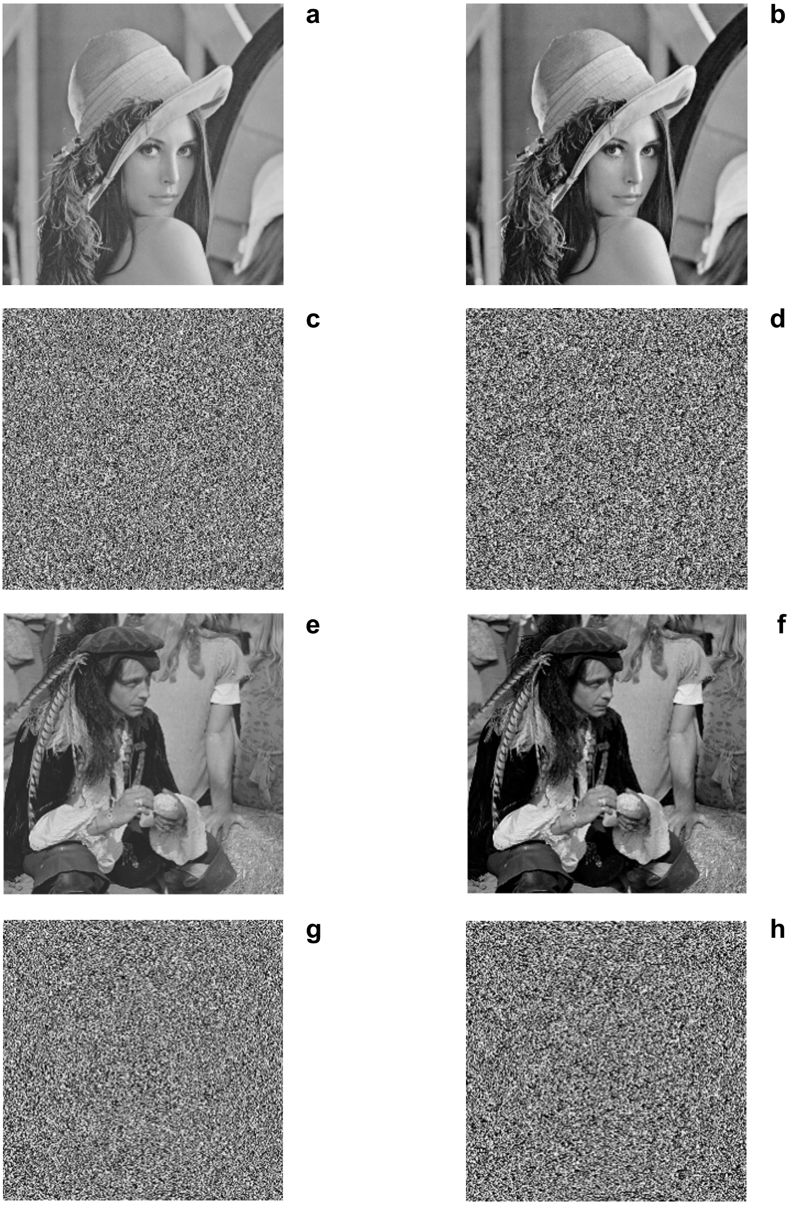

Fig. 6. The decrypted images of *Lena* and *Man*. The original image of *Lena* (**a**), the decrypted image of *Lena* with right keys (**b**), the decrypted image of *Lena* with wrong χ_0 (**c**), the decrypted image of *Lena* with wrong α (**d**), the original image of *Man* (**e**), the decrypted image of *Man* with right keys (**f**), the decrypted image of *Man* with wrong χ_0 (**g**), and the decrypted image of *Man* with wrong α (**h**).

Figures 6**c** and 6**g** denote the decrypted images of *Lena* and *Man* with incorrect χ_0, respectively. Figures 6**d** and 6**h** show the decrypted images of *Lena* and *Man* with the wrong order of the DFAT, respectively.

Apparently, the decrypted images with wrong keys are unable to provide any meaningful information of the original images. The details of the original images become blurred when the decryption key deviates from the encryption one and the variation of the decrypted images is invisible visually if a slight deviation occurs to the main keys. Therefore, the proposed image encryption algorithm is of high security.

4.4. Key space analysis

In cryptography, the key space of an encryption algorithm is one of the most important factors to measure the strength of the encryption algorithm. In fact, the key space is the set of all possible available keys. In our proposed image encryption scheme, the main keys are the order α of the discrete fractional angular transform and the initial value χ_0 of the logistic map. Suppose their corresponding key space are S_1 and S_2, respectively. The key space for key K_i can be calculated with $[\xi_i]_{i=1}^{N}$ and $[\eta_i]_{i=1}^{N}$ generated by two different initial values K_i and $K_i + \delta$, and the mean absolute error (MAE) is

$$\mathrm{MAE} = \frac{1}{N}\sum|\xi - \eta| \tag{17}$$

Generally, the key space for K_i is considered as δ_0^{-1}, where δ_0 is the exact value of δ satisfying MAE = 0. The simulation results in Fig. 5 show that the key space S_1 of α is around 10^{14}. Similarly, $S_2 = 133$. Since these keys are independent of each other, the total key space of the proposed image encryption scheme is

$$S = \prod_{i=1}^{2} S_i = 133 \times 10^{14} \tag{18}$$

4.5. Robustness analysis

The quality of the encrypted image is inextricably associated with the noises during processing and transmission, compression or the interference from the malicious hacker or attacker. Noise, compression artifact or interference may reduce the quality of the decrypted images in an apparently non-ignorable way. Therefore, to balance the security and the robustness of the proposed image encryption algorithm, it is advisable for the image encryption scheme to counteract a slight noise attack. Suppose C and $C' = C + kG$ are the genuine encrypted image and the noisy or interfered encrypted one, respectively, k is a coefficient indicating the noise or interference intensity, and G represents the white Gaussian noise with zero-mean and unit standard deviation. In the case that the Gaussian noises with different intensities are added to the encrypted image, different decrypted images are shown in Fig. 7. Figure 7 shows the decrypted images of *Lena* and *Man* with noise intensity coefficients 1, 5, 15 and 20, respectively. From Fig. 7, although the basic features of the decrypted images are still recognizable, the qualities of the decrypted images under different noise intensity coefficients turn out to be worse and worse.

To testify the robustness of the proposed image encryption scheme, the encrypted images are cut off in a random rectangle position, and the correct keys are used to decrypt

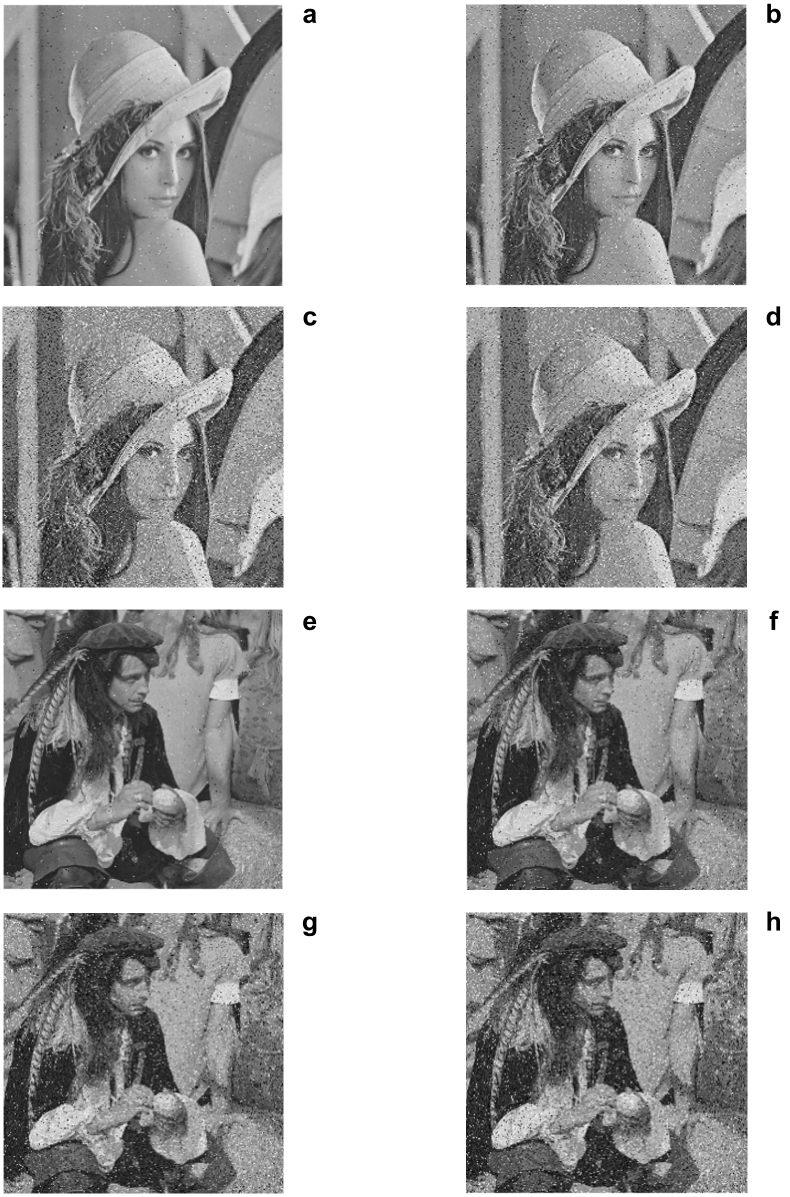

Fig. 7. Results of anti-noise. Decrypted image of *Lena* with $k = 1$ (**a**), $k = 5$ (**b**), $k = 15$ (**c**), and $k = 20$ (**d**). Decrypted image of *Man* with $k = 1$ (**e**), $k = 5$ (**f**), $k = 15$ (**g**), and $k = 20$ (**h**).

the cropped encrypted images, as shown in Fig. 8. Figures 8**a**, 8**c** and 8**e** give the cropped ciphertext, while Fig. 8**b** is the corresponding decrypted image of Fig. 8**a**. The corresponding decrypted image of Fig. 8**c** is shown in Fig. 8**d**, and Fig. 8**f** is the corresponding decrypted result of Fig. 8**e**. It is shown that the information of the original images is almost completely diffused during the encryption process and the quality of the de-

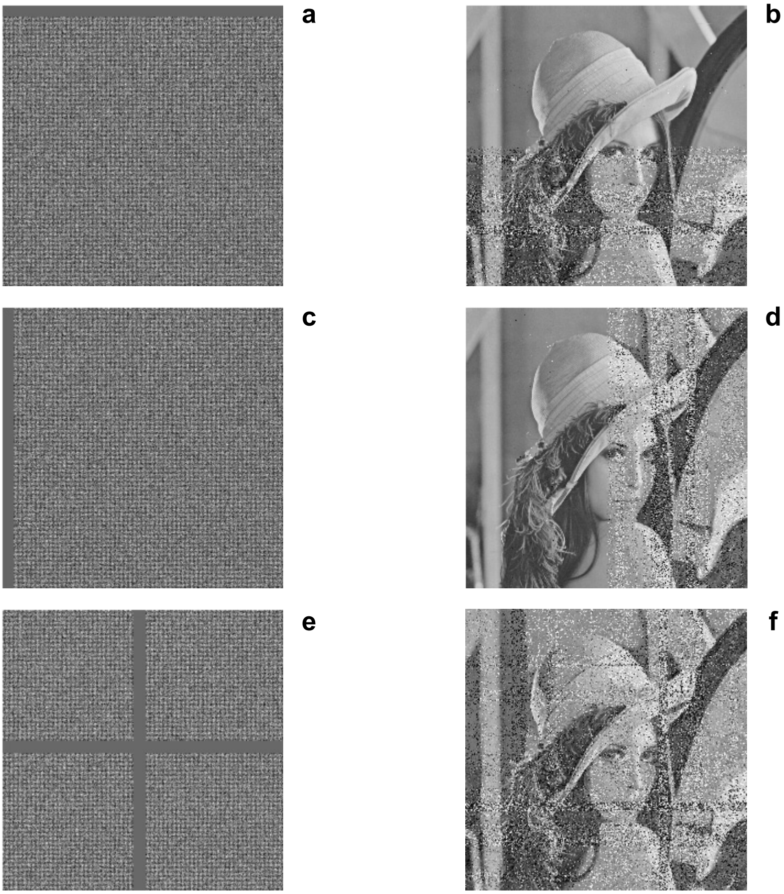

Fig. 8. Robustness against data loss: 4% data loss on the top (**a**), the corresponding decrypted image of **a** (**b**), 4% data loss on the left (**c**), the corresponding decrypted image of **c** (**d**), 8% data loss in the middle (**e**), and the corresponding decrypted image of **e** (**f**).

crypted images is still acceptable even if a relatively small part of the ciphertext is lost, which illustrates the fact that the proposed image encryption scheme can resist the shearing attack in a sense.

5. Conclusion

An improved efficient image encryption scheme by combining the logistic map with the discrete fractional angular transform is designed. A logistic map permutation process is used to disorder the plaintext image, and the plaintext image fails to be recovered unless all the keys including the initial values of chaos and the parameters of DFAT are known exactly. The proposed image encryption scheme has high resistance against the potential attacks. The parameter defining the logistic map and the angle of the discrete fractional angular transform can be served as the additional keys to enhance the security of the proposed image encryption scheme. Numerical simulations demonstrate that the performance of the proposed image encryption algorithm is acceptable.

Acknowledgments – This work is supported by the National Natural Science Foundation of China (Grant Nos. 61262084 and 61462061), the Major Academic Discipline and Technical Leader of Jiangxi Province (Grant No. 20162BCB22011) and the Opening Project of Shanghai Key Laboratory of Integrated Administration Technologies for Information Security (Grant No. AGK201602).

References

[1] PAREEK N.K., PATIDAR V., SUD K.K., *Image encryption using chaotic logistic map*, Image and Vision Computing **24**(9), 2006, pp. 926–934.

[2] ZHI-HONG GUAN, FANGJUN HUANG, WENJIE GUAN, *Chaos-based image encryption algorithm*, Physics Letters A **346**(1–3), 2005, pp. 153–157.

[3] XINGYUAN WANG, SHENGXIAN GU, YINGQIAN ZHANG, *Novel image encryption algorithm based on cycle shift and chaotic system*, Optics and Lasers in Engineering **68**, 2015, pp. 126–134.

[4] GUODONG YE, KWOK-WO WONG, *An efficient image encryption algorithm based on a generalized Arnold map*, Nonlinear Dynamics **69**(4), 2012, pp. 2079–2087.

[5] YIFAN LIU, XIAOHONG WU, YANMEI YU, DAISHENG LUO, *Image encryption based on Arnold cat map and ECC*, Journal of Sichuan University **49**(4), 2012, pp. 834–838.

[6] XINGYUAN WANG, LINTAO LIU, YINGQIAN ZHANG, *A novel chaotic block image encryption algorithm based on dynamic random growth technique*, Optics and Lasers in Engineering **66**, 2015, pp. 10–18.

[7] GUODONG YE, *Chaotic image encryption algorithm using multi-generalized logistic maps*, Journal of Computational and Theoretical Nanoscience **10**(11), 2013, pp. 2789–2795.

[8] AKHSHANI A., AKHAVAN A., LIM S.-C., HASSAN Z., *An image encryption scheme based on quantum logistic map*, Communications in Nonlinear Science and Numerical Simulation **17**(12), 2012, pp. 4653–4661.

[9] HONGJUN LIU, XINGYUAN WANG, *Color image encryption based on one-time keys and robust chaotic maps*, Computers and Mathematics with Applications **59**(10), 2010, pp. 3320–3327.

[10] HUIJUAN LI, *Image encryption based on gyrator transform and two-step phase-shifting interferometry*, Optics and Lasers in Engineering **47**(1), 2009, pp. 45–50.

[11] XINGYUAN WANG, DAPENG LUAN, *A novel image encryption algorithm using chaos and reversible cellular automata*, Communications in Nonlinear Science and Numerical Simulation **18**(11), 2013, pp. 3075–3085.

[12] TALARPOSHTI K.M., JAMEI M.K., *A secure image encryption method based on dynamic harmony search (DHS) combined with chaotic map*, Optics and Lasers in Engineering **81**, 2016, pp. 21–34.

[13] ENAYATIFAR R., ABDULLAH A.H., ISNIN I.F., *Chaos-based image encryption using a hybrid genetic algorithm and a DNA sequence*, Optics and Lasers in Engineering **56**, 2014, pp. 83–93.

[14] LU XU, ZHI LI, JIAN LI, WEI HUA, *A novel bit-level image encryption algorithm based on chaotic maps*, Optics and Lasers in Engineering **78**, 2016, pp. 17–25.

[15] XUAN LI, GUOJI ZHANG, XIAYAN ZHANG, *Image encryption algorithm with compound chaotic maps*, Journal of Ambient Intelligence and Humanized Computing **6**(5), 2015, pp. 563–570.

[16] QIWEN RAN, LIN YUAN, TIEYU ZHAO, *Image encryption based on nonseparable fractional Fourier transform and chaotic map*, Optics Communications **348**, 2015, pp. 43–49.

[17] YANBIN LI, FENG ZHANG, YUANCHAO LI, RAN TAO, *Asymmetric multiple-image encryption based on the cascaded fractional Fourier transform*, Optics and Lasers in Engineering **72**, 2015, pp. 18–25.

[18] HONGJUN LIU, KADIR A., YANGLING LI, *Asymmetric color pathological image encryption scheme based on complex hyper chaotic system*, Optik – International Journal for Light and Electron Optics **127**(15), 2016, pp. 5812–5819.

[19] Xingbin Liu, Wenbo Mei, Huiqian Du, *Optical image encryption based on compressive sensing and chaos in the fractional Fourier domain*, Journal of Modern Optics **61**(19), 2014, pp. 1570–1577.

[20] Lima J.B., Novaes L.F.G., *Image encryption based on the fractional Fourier transform over finite fields*, Signal Processing **94**, 2014, pp. 521–530.

[21] Nanrun Zhou, Xingbin Liu, Ye Zhang, Yixian Yang, *Image encryption scheme based on fractional Mellin transform and phase retrieval technique in fractional Fourier domain*, Optics and Laser Technology **47**, 2013, pp. 341–346.

[22] Nanrun Zhou, Haolin Li, Di Wang, Shumin Pan, Zhihong Zhou, *Image compression and encryption scheme based on 2D compressive sensing and fractional Mellin transform*, Optics Communications **343**, 2015, pp. 10–21.

[23] Zhengjun Liu, Lie Xu, Chuang Lin, Jingmin Dai, Shutian Liu, *Image encryption scheme by using iterative random phase encoding in gyrator transform domains*, Optics and Lasers in Engineering **49**(4), 2011, pp. 542–546.

[24] Liansheng Sui, Benqing Liu, Qiang Wang, Ye Li, Junli Liang, *Color image encryption by using Yang-Gu mixture amplitude-phase retrieval algorithm in gyrator transform domain and two-dimensional Sine logistic modulation map*, Optics and Lasers in Engineering **75**, 2015, pp. 17–26.

[25] Nanrun Zhou, Tianxiang Hua, Lihua Gong, Dongju Pei, Qinghong Liao, *Quantum image encryption based on generalized Arnold transform and double random-phase encoding*, Quantum Information Processing **14**(4), 2015, pp. 1193–1213.

[26] Zhengjun Liu, Ahmad M.A., Shutian Liu, *A discrete fractional angular transform*, Optics Communications **281**(6), 2008, pp. 1424–1429.

[27] Jun Lang, Ran Tao, Yue Wang, *Image encryption based on the multiple-parameter discrete fractional Fourier transform and chaos function*, Optics Communications **283**(10), 2010, pp. 2092–2096.

[28] Liansheng Sui, Kuaikuai Duan, Junli Liang, Xinhong Hei, *Asymmetric double-image encryption based on cascaded discrete fractional random transform and logistic maps*, Optics Express **22**(9), 2014, pp. 10605–10621.

[29] Zhengjun Liu, Min Gong, Yongkang Dou, Feng Liu, Shen Lin, Ahmad M.A., Jingmin Dai, Shutian Liu, *Double image encryption by using Arnold transform and discrete fractional angular transform*, Optics and Lasers in Engineering **50**(2), 2012, pp. 248–255.

[30] Liansheng Sui, Kuaikuai Duan, Junli Liang, *Double-image encryption based on discrete multiple -parameter fractional angular transform and two-coupled logistic maps*, Optics Communications **343**, 2015, pp. 140–149.

Received May 29, 2016
in revised form July 23, 2016