Optica Applicata, Vol. XLVIII, No. 2, 2018
DOI: 10.5277/oa180206

Image encryption combining discrete fractional angular transform with Arnold transform in image bit planes

Zhihong Zhou[1], Jing Yu[2], Qinghong Liao[2], Lihua Gong[2, 3*]

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

[2]School of Information Engineering, Nanchang University, Nanchang 330031, China

[3]Department of Electrical and Computer Engineering, University of Pittsburgh, Pittsburgh, 15261, USA

[*]Corresponding author: lhgong@ncu.edu.cn

A new image encryption algorithm by using a discrete fractional angular transform and Arnold transform in image bit planes is investigated. In the image encryption algorithm, the original image is encrypted by the Arnold transform in image bit planes firstly, and then the resulting image is encrypted by the discrete fractional angular transform further. The key of the image encryption algorithm includes the parameters of the Arnold transform and the order of the discrete fractional angular transform. It is shown that the proposed image encryption algorithm is of high security and strong enough to counteract some conventional image attack manners.

Keywords: Arnold transform, bit plane, discrete fractional angular transform, image encryption algorithm.

1. Introduction

For different purposes, various image encryption algorithms have been investigated frequently [1–5]. By making full use of the unique property of XOR operation, the chaos-based symmetric image encryption scheme employing a bit-level permutation could be cracked by chosen plaintext attacks [1]. To overcome the weaknesses of most image encryption algorithms based on low-dimensional chaos systems and reduce the possible transmission burden, an efficient image compression–encryption scheme based on hyper-chaotic system and 2D compressive sensing was proposed [2]. A new quantum image encryption scheme with generalized affine transform and logistic map has been designed, where the gray information and the position information of the quantum image are changed simultaneously in the encryption process [3]. The Arnold transform (AT) has been also regarded as a powerful tool in the field of image processing [4]. Based on the Arnold transform, a holistic approach for off-line handwritten cursive word recognition with a directional feature has been investigated [5].

In the long run, as we know, digital image encryption will be the main approach to guaranteeing security of images during the image transfer over the public network. Since the chaotic system is sensitive to the initial values, it has been regarded as one of the promising image encryption tools. A large number of chaotic systems have been studied by researchers in recent years [6–8]. Moreover, a dozen of image encryption algorithms have been developed based on chaotic systems. A new image scheme based on the spatiotemporal chaos of the mixed linear–nonlinear coupled map lattices has been proposed [9]. A novel image encryption scheme built by combining DNA permutation with Lorenz system is investigated, where the correlation between DNA computing and diffusion part was enhanced [10]. And a secure image encryption method based on dynamic harmony search (DHS) combined with the chaotic map has also been discussed [11]. The security of image encryption algorithms is of great significance. The combination of a pseudo-random mask and pixel mapping could improve the effect of chaotic image encryption; however, the encryption process is much too complicated [12]. To simplify the encryption process, an optical image encryption by using diffractive imaging with special constraint in the input plane has been presented [13].

As a powerful tool, a discrete fractional Fourier transform (DFrFT) could be viewed as an approximate of the continuous fractional Fourier transform (FrFT) [14, 15]. On the other hand, as expansions of the FrFT, the multiple-parameter discrete fractional Fourier transform (MPDFrFT) [16], and the discrete fractional random transform (DFrRT) [17] have been employed widely. An image encryption scheme combining the fractional Fourier transform with the jigsaw transform in image bit planes has been discussed [18]. Additionally, the discrete fractional angular transform (DFAT), another expansion of the FrFT, has been introduced into image encryption for its excellent properties, such as linearity, multiplicity, index additivity, Parseval energy conservation, and so on [19–22]. To further enhance the efficiency of the image encryption algorithm based on DFAT with no degradation of the security performance, we propose a partial image encryption algorithm by combining the discrete fractional angular transform with the Arnold transform.

The style of this paper is organized as follows. The preliminary knowledge including the Arnold transform, the bit planes transform and the discrete fractional angular transform is reviewed in Section 2. The proposed image encryption scheme by using the discrete fractional angular transform and the Arnold transform in image bit planes is described in detail in Section 3. Simulation results and analyses are provided in Section 4 and a brief conclusion is drawn in Section 5.

2. Preliminaries

2.1. Arnold transform

DYSON *et al*. quoted the Arnold transform [23] as an image scrambling method [24], *i.e.*,

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & t \\ m & tm+1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \bmod(N) \tag{1}$$

where (x', y') and (x, y) are the new and the original pixel positions, respectively; $x, y, x', y' \in \{0, 1, ..., N-1\}$, t and m are positive integers, N is the size of the square image. The iteration number n is used as one of the keys during the decryption. The inverse Arnold transform is:

$$\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} tm+1 & -t \\ -m & 1 \end{bmatrix} \begin{bmatrix} x' \\ y' \end{bmatrix} \bmod N \tag{2}$$

The inverse Arnold transform is used to reverse the operation of forward scrambling and bring back the pixel coefficients to their original locations. The generalized Arnold transform in the coordinate form can be expressed as:

$$\begin{cases} x' = (x + ty) \bmod (N) \\ y' = \left[mx + (tm+1)y \right] \bmod N \end{cases} \tag{3}$$

2.2. Bit planes transform

Because pixel values in a grayscale image are decimal numbers between 0 and 255, each pixel can be represented by an 8-bit binary sequence. Thus, we can obtain eight bit planes if we decompose the image with a gray value between 0 and 255. These eight bit planes can be represented by ($k = 1, 2, ..., 8$)

$$O^k(m, n) = \begin{cases} 1, & \left[O^k(m, n)/2^k \right] \bmod 2 = 1 \\ 0, & \text{else} \end{cases} \tag{4}$$

where $O^k(m, n)$ denoted the pixel at m row and n column.

The bit planes transform deployed in this paper could divide the original image into eight bit planes. The bit planes transform also plays the role in integrating eight bit planes into one integral image. The original image and the corresponding eight bit planes produced by bit planes transform are shown in Fig. 1.

2.3. Discrete fractional angular transform

The kernel matrix $\mathbf{A}_N^{\alpha,\beta}$ of the discrete fractional angular transform (DFAT) was defined as [19]:

$$\mathbf{A}_N^{\alpha,\beta} = \mathbf{V}_N^{\beta} \mathbf{D}_N^{\alpha} (\mathbf{V}_N^{\beta})^{\tau} \tag{5}$$

where α denotes the fractional order and the main variable β of matrix $\mathbf{A}_N^{\alpha,\beta}$ represents the angle. The DFAT on a 2D image signal $\boldsymbol{\gamma}$ of size $M \times N$ can be given as:

$$\mathbf{Y}_{\alpha,\beta} = \mathbf{A}_M^{\alpha,\beta} \boldsymbol{\gamma} \mathbf{A}_N^{\alpha,\beta} \tag{6}$$

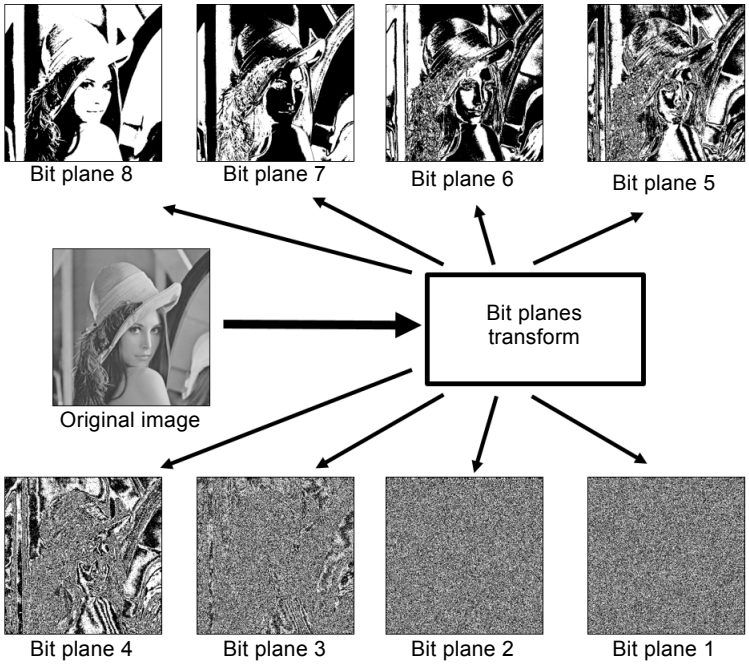

Fig. 1. Flowchart of bit planes transform.

The diagonal matrix $\mathbf{D}_N^{\alpha}$ is defined as:

$$\mathbf{D}_N^{\alpha} = \mathrm{diag}(\lambda_N^{\alpha}) \tag{7}$$

where the eigenvalue λ_N^{α} of the DFAT could be obtained by a simple matrix with recurrence

$$\lambda_N^{\alpha} = \left[1, \exp(-i2\pi\alpha), \exp(-i4\pi\alpha), \ldots, \exp(-i2(N-1)\pi\alpha)\right] \tag{8}$$

3. Image encryption and decryption algorithm

As illustrated in Fig. 2, the proposed image encryption and decryption algorithm is based on the discrete fractional angular transform and the Arnold transform in image bit planes. The image encryption algorithm includes the following steps.

1. The original image is decomposed into eight bit planes by the bit planes transform.
2. With the given parameters t and m of the Arnold transform and the iteration number n, the higher four bit planes are scrambled by the Arnold transform.
3. The lower four bit planes and the scrambled higher four bit planes are combined together.
4. With given fractional order α and angle β, $\mathbf{A}_N^{\alpha,\beta}$ could be determined. The combined image in step 3 is converted by the discrete fractional angular transform to yield the encryption image E.

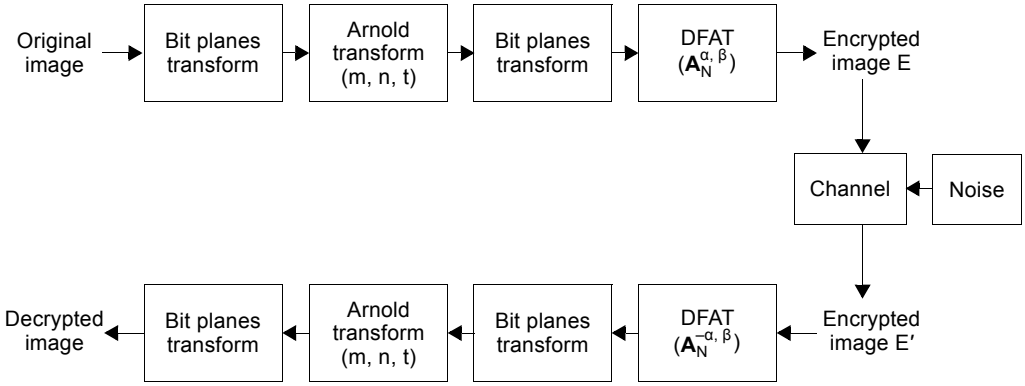

Fig. 2. Image encryption and decryption algorithm.

Parameters n, t and m of the Arnold transform, fractional order α and angle β of the DFAT are the keys of the image encryption algorithm. The decryption process depicted in Fig. 2 is similar to the encryption process with a reversed order.

4. Simulation results and performance analysis

The proposed image encryption algorithm based on the discrete fractional angular transform and the Arnold transform in image bit planes scheme is carried out in Matlab R2012a (v7.14.0.739). The original test images *Lena* and *Pepper* are shown in Figs. 3**a** and 3**d**, respectively. The initial parameters n, t, and m of the Arnold transform are taken

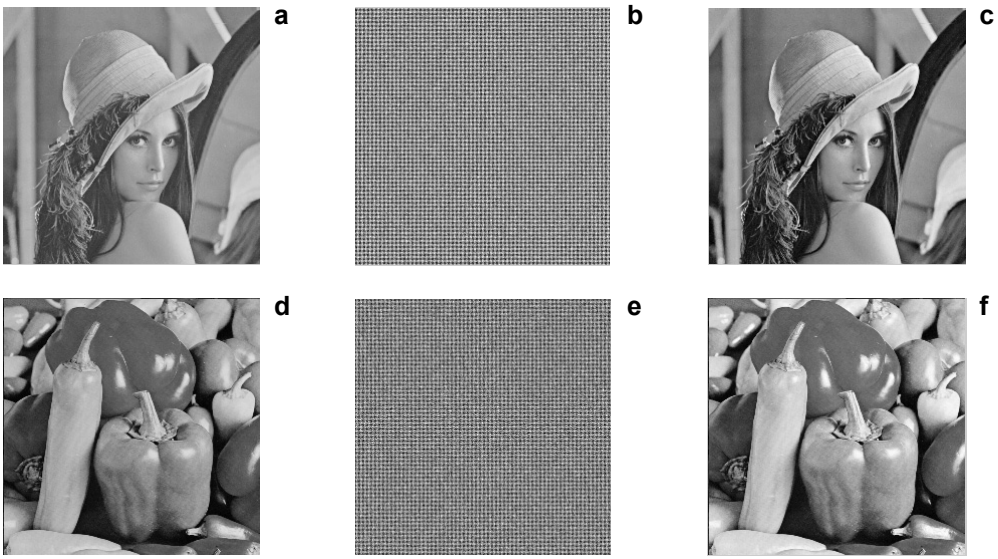

Fig. 3. Results of test images. *Lena*: original (**a**), encrypted (**b**), and decrypted (**c**). *Pepper*: original (**d**), encrypted (**e**), and decrypted (**f**).

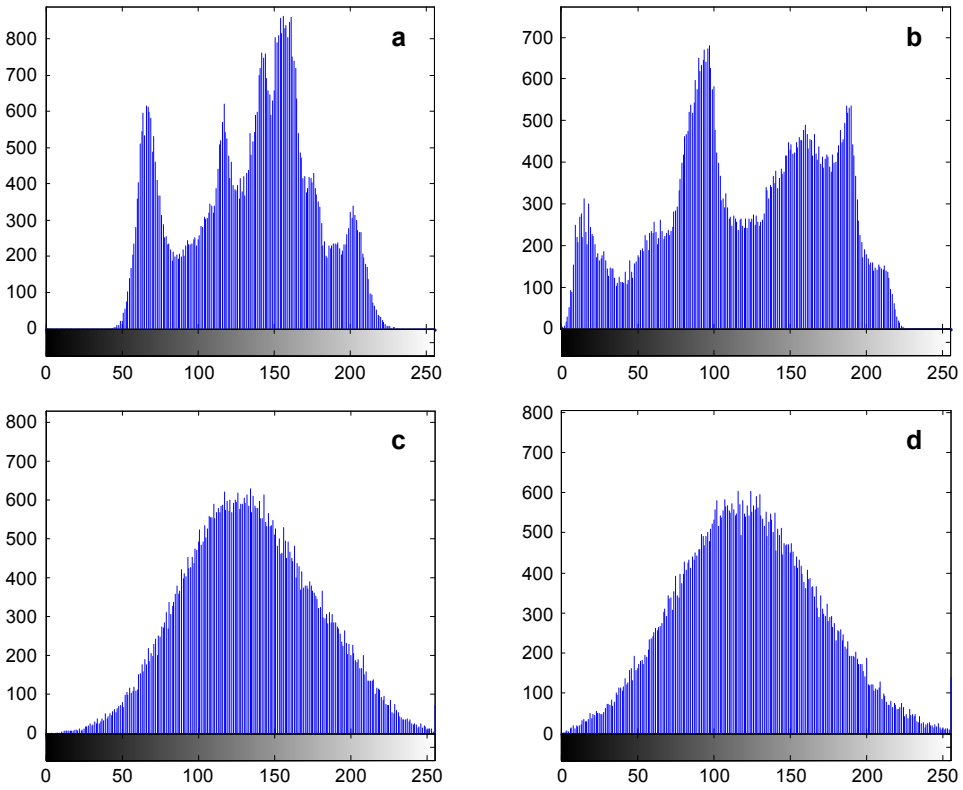

Fig. 4. Histograms: *Lena* (**a**), *Pepper* (**b**), encrypted *Lena* (**c**), and encrypted *Pepper* (**d**).

as 5, 2, and 3, respectively. The fractional order α and the angle β of the DFAT are set as 0.2 and 1.9, respectively. Figures 3**b** and 3**e** display the ciphertext images *Lena* and *Pepper*, respectively. Figures 3**c** and 3**f** are the correctly decrypted *Lena* and *Pepper*, respectively.

4.1. Statistic analysis

Figures 4**a** and 4**b** are the histograms of *Lena* and *Pepper*, respectively. Figures 4**c** and 4**d** show the histograms of their corresponding encrypted images. As is shown in Fig. 4, the shape of the histograms obtained for different test images are similar, even if the histograms of the original test images are apparently different from each other. Thus, histograms do not provide any useful information for the opponent to break the image encryption algorithm.

In order to evaluate the uniformity of the encrypted images, the variance of histogram is introduced. It can be calculated as

$$\mathrm{Var}(Z) = \frac{1}{N^2}\sum_{i=1}^{N}\sum_{j=1}^{N}\frac{1}{2}(z_i - z_j)^2 \tag{9}$$

T a b l e 1. The variances of original and encrypted images.

Image	Variance of original images	Variance of encrypted images
Lena	9.6869×10^5	3.3578×10^6
Woman	1.5387×10^6	3.3730×10^6
Peppers	4.8134×10^5	3.8443×10^6
Man	1.2013×10^6	3.8821×10^6

a

b

Fig. 5. Original *Man* (**a**), and original *Woman* (**b**).

where Z denotes the vector of the histogram values and $Z = \{z_1, z_2, ..., z_{256}\}$; z_i represents the number of pixels whose pixel value is equal to i [25]. According to Eq. (9), the variance of this histogram is inversely proportional to the uniformity of the image. The variance of the original images and cipher images are piled in Table 1 (original *Man* and *Woman* are shown in Fig. 5). It can be shown that the original images are more uniform than the ciphered images. And the ciphered images' variances are similar to each other, while the original images' variances are different from each other. This indicates that it is hard for an adversary to judge the correlation between the original image and the corresponding ciphered image.

Figure 6 gives the correlation distributions between two horizontally adjacent pixels in the two original test images and their corresponding encrypted images. The correlation coefficients are compiled in Table 2. It is seen that the adjacent pixels of the original test images are tightly correlated in the horizontal, vertical and diagonal directions and the correlation coefficients are all close to 1. The correlation coefficients of the ciphered

T a b l e 2. Correlation coefficient of adjacent pixels.

	Image	H direction	V direction	D direction
–	*Lena*	0.9543	0.9293	0.8981
Proposed algorithm	Encrypted *Lena*	0.0358	0.0629	−0.0046
Algorithm from [19]	Encrypted *Lena*	0.6699	0.6417	0.3537
–	*Pepper*	0.9297	0.9139	0.8837
Proposed algorithm	Encrypted *Pepper*	0.0214	0.0796	−0.0132
Algorithm from [19]	Encrypted *Pepper*	0.7213	0.7160	0.4501

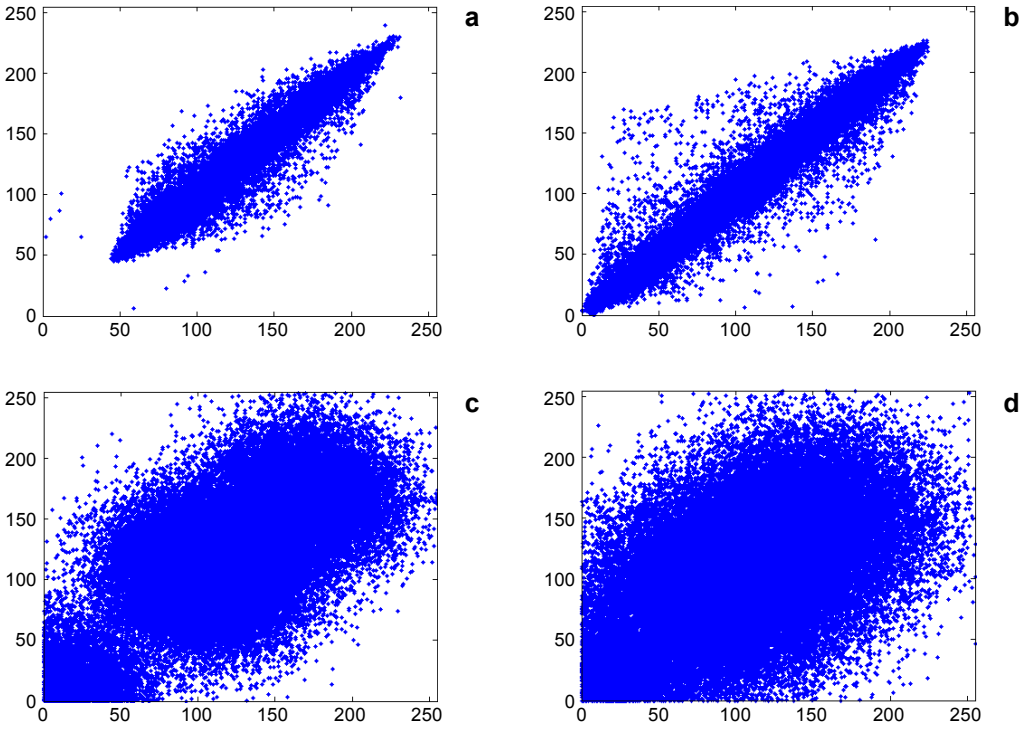

Fig. 6. Correlation distributions of two horizontally adjacent pixels in *Lena* (**a**), *Pepper* (**b**), encrypted *Lena* (**c**), and encrypted *Pepper* (**d**).

images by the proposed image encryption algorithm are smaller than those of the original test images and the images by the algorithm in [19]. Therefore, the proposed image encryption scheme could reduce the correlation of the original images greatly. It further confirms that our scheme has a strong ability to resist the statistical analysis attack.

4.2. Key sensitivity analysis

The sensitivity can be evaluated by observing the changes of the decryption images when the correct keys change slightly. Figures 7**a** and 7**b** show the relative mean square error (RMSE) *versus* the iteration number of the Arnold transform and the MSE of the DFAT order, respectively. Angle β is not discussed here since its contribution to security is relatively little and neglectable; n is more sensitive than t and m to the Arnold transform in that t and m have certain correlation.

It is time-consuming to examine the sensitivity of secret keys by enumerating all possible combinations of secret keys. Images *Lena* and *Pepper* are employed to test the key sensitivity by randomly changing the secret key a little bit. Figures 8**b** and 8**f** are the correct decrypted images. Figures 8**c** and 8**g** show the decrypted images *Lena* and *Pepper* with incorrect n, respectively. Figures 8**d** and 8**h** exhibit the decrypted images *Lena* and *Pepper* with the wrong order of the DFAT, respectively.

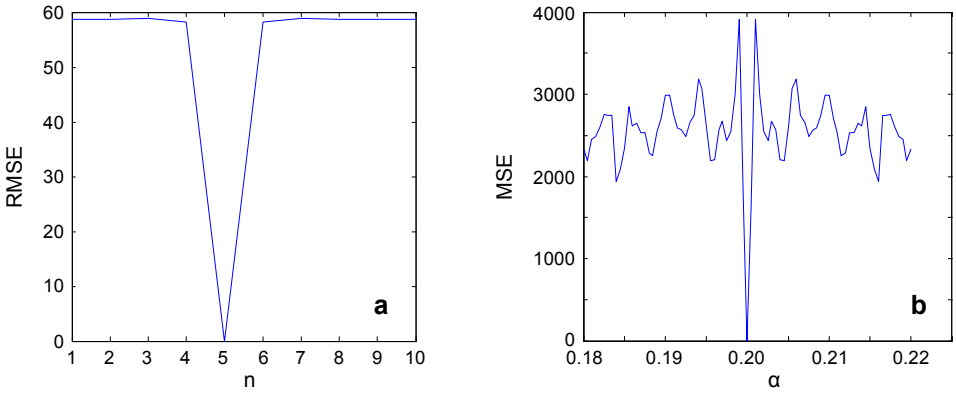

Fig. 7. RMSE *versus* n (**a**), and MSE *versus* α (**b**).

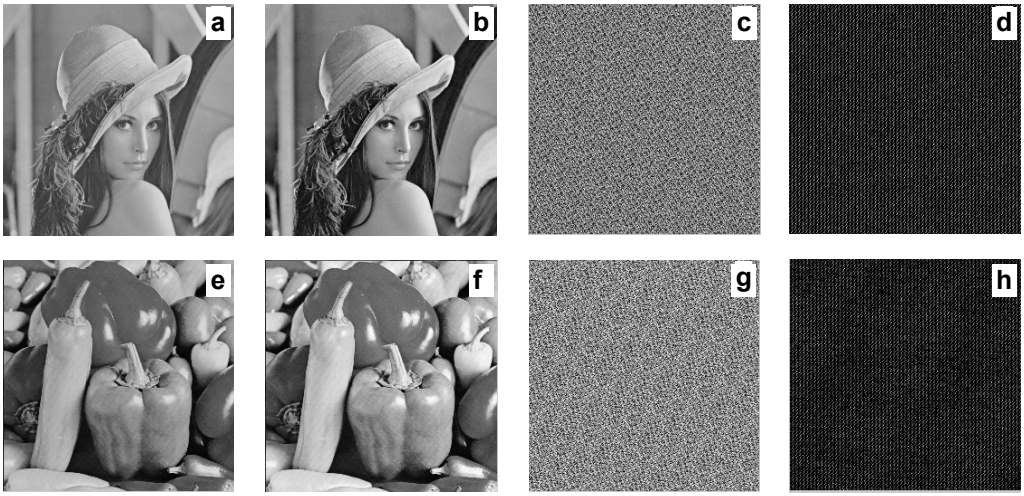

Fig. 8. Original *Lena* (**a**), and decrypted *Lena* with right keys (**b**), wrong n (**c**), and wrong α (**d**). Original *Pepper* (**e**), and decrypted *Pepper* with right keys (**f**), wrong n (**g**), and wrong α (**h**).

Apparently, the decrypted images with wrong keys are unable to provide any meaningful information about the original images. The details of the original images become blurred when the decryption keys deviate from the encryption ones and the variation of the decrypted images is invisible visually if just a slight deviation occurs to the main keys.

4.3. Robustness analysis

Different decryption images are shown in Fig. 9 when the Gaussian noises of different intensities are added to the encryption image, where the noise intensity coefficients added to the decrypted images *Lena* and *Pepper* are 1, 10, 20 and 30, respectively. It is seen that the basic features of the decrypted images under different noise intensity

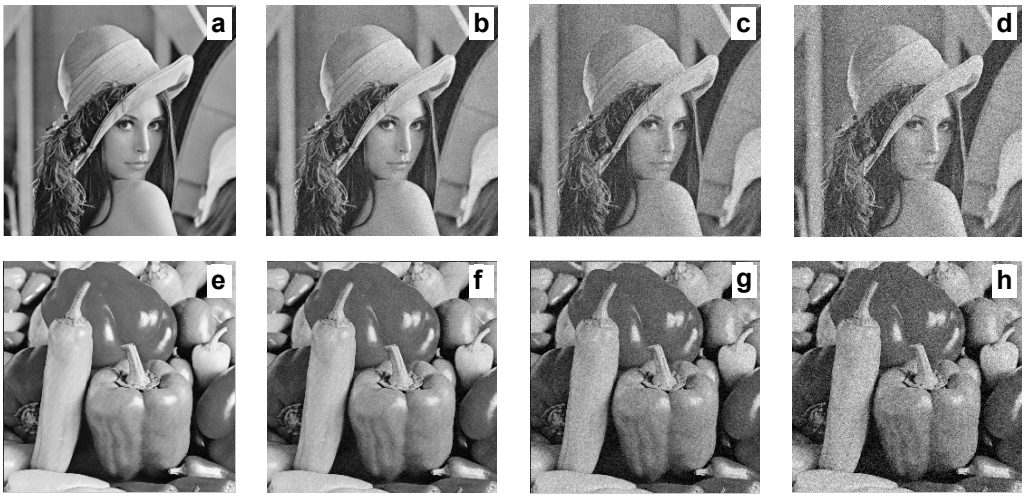

Fig. 9. Results of anti-noise. Decrypted images of *Lena* with taking $k = 1$ (**a**), $k = 10$ (**b**), $k = 20$ (**c**), and $k = 30$ (**d**). Decrypted images of *Pepper* with taking $k = 1$ (**e**), $k = 10$ (**f**), $k = 20$ (**g**), and $k = 30$ (**h**).

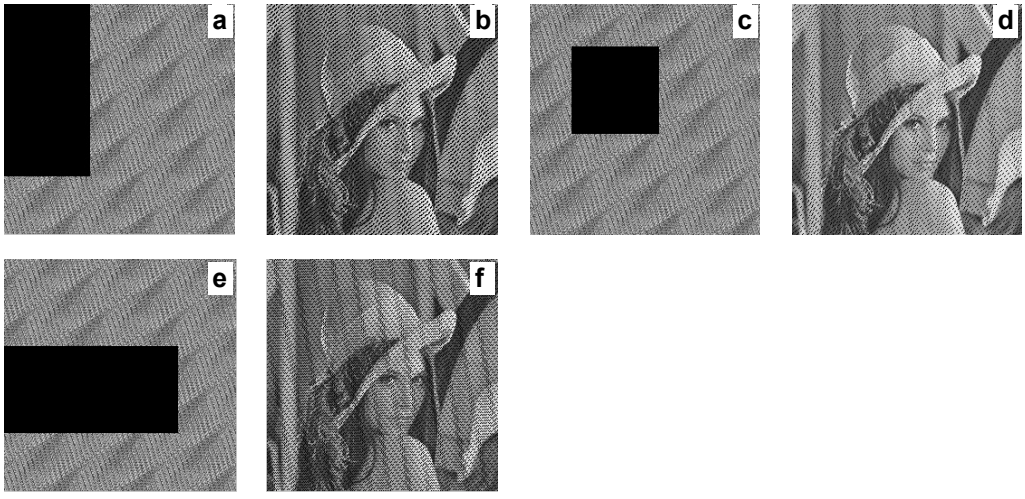

Fig. 10. Robustness against data loss. Loss of a left part (**a**), decryption the image of **a** (**b**), loss of a quarter of the center (**c**), decryption image of **c** (**d**), loss of a part of underside (**e**), and decryption image of **e** (**f**).

coefficients are still recognizable although the qualities of the decrypted images turn out to be worse and worse.

The encrypted images are supposed to be cut off in a random rectangle position, and then the cropped encrypted images are decrypted with correct ones. Figures 10**a**, 10**c** and 10**e** give the cropped ciphertext, while Fig. 10**b** shows the corresponding decrypted image of Fig. 8**a**. The corresponding decrypted image of Fig. 10**c** is shown in Fig. 10**d** and Fig. 10**f** shows the corresponding decrypted result of Fig. 10**e**.

It is shown that partial loss of ciphertext would have an impact apparently on the quality of the decrypted image. However, the decrypted images are still acceptable if a relatively small part of the ciphertext is lost, which illustrates that the proposed image encryption scheme could resist the shearing attack in a sense.

5. Conclusion

A new image encryption and decryption scheme based on the discrete fractional angular transform and the Arnold transform in image bit planes is designed. The proposed image encryption scheme has high resistance against the potential attacks. The independent parameters, the iterative times of the Arnold transform and the order of the discrete fractional angular transform are used as the keys. Numerical simulations and analysis demonstrate that the performance of the proposed image encryption algorithm is acceptable.

Acknowledgments – This work is supported by the National NSFC (Grant No. 61462061), the National Key Research and Development Program of China (2017YFB0802500), the Major Academic Discipline and Technical Leader of Jiangxi Province (Grant No. 20162BCB22011), the Natural Science Foundation of Jiangxi Province (Grant No. 20171BAB202002) and the Opening Project of Shanghai Key Laboratory of Integrated Administration Technologies for Information Security (Grant No. AGK201602).

References

[1] Ying-Qian Zhang, Xing-Yuan Wang, *Analysis and improvement of a chaos-based symmetric image encryption scheme using a bit-level permutation*, Nonlinear Dynamics 77(3), 2014, pp. 687–698.

[2] Nanrun Zhou, Shumin Pan, Shan Cheng, Zhihong Zhou, *Image compression-encryption scheme based on hyper-chaotic system and 2D compressive sensing*, Optics and Laser Technology 82, 2016, pp. 121–133.

[3] Hao-Ran Liang, Xiang-Yang Tao, Nan-Run Zhou, *Quantum image encryption based on generalized affine transform and logistic map*, Quantum Information Processing 15(7), 2016, pp. 2701–2724.

[4] Nan Run Zhou, Tian Xiang Hua, Li Hua Gong, Dong Ju Pei, Qing Hong Liao, *Quantum image encryption based on generalized Arnold transform and double random-phase encoding*, Quantum Information Processing 14(4), 2015, pp. 1193–1213.

[5] Dasgupta J., Bhattacharya K., Chanda B., *A holistic approach for off-line handwritten cursive word recognition using directional feature based on Arnold transform*, Pattern Recognition Letters 79, 2016, pp. 73–79.

[6] Ying-Qian Zhang, Xing-Yuan Wang, *Spatiotemporal chaos in mixed linear–nonlinear coupled logistic map lattice*, Physica A: Statistical Mechanics and its Applications 402, 2014, pp. 104–118.

[7] Ying-Qian Zhang, Xing-Yuan Wang, Li-Yan Liu, Yi He, Jia Liu, *Spatiotemporal chaos of fractional order logistic equation in nonlinear coupled lattices*, Communications in Nonlinear Science and Numerical Simulation 52, 2017, pp. 52–61.

[8] Ying-Qian Zhang, Xing-Yuan Wang, *A new image encryption algorithm based on non-adjacent coupled map lattices*, Applied Soft Computing 26, 2015, pp. 10–20.

[9] Ying-Qian Zhang, Xing-Yuan Wang, Jia Liu, Ze-Lin Chi, *An image encryption scheme based on the MLNCML system using DNA sequences*, Optics and Lasers in Engineering 82, 2016, pp. 95–103.

[10] Xing-Yuan Wang, Pi Li, Ying-Qian Zhang, Li-Yan Liu, Hengzhi Zhang, Xiukun Wang, *A novel color image encryption scheme using DNA permutation based on the Lorenz system*, Multimedia Tools and Applications 77(5), 2018, pp 6243–6265.

[11] KHADIJEH MIRZAEI TALARPOSHTI, MEHRZAD KHAKI JAMEI, *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.
[12] XIAOWEI LI, CHENGQING LI, IN-KWON LEE, *Chaotic image encryption using pseudo-random masks and pixel mapping*, Signal Processing 125, 2016, pp. 48–63.
[13] ZHIPENG WANG, HONGJUAN WANG, XINGQIANG YANG, PING ZHANG, CHENXIA HOU, YI QIN, *Optical image encryption by using diffractive imaging with special constraint in the input plane*, Optica Applicata 46(1), 2016, pp. 57–69.
[14] WEIMANN S., PEREZ-LEIJA A., LEBUGLE M., KEIL R., TICHY M., GRÄFE M., HEILMANN R., NOLTE S., MOYA-CESSA H., WEIHS G., CHRISTODOULIDES D.N., SZAMEIT A., *Implementation of quantum and classical discrete fractional Fourier transforms*, Nature Communications 7, 2016, article ID 11027.
[15] BHATTA I., SANTHANAM B., *A comparative study of commuting matrix approaches for the discrete fractional Fourier transform*, 2015 IEEE Signal Processing and Signal Processing Education Workshop (SP/SPE), 2015, pp. 1–6.
[16] AZOUG S.E., BOUGUEZEL S., *A non-linear preprocessing for opto-digital image encryption using multiple-parameter discrete fractional Fourier transform*, Optics Communications 359, 2016, pp. 85–94.
[17] NANRUN ZHOU, JIANPING YANG, CHANGFA TAN, SHUMIN PAN, ZHIHONG ZHOU, *Double-image encryption scheme combining DWT-based compressive sensing with discrete fractional random transform*, Optics Communications 354, 2015, pp. 112–121.
[18] SINHA A., SINGH K., *Image encryption by using fractional Fourier transform and jigsaw transform in image bit planes*, Optical Engineering 44(5), 2005, article ID 057001.
[19] ZHENGJUN LIU, AHMAD M.A., SHUTIAN LIU, *A discrete fractional angular transform*, Optics Communications 281(6), 2008, pp. 1424–1429.
[20] LIANSHENG SUI, KUAIKUAI DUAN, JUNLI LIANG, *A secure double-image sharing scheme based on Shamir's three-pass protocol and 2D Sine Logistic modulation map in discrete multiple-parameter fractional angular transform domain*, Optics and Lasers in Engineering 80, 2016, pp. 52–62.
[21] 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.
[22] JING YU, YUAN LI, XINWEN XIE, NANRUN ZHOU, ZHIHONG ZHOU, *Image encryption algorithm by using logistic map and discrete fractional angular transform*, Optica Applicata 47(1), 2017, pp. 141–155.
[23] ARNOLD V.I., AVEZ A., *Ergodic Problems of Classical Mechanics*, Benjamin, 2015.
[24] DYSON F.J., FALK H., *Period of a discrete cat mapping*, American Mathematical Monthly 99(7), 1992, pp. 603–614.
[25] YING-QIAN ZHANG, XING-YUAN WANG, *A symmetric image encryption algorithm based on mixed linear–nonlinear coupled map lattice*, Information Sciences 273, 2014, pp. 329–351.

Received July 20, 2017
in revised form October 9, 2017