Optics and Lasers in Engineering 50 (2012) 248–255

Contents lists available at SciVerse ScienceDirect

Optics and Lasers in Engineering

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

Double image encryption by using Arnold transform and discrete fractional angular transform

Zhengjun Liu [a,*], Min Gong [a], Yongkang Dou [a], Feng Liu [a], Shen Lin [a], Muhammad Ashfaq Ahmad [c], Jingmin Dai [a], Shutian Liu [b]

[a] Department of Automation Measurement and Control Engineering, Harbin Institute of Technology, Harbin 150001, PR China
[b] Department of Physics, Harbin Institute of Technology, Harbin 150001, PR China
[c] Department of Physics, COMSATS Institute of Information Technology, Lahore 54000, Pakistan

ARTICLE INFO

Article history:
Received 26 May 2011
Received in revised form
8 July 2011
Accepted 23 August 2011
Available online 16 September 2011

Keywords:
Information security
Random blocking
Pixel scrambling

ABSTRACT

Based on Arnold transform and discrete fractional angular transform, a double image encryption algorithm is designed. Two original images are regarded as the amplitude and phase of a complex function. Arnold transform is introduced for scrambling the pixels at a local area of the complex function. Subsequently the changed complex function is converted by discrete fractional angular transform. The operations mentioned will be performed many times. The amplitude of final output complex function is the encrypted image and its phase is regarded as the key of encryption algorithm. The parameters of the two transforms serve as the additional keys for enhancing the security. Some numerical simulations have been done to validate the performance of this encryption scheme.

1. Introduction

Information security has become an important topic in the processes of storage and transmission. According to the characteristic of output secret data, the reported information security algorithms can be classified into three kinds of styles: (i) image encryption, (ii) watermarking, (iii) image sharing. Some random operations and transforms [1–12] have been introduced into the design of encryption algorithm, such as random phase encoding, fractional transform and jigsaw transform. For random phase encoding, the designed phase mask is placed at the input plane of optical transform system to randomize the original data. In pure digital image encryption, chaotic sequence and logistic operation can be utilized for constructing encryption scheme [13,14]. Watermarking technology [15,16] is to protect the copyright of media product or artistic works. Image sharing [17–20] is a kind of encryption format with many output ciphers, in which some encrypted images are collected and required for recovering original secret information together.

Multiple-image encryption has been developed and researched in recent years. Using wavelength multiplexing technology a multiple encryption method has been reported by Situ and Zhang [21]. Subsequently other multiplexing technology or methods have been considered for encrypting many images, such as position multiplexing and information prechoosing [22–27]. A multiple encryption method [28] has been designed by a modified Gerchberg–Saxton phase retrieval algorithm in Fresnel domain. Double random phase encoding method has also been considered for hiding many images [29]. A multiple image encryption algorithm has been proposed using parameter multiplexing and phase-shifting interferometry [30]. Several multiple encryption schemes composed of quadrature multiplexing or fractional Fourier transform have been reported for encrypting two or three images [31–34].

As a special case of multiple-image encryption, double image encryption algorithm has been explored. A double image encryption [35] has been presented based on iterative fractional Fourier transform, in which original images are regarded as the amplitude of the transform. Afterwards, amplitude encoding and phase encoding have been researched for encrypting two secret images [36–41]. Moreover the real part and imaginary part of complex function have been considered for hiding two images [42].

In this paper, a double image encryption algorithm is designed and researched by the use of Arnold transform and discrete fractional angular transform. Two secret images are regarded as the amplitude and phase of the complex function. Arnold transform is introduced for scrambling the data at the local area of complex function. Discrete fractional angular transform is used for changing the values of 2D data. The two transforms are employed many times in order to introduce more parameters serving as key. In this encryption scheme, the phase information of the final output is the main key of this encryption method and the amplitude information is the encrypted image. The parameters

* Corresponding author. Fax: +8645186415146.
E-mail addresses: zjliu@hit.edu.cn, zjliuv@gmail.com (Z. Liu).

0143-8166/$ - see front matter © 2011 Elsevier Ltd. All rights reserved.
doi:10.1016/j.optlaseng.2011.08.006

from the two transforms will serve as the additional keys for enhancing security. Some numerical simulation results have been performed to test the performance of the proposed image encryption algorithm.

The rest of this paper is organized in the following sequence. In Section 2, the proposed double-image encryption algorithm is addressed. In Section 3, some numerical simulations are given to demonstrate the validity of this algorithm. Concluding remarks are summarized in the final section.

2. Double image encryption scheme

Before introducing the double image encryption algorithm, we present the definition and properties of the discrete fractional angular transform and Arnold transform briefly.

Discrete fractional angular transform is defined by a recursion process with two angles [43]. When the dimension of signal is 2 or 3, the eigenvector matrices are calculated as

$$V_{2,\theta}=\begin{bmatrix}\cos\theta & \sin\theta\\ -\sin\theta & \cos\theta\end{bmatrix} \tag{1}$$

and

$$V_{3,\theta}=\begin{bmatrix}\cos\theta & \sin\theta & 0\\ 0 & 0 & 1\\ -\sin\theta & \cos\theta & 0\end{bmatrix} \tag{2}$$

The matrices in Eqs. (2) and (3) will be regarded as the initial values of recursion procedure. Assuming $V_{N,\theta}$ as an orthonormal matrix, the following matrices

$$V_{2N,\theta}=\frac{1}{\sqrt{2}}\begin{bmatrix}V_{N,\theta} & V_{N,\theta}\\ -V^z_{N,\theta} & V^z_{N,\theta}\end{bmatrix} \tag{3}$$

and

$$V_{2N+1,\theta}=\frac{1}{\sqrt{2}}\begin{bmatrix}V_{N,\theta} & V_{N,\theta} & V^t_0\\ V_0 & V_0 & \sqrt{2}\\ -V^z_{N,\theta} & V^z_{N,\theta} & V^t_0\end{bmatrix} \tag{4}$$

are orthonormal and are regarded as the recursion rule. Where the superscript 'z' is to flip the corresponding matrix in the top–down direction, and V_0 is a $1\times N$ zero vector. For the computation of any eigenvector matrix $V_{k,\theta}$, whole recursion flowchart is illustrated in Fig. 1. In the first step, a half integer $[k/2]$ is considered and the eigenvector matrix $V_{[k/2],\theta}$ is obtained. Here '$[x]$' denotes to find a maximum integer is less than or equal to x. Eq. (3) or (4) will be used for converting $V_{[k/2],\theta}$ into $V_{k,\theta}$ according to the parity of the integer k. In the next step, the converting calculation between $V_{[k/2],\theta}$ and $V_{[[k/2]/2],\theta}$ will be performed using a similar operation. The process will recur until the divided half integer equals to 2 or 3, which is calculated by Eq. (1) or (2). The eigenvector matrix can be calculated quickly, because recursion process is employed only in the procedure. The kernel matrix of this transform $\mathcal{R}^{\alpha}_{\theta}$ can be expressed as

$$\mathcal{R}^{\alpha}_{\theta}=V_{N,\theta}D^{\alpha}_{N}(V_{N,\theta})^t, \tag{5}$$

where D^{α}_{N} is a diagonal matrix composed of all eigenvalues of this transform. The parameter α is an angle relating fractional order. The transform has some properties similar to fractional Fourier transform [43,44], such as linearity, unitarity, index additivity, multiplicity and Parseval energy conservation. The inverse transform of discrete fractional angular transform $\mathcal{R}^{\alpha}_{\theta}$ can be obtained by taking a negative fractional order to generate the corresponding kernel matrix, namely $\mathcal{R}^{-\alpha}_{\theta}$. The inverse transform $\mathcal{R}^{-\alpha}_{\theta}$ will be utilized for decrypting the secret images in this encryption algorithm.

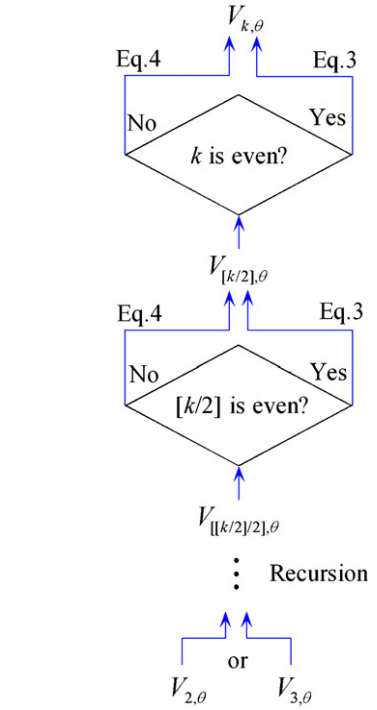

Fig. 1. Recursion calculating the eigenvector matrix $V_{k,\theta}$

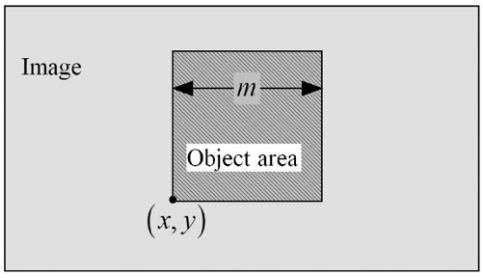

Fig. 2. Selected area scrambled by Arnold transform.

Arnold transform is to shift all the elements of a matrix and is defined as [45]

$$\mathcal{A}_M:\begin{bmatrix}x'\\ y'\end{bmatrix}=\mathrm{mod}\left(\begin{bmatrix}1, & 1\\ 1, & 2\end{bmatrix}\begin{bmatrix}x\\ y\end{bmatrix},M\right), \tag{6}$$

where $\mathcal{A}_M$ denotes the Arnold transform. The parameter M is the size of a square matrix. The variables $[x,y]^t$ and $[x',y']^t$ are the position vectors of matrix element before and after performing the Arnold transform, respectively. Eq. (6) will be executed many times in the application of Arnold transform. The transform in Eq. (6) cannot deal with whole image directly, when the input image is not a square. To solve this limitation, a local processing scheme is considered and is displayed in Fig. 2. The region marked with 'object area' is square and is defined by the three parameters (x,y,m), which restricts the position and size of selected range. The constraint condition of the parameters (x,y,m) is that the selected sub-image should be in whole image. The sub-image will be scrambled by Arnold transform in this encryption algorithm. The transform is periodic at the aspect of executing number. Thereby the sum of number performing the Arnold transform and corresponding inverse transform is equal to its period.

Fig. 3(a) gives the illustration of the proposed image encryption. The two original images I_1 and I_2 are regarded as the

amplitude and normalized phase of the complex function C_1, respectively. When the pixel value of image I_1 is equal to 0, which will hide the corresponding phase information, a pretreatment should be considered and is expressed as

$$I_1'(x,y) = I_1(x,y) + \delta, \tag{7}$$

where δ is a positive number to ensure that all pixels of the image I_1 is nonzero. The image $I_1'(x,y)$ will substitute for the image I_1 in next calculation and then a square sub-image defined with the parameters (x_1,y_1,m_1) in the complex function C_1, will be scrambled by Arnold transform $\mathcal{A}_{m_1}$. The scrambled complex function will be converted by discrete fractional angular transform $\mathcal{R}_\theta^\alpha$, in which the complex function C_2 is received. According to the operations mentioned above, the two transforms will be employed iteratively for enhancing the security of encryption scheme. Here the values of parameters defined sub-image are different in every calculation. The final output of this algorithm is the complex function C_{k+1}, which includes the amplitude A and normalized phase φ serving as the encrypted image and key, respectively. Fig. 3(b) shows the process of image decryption, in which the corresponding inverse transforms are utilized.

In this algorithm, the parameters (x_k, y_k, m_k, θ and α) of Arnold transform and discrete fractional angular transform are independent of the encryption process and are regarded as the additional keys for increasing the security. In the double random phase encoding method, random phase is independent of the encryption algorithm [1]. However, the normalized phase φ is generated by the proposed double image encryption scheme and serves as the main key of this algorithm, which includes many independent data. The contribution of these keys to security will be discussed in the next section.

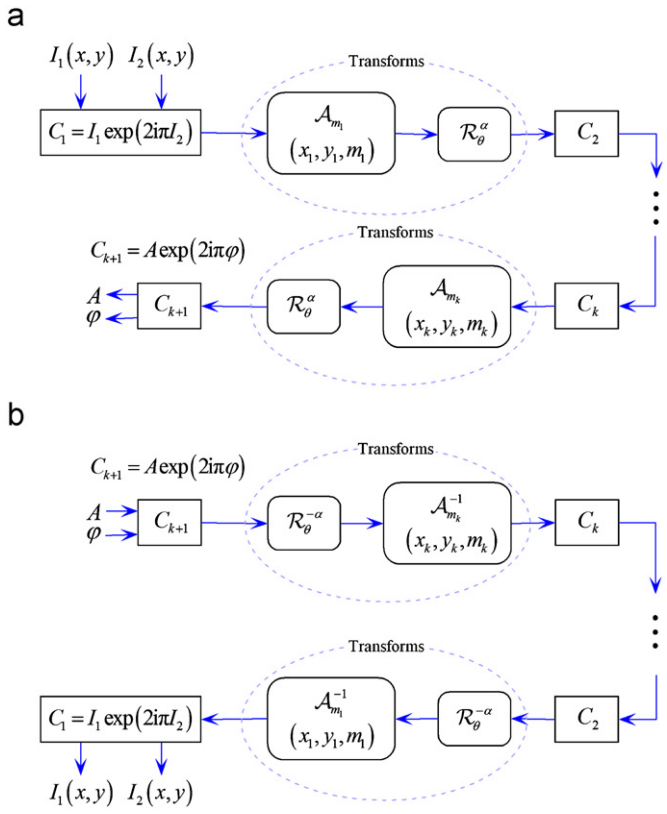

Fig. 3. Flowchart of the proposed double image encryption algorithm.

3. Numerical simulation

As an example, two gray-level images having 384×256 pixels are shown in Fig. 4 and are regarded as the original images in numerical simulation. For discrete fractional angular transform, the angles θ and α are fixed at 1.9 and 1.2, respectively. The iterative number of the encryption process is taken at 4 in the test. The parameters of Arnold transform are listed in Table 1. Here the variables y_k and x_k are the indices of row and column of a matrix, respectively. The symbols 'j_k' and 'T_k' indicate the executing number of Arnold transform and its period, respectively. By the use of the proposed algorithm with the parameters mentioned above, an encrypted result is illustrated in Fig. 5, in which both the images are random pattern. Using right decryption process with

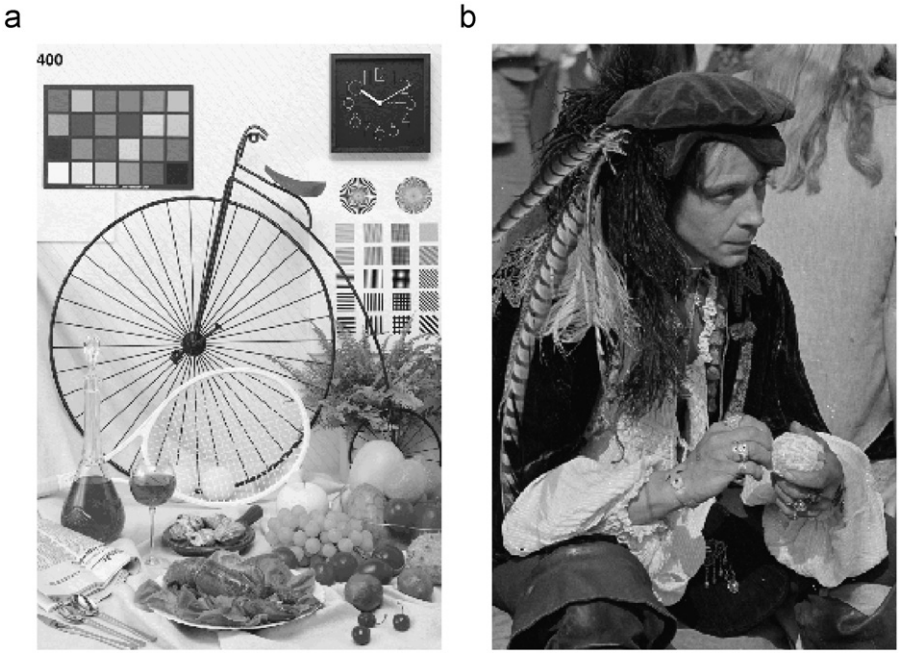

Fig. 4. Two original images having 768×512 pixels in numerical simulation.

Table 1
The parameters of Arnold transform in numerical simulation.

	The iterative number k			
	1	2	3	4
x_k	2	8	4	6
y_k	1	3	5	7
m_k	193	196	215	227
j_k	43	56	78	60
T_k	194	168	220	228

all correct keys, the retrieved images are displayed in Fig. 6, which are consistent with the original images.

The quality of encrypted data is weighted by histogram distribution, entropy and correlation coefficient. The last two statistical functions are defined as

$$\bar{I} = \frac{1}{MN}\sum_{\forall m,n} I_{m,n},$$

$$\sigma^2(I) = \frac{1}{MN}\sum_{\forall m,n}[I_{m,n}-\bar{I}]^2,$$

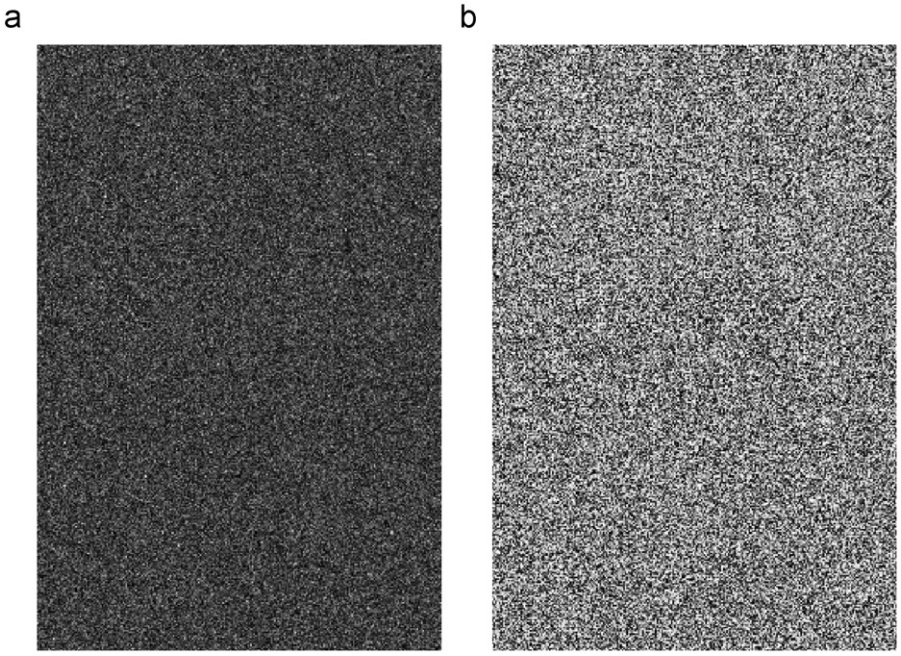

Fig. 5. Output of the encryption scheme: (a) the amplitude A and (b) the phase φ.

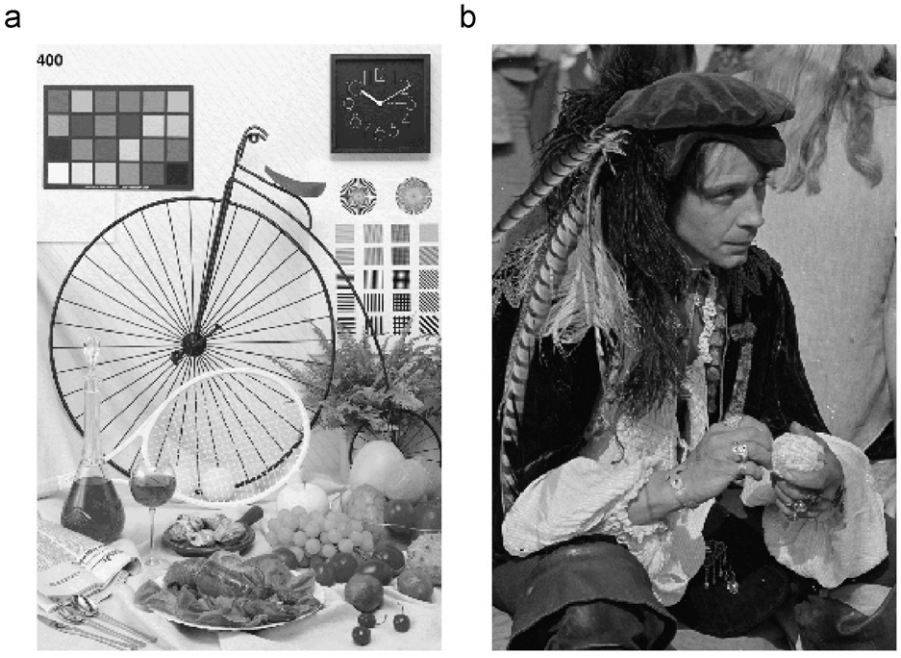

Fig. 6. Recovered result obtained using correct decryption process with all correct keys.

$$\mathrm{cov}(I,J)=\frac{1}{MN}\sum_{\forall m,n}[I_{m,n}-\bar{I}][J_{m,n}-\bar{J}],$$

$$cc=\frac{\mathrm{cov}(I,J)}{\sqrt{\sigma^2(I)\sigma^2(J)}}, \tag{8}$$

$$E(I)=-\sum_{k=0}^{255}p(I_k)\log_2[p(I_k)], \tag{9}$$

where I and J are the compared image and the original image, respectively. The values of I and J are normalized into the interval [0,255]. 'cc' is the correlation coefficient. The symbol '$E(I)$' denotes the entropy of the image I. The $p(I_k)$ is a probability function. The histogram distribution of encrypted data A and the key is displayed in Fig. 7, in which the original images are also calculated and expressed. The histogram of encrypted data is different from the original images. The correlation coefficient and entropy are computed and shown in Table 2 for testing the distribution of secret information.

To express the error of the decrypted image I_d and original image I_o quantitatively, the relative mean square error (RMSE) function is considered and defined as follows:

$$\mathrm{RMSE}=\mathrm{rmse}(I_d,I_o)=\frac{\sum_{\forall p,q}[I_d(p,q)-I_o(p,q)]^2}{\sum_{\forall p,q}[I_o(p,q)]^2}. \tag{10}$$

The RMSE value will be calculated for weighting the difference of recovered image and original image as a criterion.

The sensitiveness of two angles in discrete fractional angular transform is considered and calculated first. Here the decryption process and the parameters of Arnold transform and the key φ are taken in correct format. The decryption test with various values of the order α and the angle θ, is shown in Figs. 8 and 9, respectively. Here only one between the two angles is altered in calculation. For the effective range in decryption, the order α is more sensitive than the angle θ. Two pairs of recovered images are illustrated in Figs. 8 and 9 for $\alpha=1.1992$ and $\theta=1.5$. From the two figures, the fractional order α can protect the secret images and the contribution of the angle θ to security is very small. To enhance the sensitiveness, a big number N_0 can be introduced into the computation of the angle θ, namely the angle θ is replaced with $N_0\theta$ in Eqs. (1) and (2). For example, the parameter N_0 can be fixed at N in Eq. (5).

The contribution of the parameters of Arnold transform to the security is checked by changing the corresponding values. Here four examples are calculated with some incorrect data replacing with the parameters (x_k,y_k,m_k,j_k). In every example, the parameters controlling Arnold transform in all iterative decryption process are taken in the data in a column of Table 1. The angles in discrete fractional angular transform and the key φ are fixed at

Table 2
Values of statistical function of the encrypted data A and the key φ.

	A	φ
Entropy	7.071	7.992
cc calculated with I_1	2.0×10^{-3}	4.9×10^{-3}
cc calculated with I_2	2.4×10^{-3}	1.4×10^{-3}

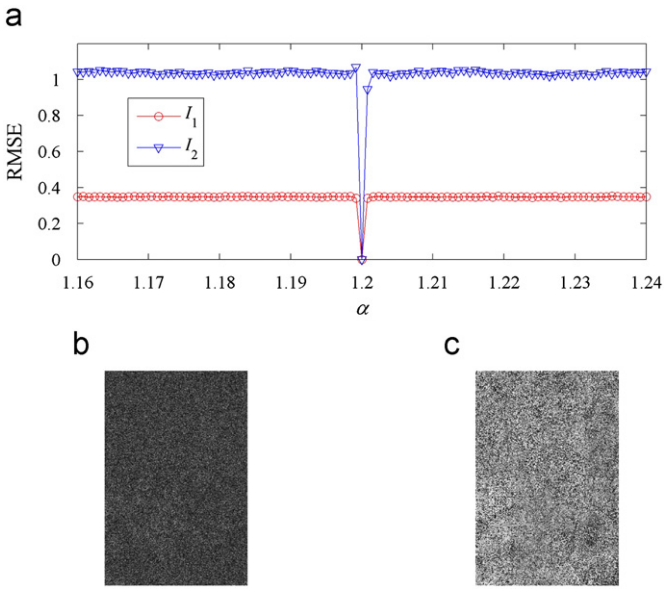

Fig. 8. Sensitiveness of the fractional order α in decryption process: (a) RMSE curve, (b) the first decrypted image $I_{1,d}$ and (c) the second decrypted image $I_{2,d}$ using $\alpha=1.1992$.

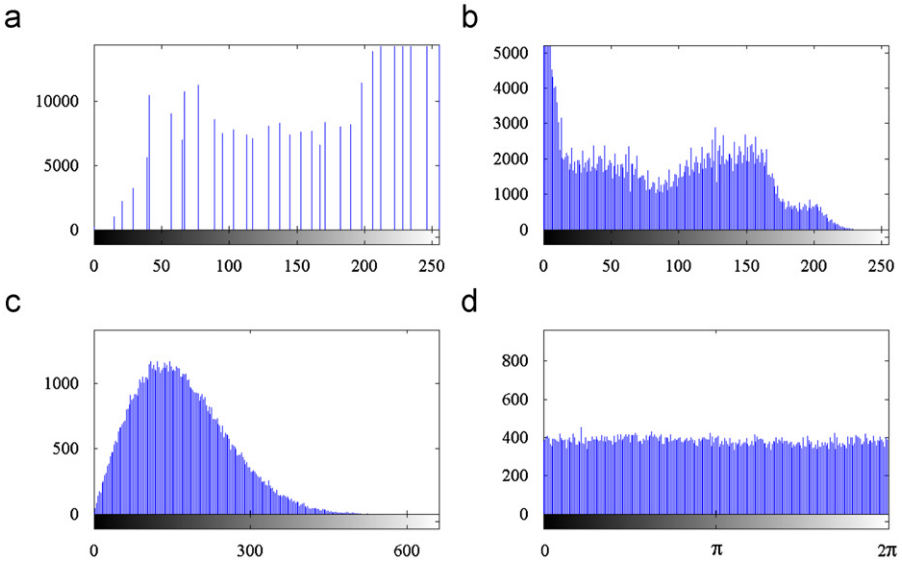

Fig. 7. Histogram of the images: (a) Fig. 4(a), (b) Fig. 4(b), (c) Fig. 5(a), (d) Fig. 5(b).

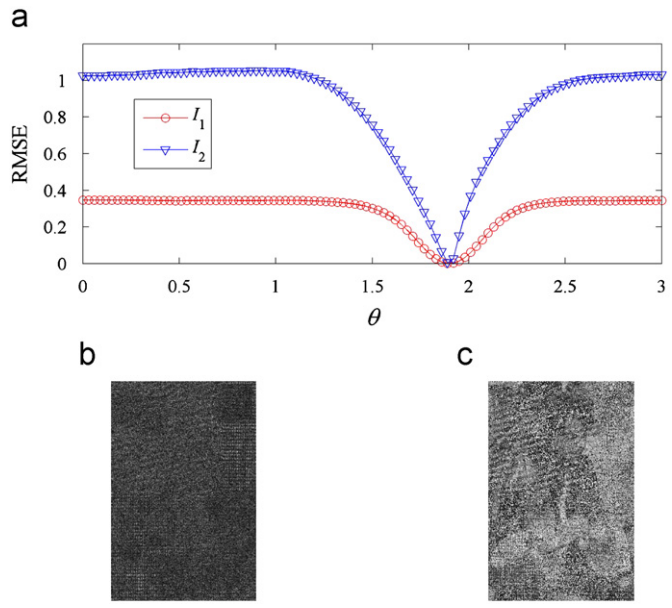

Fig. 9. Sensitiveness of the angle θ in decryption process: (a) RMSE curve, (b) the first decrypted image $I_{1,d}$ and (c) the second decrypted image $I_{2,d}$ using $\theta=1.5$.

Table 3
The decryption result using the incorrect parameters of Arnold transform.

		Test label			
		(1)	(2)	(3)	(4)
RMSE	$I_{1,d}$	0.3478	0.3450	0.3356	0.3446
	$I_{2,d}$	1.0011	0.9665	0.9220	0.9856

the right value. The RMSE values of two retrieved images are computed and shown in Table 3, which implies that the decrypted results are noise-like images. From Table 3, the parameters of Arnold transform can serve as key to hide secret images as well.

The normalized phase φ is the main body of this encryption algorithm. In this paper, the corresponding decryption will be calculated and analyzed, when the key φ is known by attacker partly. The effective scale of key on security can also be evaluated for analyzing key space. Fig. 10 gives two recovering cases under the case that a half of the key φ is determined. The unknown data of the key φ is replaced with 0.5 in numerical simulation. Here the parameters of Arnold transform and discrete fractional angular transform are fixed at the correct values. The pattern of the known key φ is displayed in Fig. 10(a) and (d), which will be used in image decryption test. The decrypted result of the first image shown in Fig. 10(b) and (e) are random pattern. However, a blurry outline of the second image can be recognized from the results illustrated in Fig. 10(c) and (f). From Fig. 10, the first image is safer than the second image in this encryption scheme.

Sometimes the data of encrypted information will be destroyed or polluted by noise in storage and transmission. An example of noise polluting the data is simulated and defined as follows:

$$I'_e(p,q) = I_e(p,q)[1+s\sigma_{0,1}(p,q)], \tag{11}$$

where the symbols I_e and I'_e denote the images before and after adding noise, respectively. The parameter s is a coefficient controlling the intensity of noise. The function $\sigma_{0,1}(p,q)$ having the mean value 0 and the standard deviation 1 is a random. The noise function $\sigma_{0,1}(p,q)$ satisfies uniform distribution. By the use of all correct keys, the RMSE curves are computed and drawn in Fig. 11(a). When $s=0.7$, two decrypted images are shown in Fig. 11(b) and (c), from which the basic outlook of the two original

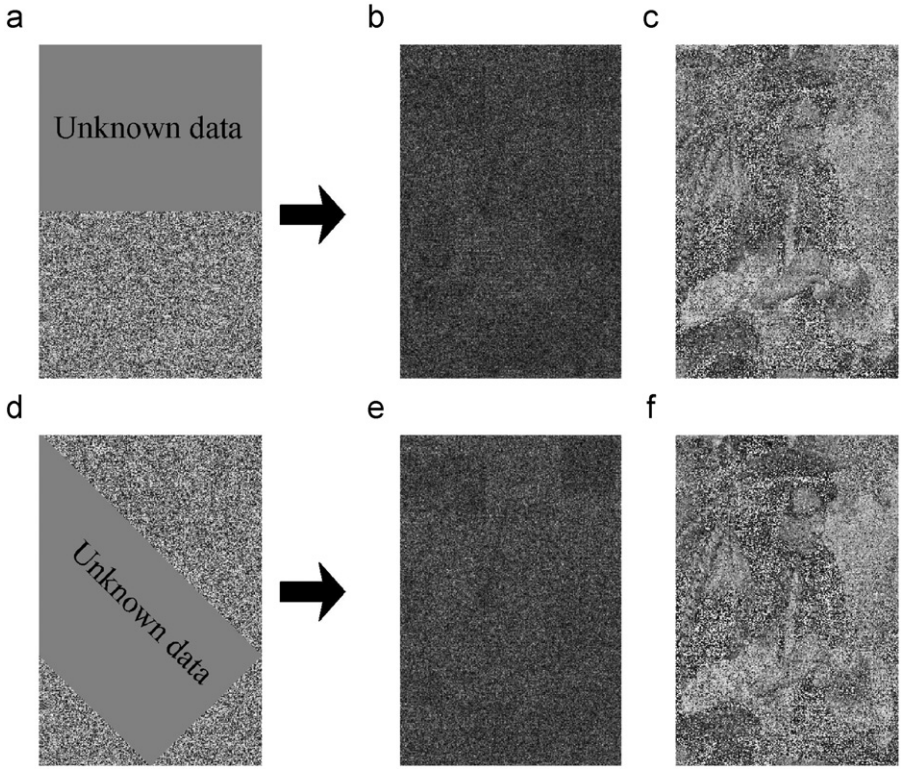

Fig. 10. Decryption results obtained using a half of the known data of the key φ: (a) the known key φ, (b) the decrypted image $I_{1,d}$ with RMSE=0.2989, (c) the decrypted image $I_{1,d}$ with RMSE=0.7590; (d) the known key φ, (e) the decrypted image $I_{1,d}$ with RMSE=0.2932, (f) the decrypted image $I_{1,d}$ with RMSE=0.7678. Here the decrypted images (b) and (c) are from the key shown in Fig. 9(a). The decrypted images (e) and (f) are from the key shown in Fig. 10(d).

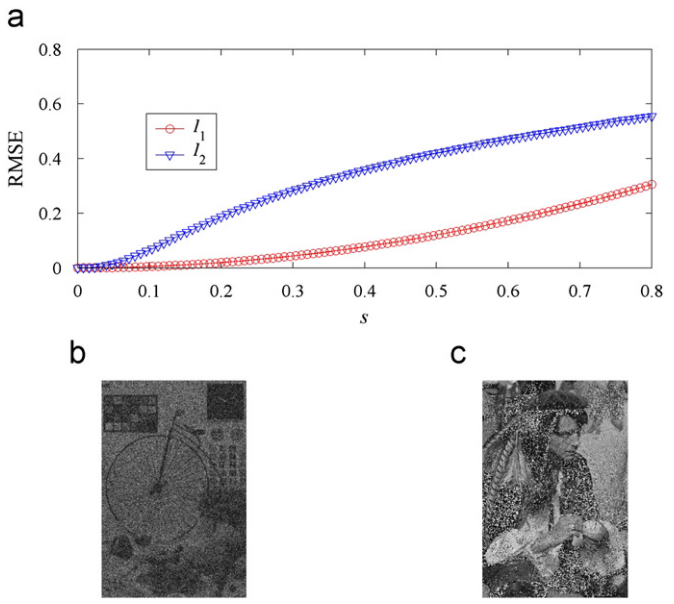

Fig. 11. Robustness test of the encryption algorithm: (a) RMSE curves with various values of the parameter s, (b) the decrypted result of the first image $I_{1,d}$ with RMSE=0.2341, (c) the decrypted result of the first image $I_{2,d}$ with RMSE=0.5140. Here the image shown in Fig. 11(b) and (c) are obtained using $s=0.7$.

secret images can be identified in vision. The two original images can be retrieved, when the encrypted image is changed by noise.

In some random phase encoding in linear encryption techniques, random data is regarded as key and is employed to obtain encrypted image, such as double random phase encoding. If the random phase is used for encrypting other images, the encryption method will be threatened by chosen-plaintext attack or known-plaintext attack [8,9]. In the proposed algorithm, the key is generated from the phase distribution of output data. This key will depend on the original image. In other words, the key cannot be employed to hide other images.

4. Conclusion

We have researched a double-image encryption method using Arnold transform and discrete fractional angular transform. The two original secret images are encoded as the amplitude and phase of a complex function. Arnold transform is introduced for scrambling the local square area of the complex function and its spectrum of discrete fractional angular transform. The size and position of the square area are defined with three parameters. The Arnold transform and discrete fractional angular transform are executed iteratively. The amplitude and phase of output data of the encryption algorithm are regarded as the encrypted image and key, respectively. The parameters defining Arnold transform and fractional order of discrete fractional angular transform can serve as the additional key for increasing the security of encryption scheme. Some numerical simulations have been achieved to demonstrate the performance of the proposed double image encryption algorithm.

Acknowledgments

This work was supported by the National Natural Science Foundation of China under Grant 11104049, 10974039 and 11047153, Specialized Research Fund for the Doctoral Program of Higher Education (Grant 20102302120009), the development program for outstanding young teachers in Harbin Institute of Technology (Grant HITQNJS. 2008. 027) and the Fundamental Research Funds for the Central Universities (Grant HIT.NSRIF.2009038). The authors wish to thank the two reviewers for their useful suggestions.

References

[1] Refregier P, Javidi B. Optical image encryption based on input plane and Fourier plane random encoding. Opt Lett 1995;20:767–9.
[2] Liu Z, Liu S. Random fractional Fourier transform. Opt Lett 2007;32:2088–90.
[3] Hennelly B, Sheridan JT. Optical image encryption by random shifting in fractional Fourier domains. Opt Lett 2003;28:269–71.
[4] Zhou N, Dong T, Wu J. Novel image encryption algorithm based on multiple-parameter discrete fractional random transform. Opt Commun 2010;283:3037–42.
[5] Zhang Y, Wang B. Optical image encryption based on interference. Opt Lett 2008;33:2443–5.
[6] Liu Z, Guo Q, Xu L, Ahmad MA, Liu Shutian. Double image encryption by using iterative random binary encoding in gyrator domains. Opt Express 2010;18:12033–43.
[7] Chen L, Zhao D. Color information processing (coding and synthesis) with fractional Fourier transforms and digital holography. Opt Express 2007;15:16080–9.
[8] Peng X, Wei H, Zhang P. Chosen-plaintext attack on lensless double-random phase encoding in the Fresnel domain. Opt Lett 2006;31:3261–3.
[9] Peng X, Zhang P, Wei H, Yu B. Known-plaintext attack on optical encryption based on double random phase keys. Opt Lett 2006;31:1044–6.
[10] Pei S-C, Ding J-J. Two-dimensional affine generalized fractional Fourier transform. IEEE Trans Signal Process 2001;49:878–97.
[11] Unnikrishnan G, Joseph J, Singh K. Optical encryption by double-random phase encoding in the fractional Fourier domain. Opt Lett 2000;25:887–9.
[12] Kumar P, Joseph J, Singh K. Double random phase encryption with in-plane rotation of a modified Lohmann's second-type system in the anamorphic fractional Fourier domain. Opt Eng 2008;47:117001.
[13] Tong X, Cui M. Image encryption scheme based on 3D baker with dynamical compound chaotic sequence cipher generator. Signal Process 2009;89:480–91.
[14] Liao X, Lai S, Zhou Q. A novel image encryption algorithm based on self-adaptive wave transmission. Signal Process 2010;90:2714–22.
[15] AliAkhaee M, Kalantari NK, Marvasti F. Robust audio and speech watermarking using Gaussian and Laplacian modeling. Signal Process 2010;90:2487–97.
[16] Liu Y, Zhao J. A new video watermarking algorithm based on 1D DFT and Radon transform. Signal Process 2010;90:626–39.
[17] Chen T-H, Wu C-S. Efficient multi-secret image sharing based on Boolean operations. Signal Process 2011;91:90–7.
[18] Liu Z, Ahmad MA, Liu S. Image sharing scheme based on combination theory. Opt Commun 2008;281:5322–5.
[19] Yang C-N, Huang S-M. Constructions and properties of k out of n scalable secret image sharing. Opt Commun 2010;283:1750–62.
[20] Liu Z, Liu S, Ahmad MA. Image sharing scheme based on discrete fractional random transform. Optik 2010;121:495–9.
[21] Situ G, Zhang J. Multiple-image encryption by wavelength multiplexing. Opt Lett 2005;30:1306–8.
[22] Situ G, Zhang J. Position multiplexing for multiple-image encryption. J Opt A: Pure Appl Opt 2006;8:391–7.
[23] Shi Y, Situ G, Zhang J. Multiple-image hiding by information prechoosing. Opt Lett 2008;33:542–4.
[24] Shi Y, Situ G, Zhang J. Multiple-image hiding in the Fresnel domain. Opt Lett 2007;32:1914–6.
[25] Xiao Y-L, Zhou X, Yuan S, Chen Y-Y. Multiple-image parallel optical encryption. Opt Commun 2010;283:2789–93.
[26] Xiao Y-L, Zhou X, Yuan S, Liu Q, Li Y-C. Multiple-image optical encryption: an improved encoding approach. Appl Opt 2009;48:2686–92.
[27] Barrera JF, Henao R, Tebaldi M, Torroba R, Bolognini N. Multiple-encoding retrieval for optical security. Opt Commun 2007;276:231–6.
[28] Hwang HE, Chang HT, Lie WN. Multiple-image encryption and multiplexing using a modified Gerchberg–Saxton algorithm and phase modulation in Fresnel-transform domain. Opt Lett 2009;34:3917–9.
[29] Alfalou A, Mansour A. Double random phase encryption scheme to multiplex and simultaneous encode multiple images. Appl Opt 2009;48:5933–47.
[30] Meng XF, Cai LZ, Wang YR, Yang XL, Xu XF, Dong GY, et al. Digital image synthesis and multiple-image encryption based on parameter multiplexing and phase-shifting interferometry. Opt Lasers Eng 2009;47:96–102.
[31] Joshi M, Shakher C, Singh K. Fractional Fourier transform based image multiplexing and encryption technique for four-RGB images using input images as key. Opt Commun 2010;283:2496–505.
[32] Joshi M, Shakher C, Singh K. Color image encryption and decryption for twin images in fractional Fourier domain. Opt Commun 2008;281:5713–20.
[33] Islam MN, Alam MS, Karim MA. Optical security system employing qudrarature multiplexing. Opt Eng 2008;47:048201.
[34] Joshi M, Singh K. Simultaneous encryption of a color and a gray-scale image using byte-level encoding based on single-channel double random-phase

encoding architecture in fractional Fourier domain. Opt Eng 2011;50: 0047007.
[35] Liu Z, Liu S. Double image encryption based on iterative fractional Fourier transform. Opt Commun 2007;275:324–9.
[36] Tao R, Xin Y, Wang Y. Double image encryption based on random phase encoding in the fractional Fourier domain. Opt Express 2007;15:16067–79.
[37] Liu Z, Li Q, Dai J, Sun X, Liu S, Ahmad MA. A new kind of double image encryption by using a cutting spectrum in the 1D fractional Fourier transform domains. Opt Commun 2009;282:1536–40.
[38] Li H, Wang Y. Double-image encryption based on iterative gyrator transform. Opt Commun 2008;281:5745–9.
[39] Liu Z, Dai J, Sun X, Liu S. Triple image encryption scheme in fractional Fourier transform domains. Opt Commun 2009;282:518–22.
[40] Chen W, Quan C, Jay C. Optical color image encryption based on Arnold transform and interference method. Opt Commun 2009;282:3680–5.
[41] Wu J, Zhang L, Zhou N. Image encryption based on the multiple-order discrete fractional cosine transform. Opt Commun 2010;283:1720–5.
[42] Liu Z, Chen H, Liu T, Li P, Dai J, Sun X, et al. Double-image encryption based on the affine transform and the gyrator transform. J Opt 2010;12:035407.
[43] Liu Z, Ahmad MA, Liu S. A discrete fractional angular transform. Opt Commun 2008;281:1424–9.
[44] Ozaktas HM, Zalevsky Z, Kutay MA. The Fractional Fourier Transform with Applications in Optics and Signal Processing. New York: John Wiley & Sons; 2000.
[45] Dyson FJ, Falk H. Period of a discrete cat mapping. Am Math Mon 1992;99: 603–24.