Optics and Lasers in Engineering 51 (2013) 472–480

Contents lists available at SciVerse ScienceDirect

Optics and Lasers in Engineering

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

Double optical image encryption using discrete Chirikov standard map and chaos-based fractional random transform

Yushu Zhang, Di Xiao *

College of Computer Science, Chongqing University, Chongqing 400044, China

ARTICLE INFO

Article history:
Received 14 August 2012
Received in revised form
14 November 2012
Accepted 14 November 2012
Available online 6 December 2012

Keywords:
Chaos-based discrete fractional random transform
Chirikov standard map
Discrete Chirikov standard transform
Chaotic random phase masks
Optical image encryption

ABSTRACT

In this paper, we design a novel discrete fractional random transform based on 2D chaotic logistic maps and two chaotic random masks resulting from Chirikov standard map. Then, a double optical image encryption scheme using discrete Chirikov standard map and chaos-based discrete fractional random transform is proposed. The discrete version of Chirikov standard map is employed to scramble the pixels of two images due to its property of area-preserving. Two scrambled images are regarded as the amplitude and phase of the synthesized input signal. Moreover, with the help of the chaos-based discrete fractional random transform and two chaotic random masks, double random phase encoding is utilized to complete encryption. Numerical simulations demonstrate the effectiveness and the security of the proposed scheme.

1. Introduction

In recent years, some classic encryption techniques such as optical transforms and chaotic maps have become a vital role in protecting images due to the increasing requirement for image storage and transmission. On the one hand, optical encryption methods have attracted much attention for their high speed, parallel processing and large storage memories. Much work has been done on optical image encryption [1–9]. On the other hand, chaos has also been introduced to image security thanks to its ergodicity, pseudo-randomness and sensitivity to initial conditions and control parameters. These inherent properties make chaotic maps a potential choice for designing cryptosystem [10–16]. Each of the two techniques mentioned above contains its own strengths and weaknesses. Apparently, combining their advantages together can be used to construct new-type image encryption schemes [17–26], which are better than single encryption techniques and further make up for their respective defects. Singh and Sinha [17] proposed a new idea to encrypt the image by using fractional Fourier transform (FrFT) and three chaos functions which was used to generate the chaotic random phase masks. Gyrator transform and two chaotic random phase masks have also been proposed [18]. Li and Wang [19] proposed a double-image encryption algorithm based on discrete fractional random transform (DFrRT) and two chaotic maps. These two maps are employed to generate the random matrices used in the DFrRT and scramble the image, respectively. Besides, chaos-based scrambling methods have also been used in optical communication [20–26].

In this paper, we propose a double image encryption algorithm using discrete Chirikov standard transform (DCST) and chaos-based discrete fractional random transform (CBDFrRT). DCST is first introduced for scrambling the pixel positions of two images. Then, two images are regarded as the amplitude and phase of the complex function. In addition, we design a chaos-based discrete fractional random transform and two chaotic random masks resulting from Chirikov standard map. Finally, random phase encoding is utilized to complete encryption. The novelty of the proposed scheme lies in the utilization of DCST and CBDFrRT. The CBDFrRT integrates the advantages of both chaos system and optical transform. The scrambling technique of DCST improves the security of the optical transform-only cryptosystem.

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

2. The proposed approach

A block diagram of our approach is shown in Fig. 1. Chirikov standard map and its discrete version are applied to generate chaotic random phase masks and scramble pixels, respectively. Chaos-based discrete fractional random transform and random

* Corresponding author. Tel.: +86 23 8633 3521; fax: +86 23 6510 4570.
E-mail address: xiaodi_cqu@hotmail.com (D. Xiao).

0143-8166/$ - see front matter © 2012 Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.optlaseng.2012.11.001

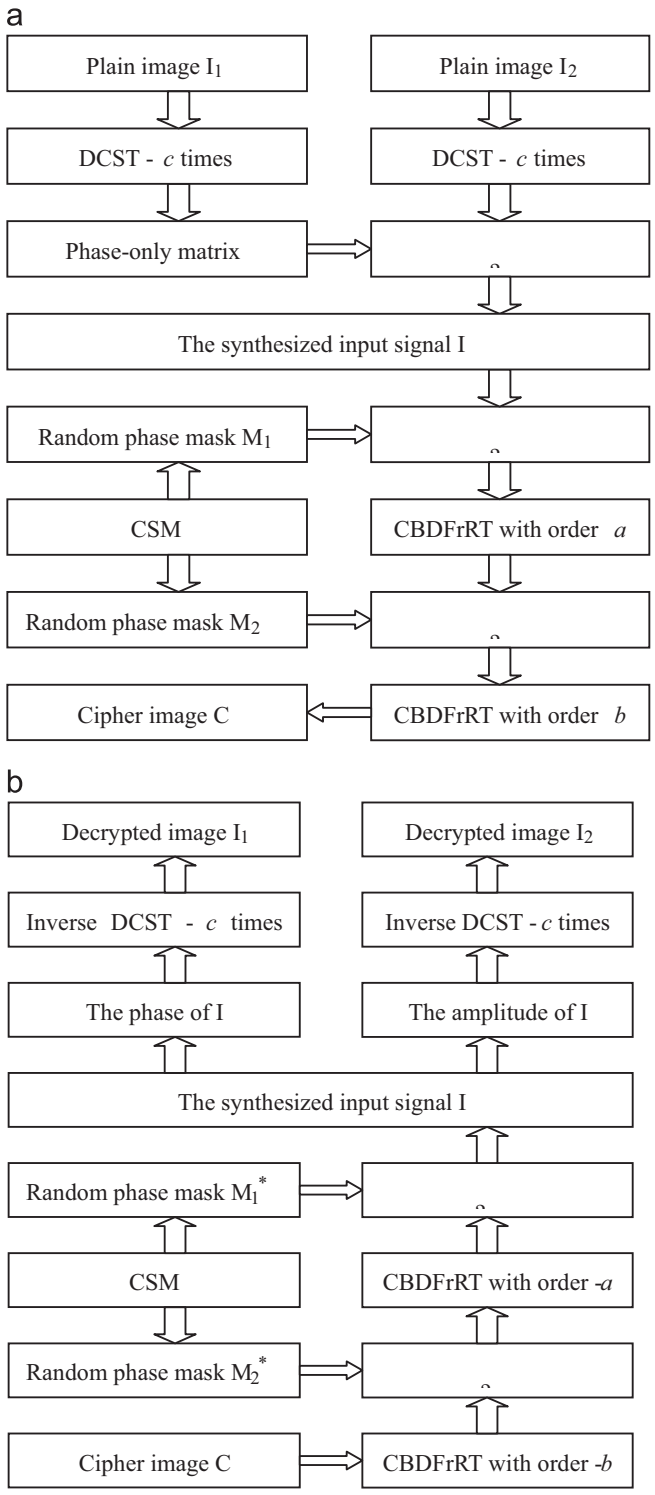

Fig. 1. A block diagram of the proposed scheme: (a) the encryption process and (b) the decryption process.

phase encoding are used for changing the pixel values. Details of the proposed approach are described as follows:

2.1. Discrete Chirikov standard map

Chirikov standard map (CSM) is an invertible area-preserving chaotic map for two canonical dynamical variables from a square with side 2π onto itself [27,28]. It is described by the following formulas:

$$\begin{cases} m_{i+1} = (m_i + n_i) \bmod 2\pi \\ n_{i+1} = (m_i + \varepsilon \sin(m_i + n_i)) \bmod 2\pi' \end{cases} \tag{1}$$

where $\varepsilon > 0$ is the control parameter, and the ith states m_i and n_i both take real values in $(0,2\pi)$ for all i.

As to CSM, the discretized version is defined in [29] by means of modifying the range from the square $(0,2\pi)\times(0,2\pi)$ to the positive integer $N \times N$. Its mathematical representation is given by

$$\begin{cases} x' = (x+y) \bmod N \\ y' = \left(y + \xi round\left(\sin\left(\frac{2\pi x'}{N}\right)\right)\right) \bmod N' \end{cases} \tag{2}$$

where N is the width or length of a square image, and ξ is a positive integer which can be used as the permutation key. The inverse transform for decryption is expressed as:

$$\begin{cases} x = \left(x' - y' + \xi round\left(\sin\left(\frac{2\pi x'}{N}\right)\right)\right) \bmod N \\ y = \left(y' - \xi round\left(\sin\left(\frac{2\pi x'}{N}\right)\right)\right) \bmod N \end{cases} \tag{3}$$

In order to test efficiency to scramble the pixel positions by using the Discrete Chirikov standard transform (DCST), A test image "Peppers" with 256×256 size for different permutation times is shown in Fig. 2. Results demonstrate that the correlation among the adjacent pixels is totally disturbed and it is impossible to recognize the image.

2.2. Chaos-based discrete fractional random transform

The discrete fractional random transform (DFrRT) [30] of 1D signal x can be written as matrix multiplications as follows:

$$\Re^{\alpha}(x) = \mathbf{R}^{\alpha} x \tag{4}$$

where $\mathbf{R}^{\alpha}$is the kernel transforms of the DFrRT and α indicates the fractional order.

$\boldsymbol{R}^{\alpha}$ can be written as

$$\mathbf{R}^{\alpha} = \mathbf{V}\mathbf{D}^{\alpha}\mathbf{V}^{t} \tag{5}$$

Here, $\mathbf{V}\mathbf{V}^{t} = \mathbf{I}$ and $\mathbf{D}^{\alpha}$ is a diagonal matrix as

$$\mathbf{D}^{\alpha} = \mathrm{diag}\left\{1, \exp\left(-\mathrm{i}\frac{2\pi\alpha}{T}\right), \exp\left(-\mathrm{i}\frac{4\pi\alpha}{T}\right), \cdots, \exp\left(-\mathrm{i}\frac{2(N-1)\pi\alpha}{T}\right)\right\}, \tag{6}$$

where T is a positive number. In this paper, we always take $T=1$. The randomness of the transform results from the matrix $\mathbf{V}$, which is generated by the eigenvectors of a symmetric random matrix $\mathbf{S}$. The matrix $\mathbf{S}$ is constructed by a $N \times N$ real random matrix $\mathbf{E}$ given by

$$\mathbf{S} = \frac{\mathbf{E} + \mathbf{E}^{t}}{2}. \tag{7}$$

In this paper, the random matrix $\boldsymbol{E}$ can be obtained from 2D chaotic Logistic maps [31] as follows:

$$\begin{cases} x_{i+1} = \mu_1 x_i (1 - x_i) + \gamma_1 y_i^2 \\ y_{i+1} = \mu_2 y_i (1 - y_i) + \gamma_2 (x_i^2 + x_i y_i) \end{cases}. \tag{8}$$

When $2.75 < \mu_1 < 3.4$, $2.75 < \mu_2 < 3.45$, $0.15 < \gamma_1 < 0.21$, $0.13 < \gamma_2 \le 0.15$, the system is in a chaotic state and can generate two sequences $\mathbf{p}$ and $\mathbf{q}$ of size N^2 elements in the interval (0,1). We set $\gamma_1 = 0.19$ and $\gamma_2 = 0.14$ due to a small value range and the other parameters are used for secret keys. The sequences $\mathbf{p}$ and $\mathbf{q}$ are then changed into the matrices $\mathbf{P}$ and $\mathbf{Q}$ of size $N \times N$, respectively. Moreover, the matrix $\mathbf{E}$ is defined as

$$\mathbf{E} = \lambda\mathbf{P} + (1 - \lambda)\mathbf{Q}, \tag{9}$$

where λ as a key satisfies $0 < \lambda < 1$. Eq. (9) means that the matrix $\mathbf{E}$ is coupled of $\mathbf{P}$ and $\mathbf{Q}$. The coupling effect similar to coupled

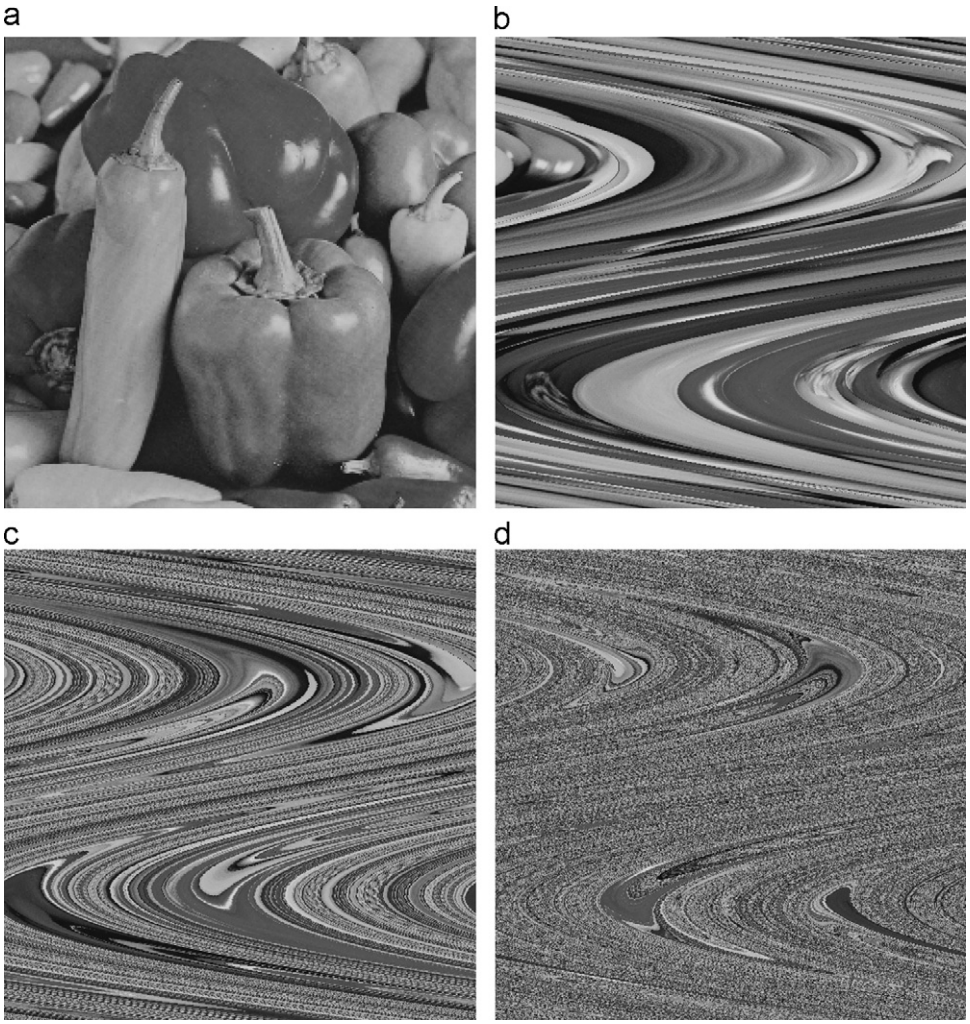

Fig. 2. The test images using DCST for different permutation times: (a) the original image, (b) the test image using DCST once, (c) the test image using DCST three times and (d) the test image using DCST five times.

map lattices endures that each element value of the matrix **E**, like **P** and **Q**, ranges from 0 to 1.

Based on the above description, we can get the chaos-based discrete fractional random transform (CBDFrRT), which not only inherits some similar mathematical characteristics of the fractional Fourier transform such as linearity, unitarity, index additivity, multiplicity and Parseval energy conservation, but also develops some properties of chaotic system such as pseudo-randomness and sensitivity to initial conditions and control parameters.

2.3. The encryption procedures

Our proposed double image encryption scheme is illustrated in Fig. 1(a) and the detailed procedures are described as follows:

1) With no loss of generality, we assume that the original image is an $N \times N$ image. Otherwise, we pad the image by replication of the left-most column and the bottom row to make sure that the number of rows and columns in the image are both a multiple of N. The padded image is then divided into matrices of size $N \times N$, each of which will be encrypted separately. Let $\mathbf{I}_1$ and $\mathbf{I}_2$ of size $N \times N$ denote the two original images normalized with maxima as 1. DCST in Eq. (2) as the pixel scrambling operation is applied $c(c > 5)$ times to the two original images. The scrambled result DCST($\mathbf{I}_1$) is then encoded into a phase-only matrix $\exp[i\pi\mathrm{DCST}(\mathbf{I}_1)]$, which is multiplied by the other scrambled result DCST($\mathbf{I}_2$) to obtain the synthesized input signal
$$\mathbf{I} = \mathrm{DCST}(\mathbf{I}_2) \odot \exp[i\pi\mathrm{DCST}(\mathbf{I}_1)], \tag{10}$$
where $\odot$ represents the element-by-element multiplication.
2) Iterate CSM in Eq. (1) to generate two vectors m and n with N^2 elements, which are further transformed into two matrices A and B, respectively. Next, **A** and **B** are utilized to construct two chaotic random phase masks, namely,
$$\mathbf{M}_1 = \exp(i\mathbf{A}), \quad \mathbf{M}_2 = \exp(i\mathbf{B}). \tag{11}$$
3) Generate the kernel transforms of CBDFrRT by calculating Eqs. (7)–(9) and (5) in turn. As shown in Fig. 2, double random phase encoding is also used in the proposed scheme and the final output encrypted image **C** can be obtained by
$$\mathbf{C} = \Re^b[\Re^a(\mathbf{I} \odot \mathbf{M}_1) \odot \mathbf{M}_2]. \tag{12}$$

The decryption process is depicted in Fig. 1(b), which is similar to that of the encryption process but in the reversed order. It should be paid attention to the two main steps:

1) The decrypted synthesized signal **I** can be obtained by using the inverse of double random phase as follows:
$$\mathbf{I} = \Re^{-a}[\Re^{-b}(\mathbf{C}) \odot \mathbf{M}_2^*] \odot \mathbf{M}_1^*. \tag{13}$$

2) The obtained images after decryption can be respectively expressed as

$$\mathbf{I}_1 = \mathrm{DCST}^{-1}\left|\arg(\mathbf{I})/\pi\right|, \tag{14}$$

$$\mathbf{I}_2 = \mathrm{DCST}^{-1}\left|\mathbf{I}\right|, \tag{15}$$

where DCST^{-1} stands for the inverse transform of DCST.

3. Simulation results and performance analysis

Numerical simulations have been performed on a Matlab 7.10.0 (R2010a) platform to verify the performance of the proposed scheme. The two original images with "Peppers" (256×256) and "Lena" (256×256) is encrypted using the secret keys ($\varepsilon=3.6522$,$m_0=0.3567$ and $n_0=3.1415$ in Eq. (1), $\xi=128$ in Eq. (2), $x_0=0.0954$, $y_0=0.9584$, $\mu_1=3.0231$ and $\mu_2=2.9974$ in

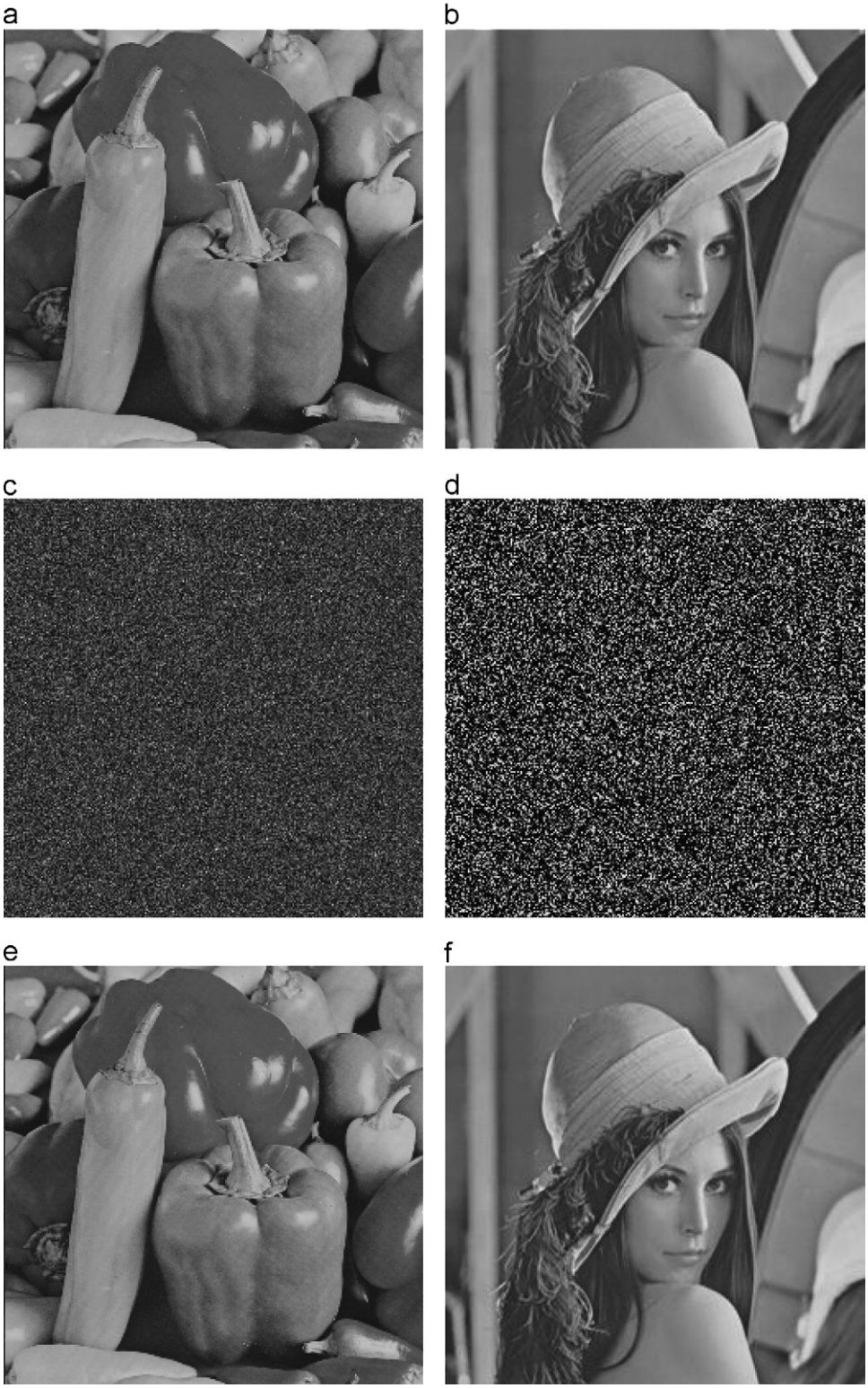

Fig. 3. Encryption and decryption results: (a) original image "Peppers", (b) original image "Lena", (c) amplitude of the encrypted image, (d) phase of the encrypted image, (e) decrypted image "Peppers", and (f) decrypted image "Lena".

Eq. (8), $\lambda=0.2525$in Eq. (9), $a=0.3661$ and $b=0.2666$ in Eq. (12)). The encryption and decryption results are given in Fig. 3.

3.1. Key space analysis

The size of key space is the total number of different keys used in the encryption. With respect to an ideal cryptosystem, it should be large enough to make brute-force attacks infeasible. Furthermore, the size of the key space should not be smaller than 2^{100} to provide a high level of security. In our scheme, if the precision is 10^{-14}, the key space size is over 2^{465}. When two rounds or more rounds are used in the encryption process, it will increase rapidly. It shows that the size is enormous enough to resist all kinds of brute-force attacks.

3.2. Statistical analysis

Fig. 4(a)–(d) is the histograms for the amplitude, the phase, the real part and the imaginary part of the encrypted image. Moreover, more pairs of images are chosen as test images whose histograms are similar to Fig. 4(a)–(d), respectively. Accordingly, we conclude that the different encrypted images have consistent statistical properties. That is to say, the values of the encrypted image are subject to Rayleigh distribution for the amplitude, to uniform distribution for the phase, to normal distribution for the real and imaginary parts. Thus, it does not provide any useful information for the opponents to perform any statistical analysis attack on the encrypted image.

The self-correlation coefficient of an image is defined as

$$r_{pq}=\left|\frac{N\sum_{i=1}^{N}(p_iq_i)-\sum_{i=1}^{N}q_i\sum_{i=1}^{N}q_i}{\sqrt{\left(N\sum_{i=1}^{N}p_i^2-\left(\sum_{i=1}^{N}p_i\right)^2\right)\left(N\sum_{i=1}^{N}q_i^2-\left(\sum_{i=1}^{N}q_i\right)^2\right)}}\right|, \tag{16}$$

where p_i and q_i are the values of two adjacent pixels in the image and N is the total number of pixels selected from the image for the calculation. We randomly selected 2000 pairs of two adjacent pixels in horizontal, vertical and diagonal directions, respectively, and the corresponding results are given in Table 1. One can see that the self-correlation is much weaker than that of the original two images. Therefore, this can further confirm that our scheme has strong capability of resisting statistical analysis

3.3. Key sensitivity analysis

Apparently, the security of the proposed scheme is mainly determined by the initial values and parameters of the chaotic systems and the fractional orders of the CBDFrRT. To evaluate the key sensitivity, the decryption is repeated with a tiny alteration introduced in one of the correct keys each time. Three types of tests on the sensitivity of the secret initial values and parameters, i.e., $m_0=0.3567+10^{-14}$ in Eq. (1), $\xi=128+1$ in Eq. (2) and $\mu_1=3.0231+10^{-14}$ in Eq. (8) are performed. The corresponding decrypted images listed in Fig. 5 indicate that any slight fluctuation will lead to a wrong decryption.

In order to further measure the sensitivity of fractional orders, the mean square error (MSE) function between the decrypted

Table 1
Self-correlation coefficients of the original and encrypted images.

Direction	Peppers	Lena	Encrypted image
Horizontal	0.9506	0.9807	0.0117
Vertical	0.9467	0.9508	0.0183
Diagonal	0.9345	0.9211	0.0255

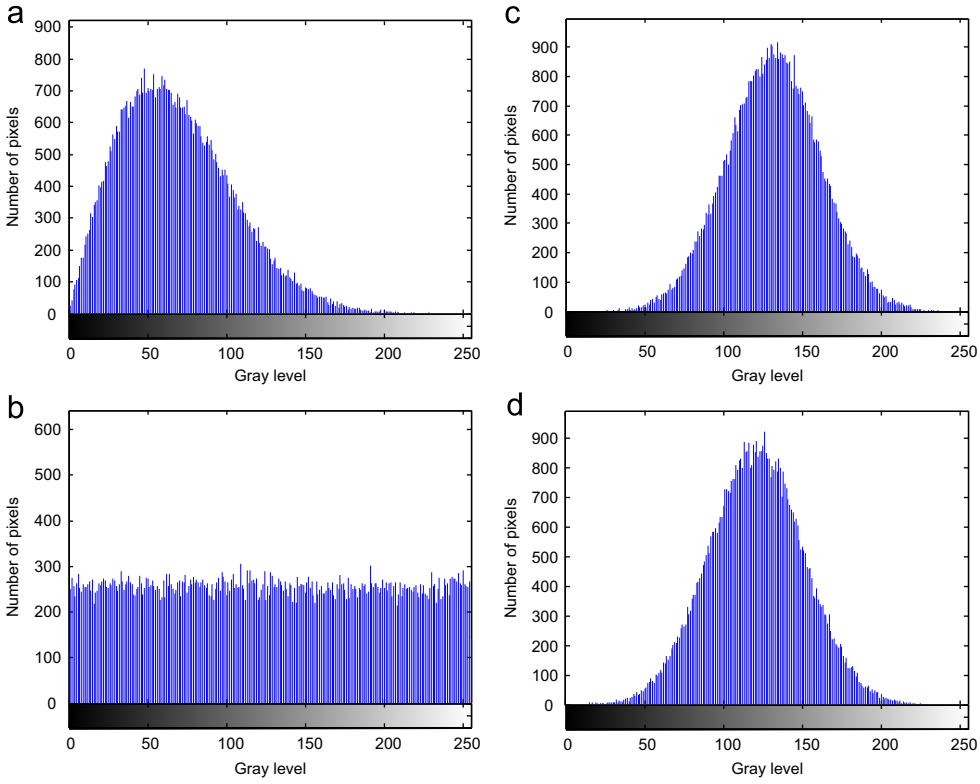

Fig. 4. Histograms: (a) histogram of the amplitude, (b) histogram of the phase, (c) histogram of the real part, and (d) histogram of the imaginary part.

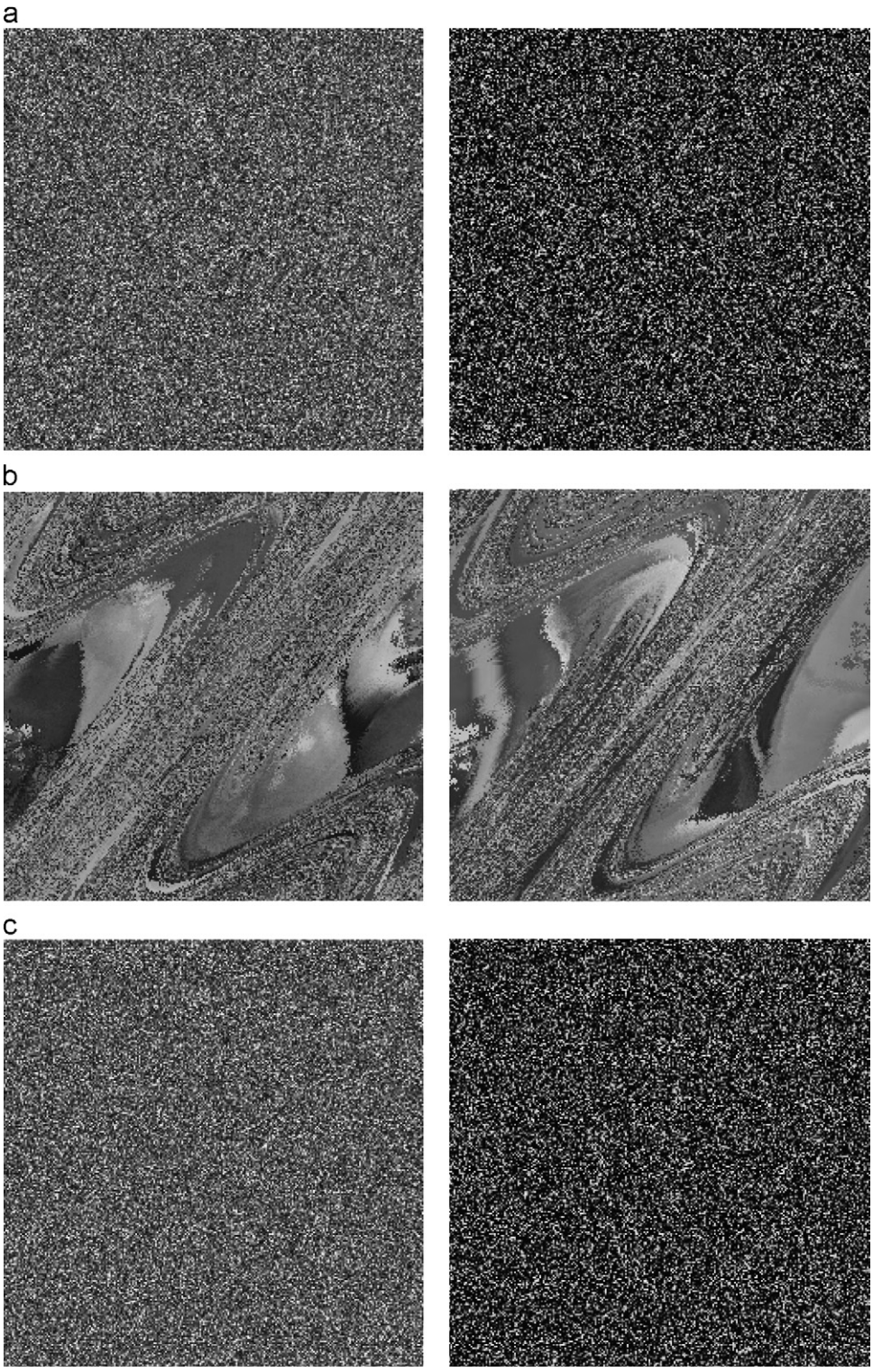

Fig. 5. Decrypted images using wrong secret keys: (a) $m_0=0.3567+10^{-14}$ in Eq. (1), (b) $\xi=128+1$ in Eq. (2), and (c) $\mu_1=3.0231+10^{-14}$ in Eq. (8).

image $I'$and the original image I is calculated as follows:

$$MSE=\frac{1}{MN}\sum_{p=1}^{M}\sum_{q=1}^{N}\left|I'(p,q)-I(p,q)\right|^2, \tag{17}$$

where $M\times N$ are the size of the image.

Fig. 6 shows the MSE curves for different fraction orders with respect to a and b. It can be seen that the MSE value approximates to zero when the fractional orders approach to the correct one. If there is a deviation from the correct order a or b, the MSE decreases rapidly. This implies that the fractional order possesses a high sensitivity.

3.4. Robustness analysis

One important requirement in the process of image communication is the robustness of a cryptosystem against noise, such as salt & pepper. The encrypted image is affected by salt & pepper noise with different percent, respectively, and its corresponding

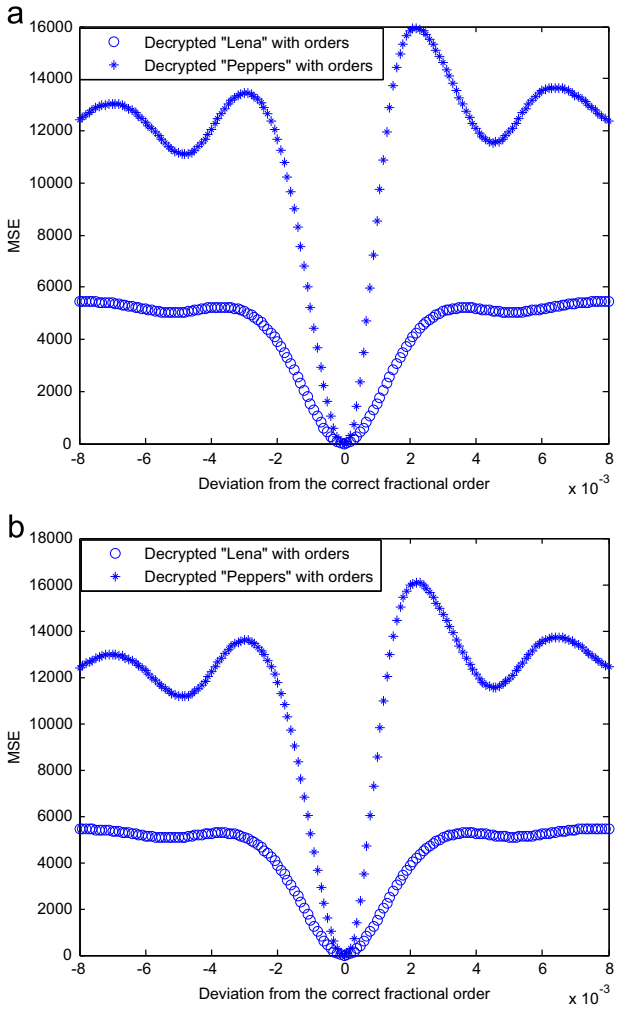

Fig. 6. MSE versus the deviation of the correct orders: (a) MSE versus the deviation of the correct order $a=0.3661$ and (b) MSE versus the deviation of the correct order $b=0.2666$.

decrypted images are shown in Fig. 7. In comparison with the original images, the decrypted images maintain the overall original image information for the human eye. In addition, the quality of the decrypted image is also measured by calculating the MSE in Eq. (17) and the peak signal-to-noise ratio (PSNR) expressed as Eq. (18).

$$\mathrm{PSNR} = 10\log_{10}\left(\frac{255\times 255}{MSE}\right)(dB). \tag{18}$$

To use the MSE and PSNR values for evaluating the quality of the decrypted image, the simulation results are listed in Tables 2 and 3, respectively. The test results show that the decrypted images can be recognized despite of some noise interference and are tolerated with a certain range of noise level. The quality of the decrypted image decreases as the noise level increases.

On the other hand, the robustness test of the proposed scheme is also verified against occlusion attack on encrypted image with 25%, 50% and 70%. Occlusion sizes are shown in Fig. 8(a), (d) and (g), respectively, and corresponding recovered image are displayed in Fig. 8(b, c), (e, f), and (h, i), respectively. From these figures we can see that the retrieved images can be recognized without doubt in all cases, and this method has certain robustness against occlusion attack.

3.5. Potential attacks analysis

Based on Kerckhoff's principle, one should always assume that the adversary knows the encryption/decryption algorithm. The resistance of the cipher to attack must be based only on the secrecy of the key. Usually, there are four potential types of attacks:

Cipher only attack: the adversary has access to only some ciphertext.
Known plaintext attack: the adversary has access to some plaintext/ciphertext pairs in addition to the intercepted ciphertext that he or she wants to break.
Chosen plaintext attack: it is similar to the known-plaintext attack, but the plaintext/ciphertext pairs have been chosen by the adversary.

Fig. 7. The encrypted image is affected by salt & pepper noise with different percents, respectively, and its corresponding decrypted images: (a) 0.1% salt & pepper noise, (b) 0.5% salt & pepper noise, (c) 1% salt & pepper noise, and (d) 5% salt & pepper noise.

Chosen ciphertext attack: it is similar to the chosen-plaintext attack, except that the adversary chooses some cipher and decrypts it to form a ciphertext/plaintext pair.

Apparently, chosen plaintext attack is the most powerful attack. If a cryptosystem can resist this attack, it can resist other types of attack. As to optical encryption, Frauel and Castro give the resistance of the double random phase encryption against various attacks [32]. The results verified that double random phase encryption is susceptible to chosen and known plaintext attacks. This is mainly due to the linearity of double random phase encryption only. However, in the proposed scheme, not only chaos-based discrete fractional random transform makes the algorithm more complex, but also discrete Chirikov standard transform strengthens the nonlinearity. Thus, the proposed algorithm can resist these classical types of attacks.

Table 2
MSE performance.

Salt & pepper noise	0.1%	0.5%	1.0%	5%
Decrypted "Peppers"	29.7694	145.0776	289.1082	1397.1740
Decrypted "Lena"	38.1496	231.2067	437.1599	1660.8500

Table 3
PSNR performance.

Salt & pepper noise	0.1%	0.5%	1.0%	5%
Decrypted "Peppers"	33.3931	26.5148	23.5202	16.6783
Decrypted "Lena"	32.3159	24.4908	21.7244	15.9275

4. Conclusion

In this paper, we construct a new discrete fractional random transform based on 2D chaotic logistic maps and two chaotic random masks resulting from Chirikov standard map. Then, we propose a double optical image encryption method with detailed analyses of feasibility and security. Discrete Chirikov standard map and double random phase coding are utilized to scramble the pixel positions and change the pixel values, respectively, which is equivalent to the confusion–diffusion architecture in the cryptography. The keys depend mainly on the initial values and parameters of chaotic maps and the orders of the transform. Simulation analyses show that the proposed scheme has the following special advantages: the key space is enormous enough to resist all kinds of brute-force attacks; the scheme has strong capability of resisting statistical analysis; the fractional order

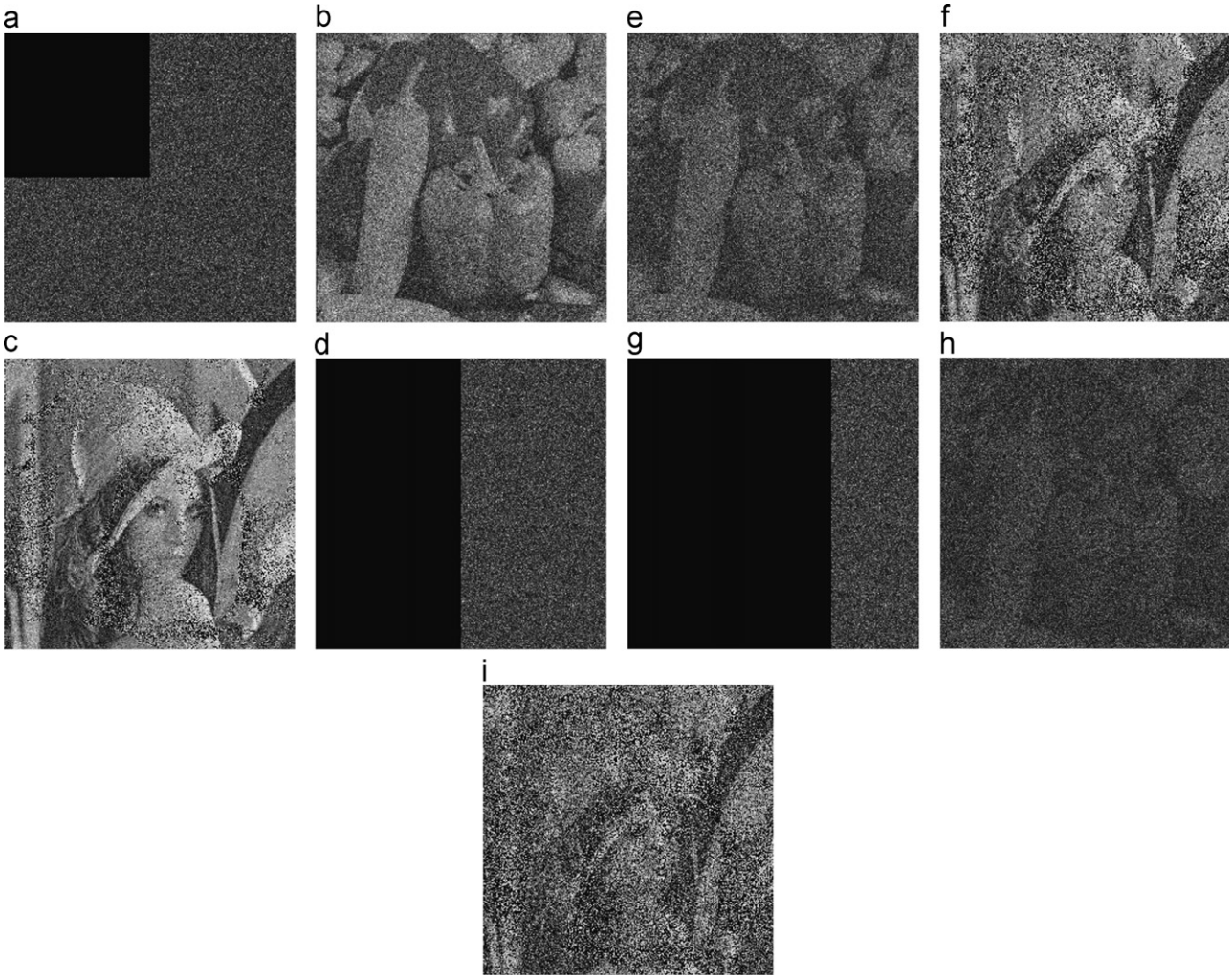

Fig. 8. Robustness against occlusion attack: (a) with 25% occlusion, (b) corresponding recovered "Peppers" image from (a), (c) corresponding recovered "Lena" image from (a), (d) with 50% occlusion, (e) corresponding recovered "Peppers" image from (d), (f) corresponding recovered "Lena" image from (d), (g) with 75% occlusion, (h) corresponding recovered "Peppers" image from (g), and (i) corresponding recovered "Lena" image from (g).

possesses a high sensitivity; the scheme is tolerated with a certain range of noise level; the scheme can resist some classical types of attacks such as known plaintext attack and chosen plaintext attack.

Acknowledgment

The work was funded by the Natural Science Foundation Project of CQ CSTC (Grant no. 2011jjjq40001), the National Natural Science Foundation of China (Grant nos. 61070246 and 61103211), the Graduate Innovation Foundation of Chongqing University (Grant no. CDJXS12180009) and the Project no. CDJZR10180003 supported by the Fundamental Research Funds for the Central Universities.

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] Hennelly B, Sheridan JT. Optical image encryption by random shifting in fractional Fourier domains. Opt Lett 2003;28:269–71.
[3] Li H, Wang Y. Information security system based on iterative multiple-phase retrieval in gyrator domain. Opt Laser Technol 2008;40:962–6.
[4] 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.
[5] Li H. Image encryption based on gyrator transform and two-step phase-shifting interferometry. Opt Lasers Eng 2009;47:45–50.
[6] Liu ZJ, Guo Q, et al. Double image encryption by using iterative random binary encoding in gyrator domains. Opt Express 2010;18:12033–43.
[7] Jin J. An image encryption based on elementary cellular automata. Opt Lasers Eng 2012;50:1836–43.
[8] Liu Z, Li S, Yang M, Liu W, Liu S. Image encryption based on the random rotation operation in the fractional Fourier transform domains. Opt Lasers Eng 2012;50:1352–8.
[9] Liu Z, Li S, Liu W, Wang Y, Liu S. Image encryption algorithm by using fractional Fourier transform and pixel scrambling operation based on double random phase encoding. Opt Lasers Eng 2013;51:8–14.
[10] Xiao D, Liao XF, Wei PC. Analysis and improvement of a chaos-based image encryption algorithm. Chaos, Soliton Fractals 2009;40:2191–9.
[11] Wong KW, Kwok B, Law W. A fast image encryption scheme based on chaotic standard map. Phys Lett A 2008;372:2645–52.
[12] Xiao D, Shih FY. Using the self-synchronizing method to improve security of the multi chaotic systems-based image encryption. Opt Commun 2010;283:3030–6.
[13] Zhou Q, Wong KW, Liao XF, Xiang T, Hu Y. Parallel image encryption algorithm based on discretized chaotic map. Chaos Solitons Fractals 2008;38:1081–92.
[14] Xiao D, Liao XF, Deng SJ. A novel key agreement protocol based on chaotic maps. Inf Sci 2007;177:1136–42.
[15] Wang Y, Wong KW, Liao XF, Chen GR. A new chaos-based fast image encryption algorithm. Appl Soft Comput 2011;11:514–22.
[16] Xiang T, Wong KW, Liao XF. A novel symmetrical cryptosystem based on discretized two-dimensional chaotic map. Phys Lett A 2007;364:252–8.
[17] Singh N, Sinha A. Optical image encryption using fractional Fourier transform and chaos. Opt Lasers Eng 2008;46:117–23.
[18] Singh N, Sinha A. Gyrator transform-based optical image encryption, using chaos. Opt Lasers Eng 2009;47:539–46.
[19] Li HJ, Wang YR. Double-image encryption based on discrete fractional random transform and chaotic maps. Opt Lasers Eng 2011;49:753–7.
[20] Lang J, Tao R, Wang Y. Image encryption based on the multiple-parameter discrete fractional Fourier transform and chaos function. Opt Commun 2010;283:2092–6.
[21] Zhou NR, Wang YX, et al. Novel single-channel color image encryption algorithm based on chaos and fractional Fourier transform. Opt Commun 2011;284:2789–96.
[22] Lang J. Image encryption based on the reality-preserving multiple-parameter fractional Fourier transform and chaos permutation. Opt Lasers Eng 2012;50:929–37.
[23] Liu ZJ, Xu L, et al. Color image encryption by using Arnold transform and color-blend operation in discrete cosine transform domains. Opt Commun 2011;284:123–8.
[24] Liu ZJ, Gong M, et al. Double image encryption by using Arnold transform and discrete fractional angular transform. Opt Lasers Eng 2012;50:248–55.
[25] Abutrrab MR. Securing color information using Arnold transform in gyrator transform domain. Opt Lasers Eng 2012;50:772–9.
[26] Chen W, Quan C, Tay CJ. Optical color image encryption based on Arnold transform and interference method. Opt Commun 2009;282:3680–5.
[27] Rannou F. Numberical study of discrete plane area-preserving mapping. Astron Astrophys 1974;31:289–301.
[28] Litchenberg AJ, Lieberman MA. Regular and stochastic motion. New York: Springer; 1983.
[29] Fu C, Chen JJ, et al. A chaos-based digital image encryption scheme with an improved diffusion strategy. Opt Express 2012;20:2363–78.
[30] Liu ZJ, Zhao HF, Liu ST. A discrete fractional random transform. Opt Commun 2005;255:357–65.
[31] Zhang Q, Guo L, Wei XP. Image encryption using DNA addition combing with chaotic maps. Math Comput Modelling 2010;52:2028–35.
[32] Frauel Y, Castro A, et al. Resistance of the double random phase encryption against various attacks. Opt Express 2007;15:10253–65.