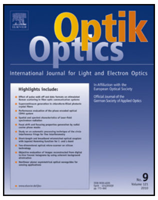
Optik 125 (2014) 4474–4479

Contents lists available at ScienceDirect

Optik

journal homepage: www.elsevier.de/ijleo



Triple color images encryption algorithm based on scrambling and the reality-preserving fractional discrete cosine transform

Jianhua Wu[a,*], Fangfang Guo[a], Yaru Liang[b], Nanrun Zhou[a]

[a] *Department of Electronic Information Engineering, Nanchang University, China*
[b] *School of Mechatronic Engineering, Nanchang University, China*

ARTICLE INFO

Article history:
Received 8 August 2013
Accepted 12 February 2014

Keywords:
Image encryption
Cyclic shift
Arnold transform
Reality-preserving fractional discrete cosine transform
Generating sequence

ABSTRACT

An image encryption algorithm to secure three color images simultaneously by combining scrambling with the reality-preserving fractional discrete cosine transform (RPFrDCT) is proposed. The three color images to be encrypted are converted to their indexed formats by extracting their color maps, which can be considered as the three components of a color image. These three components are affected each other by scrambling the interims obtained from vertically and horizontally combining the three indexed formats with the help of the chaos-based cyclic shift. The three scrambled components are separately transformed with the RPFrDCT, in which the generating sequences are determined by the Chirikov standard chaotic map. Arnold transform is used to further enhance the security. Due to the inherent properties of the chaotic maps, the cipher keys are highly sensitive. Additionally, the cipher image is a single color image instead of three color ones, and is convenient for display, storage and transmission due to the reality property of RPFrDCT. Numerical simulations are performed to show the validity of the proposed algorithm.

1. Introduction

The past few decades have witnessed the rapid development of the network multimedia, communication and propagation techniques and the exchange of digital information especially images has also greatly increased. Image encryption has become a major task for information security since the issues about illegal data access on Internet are becoming more and more serious. Since optical image encryption system based on double random phase encoding (DPRE) by the Fourier transform was firstly proposed by Refregier and Javidi [1], it has been extended to other optical transform domains [2–10]. With the emergence of color images, color image encryption [11–16] has become an important issue because of the usefulness of the color information in practical applications. The most common method is the multichannel decomposition based on the RGB model or HSI model, however, the complexity and the cost will be increased since multiple channels must be involved during the encryption and transmission processes. A representative method of single-channel color image encryption is based on the digital transformation of the color image to indexed format [16], which is more compact and reliable than the multichannel ones.

As a new concept in image encryption field, multiple-image encryption has attracted much attention, which encrypts several different images together. Situ and Zhang [17] firstly employed wavelength multiplexing to realize multiple-image encryption. The qualities of the corresponding decrypted images in the algorithm, however, are not perfect due to the cross-talk effects between images. Subsequently, various multiple-image encryption schemes have been designed [18–28]. The most commonly used for two images is based on the complex function, in which two original images are respectively regarded as the real/amplitude and the imaginary/phase of the complex function. Although it can realize multiple-image encryption through the complex function, it may not be implemented in real time since the encrypted images contain both amplitude information and phase information, which makes it difficult to display, store and transfer. Wang and Zhao [27,28] proposed the multiple-image encryption method using the phase-truncation and phase retrieval, which makes the cryptosystem nonlinear and the output real-valued. However, the truncated phases as the cipher keys, whose size is the same as the cipher images, need to be transferred to the receivers for decryption, giving rise to increase of the burden of transmission. Besides, the phase-retrieval process is very time consuming.

* Corresponding author at: Department of Electronic Information Engineering, Nanchang University, 999 Rd. Xuefu, Honggutan New District, Nanchang 330031, P. R. China. Tel.: +86 791 83969336; fax: +86 791 83969338.

E-mail addresses: jhwu@ncu.edu.cn (J. Wu), hellosuger@qq.com (F. Guo), liangyaru@126.com (Y. Liang), nrzhou@ncu.edu.cn (N. Zhou).

http://dx.doi.org/10.1016/j.ijleo.2014.02.026
0030-4026/© 2014 Elsevier GmbH. All rights reserved.

To display, store and transfer images conveniently, in this paper, we present a new encryption algorithm to secure three color images simultaneously by use of scrambling and the reality-preserving fractional discrete cosine transform (RPFrDCT). The encrypted image is a single real-valued color image, which is convenient for display, storage and transmission. Firstly, the three color images to be encrypted are separately converted to their indexed formats by extracting their color maps, which can be considered as the three components of a color image. Then two scrambling schemes are implemented to make these three components affect each other by scrambling the interims obtained from vertically and horizontally combining the three indexed formats with the help of the chaos-based cyclic shift. Next, the three scrambled components are separately transformed with the RPFrDCT, in which the generating sequences are determined by the chaotic map. Finally, Arnold transform is used to further enhance the security. Due to the inherent properties of the chaotic maps, the system is highly sensitive to the cipher keys. Numerical simulation results show the feasibility and the validity of the proposed algorithm.

The rest of this paper is organized as follows. Section 2 reviews the principles of the reality-preserving fractional discrete cosine transform, the concept of true color and indexed color images, the Chirikov standard chaotic map, and the Arnold transform. The proposed encryption algorithm is also described in Section 2. Simulations and discussion are given in Section 3. Finally, a brief conclusion is drawn in last section.

2. Principles

2.1. Definition of the reality-preserving fractional discrete cosine transform

The fractional discrete cosine transform (FrDCT) is a generalization of the DCT. In current documents, even though several versions of fractional cosine transform have been derived, the FrDCT [31] different from those defined in [29,30] possesses the mathematical properties of reality in addition to the fundamental properties such as linearity, unitarity and additivity. And the reality is of importance for image encryption, which ensures the outputs are real for real inputs.

The FrDCT is derived based on the eigen-decomposition and eigenvalue substitution of the DCT-II kernel, which is denoted as:

$$\mathbf{C} = \left\| \frac{1}{\sqrt{N}} \varepsilon_k \cos\left(2\pi \frac{(2n+1)k}{4N}\right) \right\| \tag{1}$$

where $n, k = 0, 1, \ldots, N-1$ and $\varepsilon_0 = 1$, $\varepsilon_k = \sqrt{2}$ for $k > 1$.

The eigen decomposition of an $N \times N$ DCT-II matrix $\mathbf{C}$ can be expressed by:

$$\mathbf{C} = \mathbf{U}\Lambda\mathbf{U}^* = \sum_n \mathbf{U}_n \, e^{j\varphi_n} \tag{2}$$

where $\mathbf{U}$ is a unitary matrix, composed of columns (eigenvectors) $\mathbf{u}_n, \mathbf{u}_m^*\mathbf{u}_n = \delta_{mn}, \mathbf{U}_n = \mathbf{u}_n\mathbf{u}_n^*$, and $\mathbf{\Lambda}$ is the diagonal matrix with diagonal entries, i.e. eigenvalues λ_n, $\lambda_n = e^{j\varphi_n}$ with $0 < \varphi_n < \pi$.

The fractional discrete cosine transform matrix $\mathbf{C}_\alpha$ can be written by substituting the eigenvalues λ_n with their αth powers λ_n^α as follows:

$$\mathbf{C}_\alpha = \mathbf{U}\Lambda^\alpha\mathbf{U}^* \tag{3}$$

The matrix $\mathbf{C}_\alpha$ given by (3) can be rewritten in an alternative form in accordance with the eigenstructure of matrix $\mathbf{C}$:

$$C_\alpha = 2\mathrm{Re}\left[\sum_{n=1}^{K} \mathbf{U}_n \lambda_n^\alpha\right] + \mathbf{V}_1(1)^\alpha + \mathbf{V}_{-1}(-1)^\alpha \tag{4}$$

where $\mathbf{U}_n = \mathbf{u}_n\mathbf{u}_n^*$, $K = (N - \mu_1 - \mu_{-1})/2$, μ_1 and μ_{-1} represent the multiplicities of the eigenvalues 1 and -1, respectively. $\mathbf{V}_1$ collects the μ_1 matrices $\mathbf{U}_n$ corresponding to the eigenvalue 1 and similarly for $\mathbf{V}_{-1}$.

If $N = 4N_0$, N_0 is an integer, the absence of the $(\pm 1)^\alpha$ in (4) guarantees that $\mathbf{C}_\alpha$ becomes a real-valued matrix and can be written as:

$$\mathbf{C}_\alpha = 2\mathrm{Re}\left[\sum_{n=1}^{N/2} \mathbf{U}_n \, e^{j\omega_n\alpha}\right] = \sum_{n=1}^{N/2} (\mathbf{A}_n \cos\omega_n\alpha + \mathbf{B}_n \sin\omega_n\alpha) \tag{5}$$

$$\omega_n = \varphi_n + 2\pi q_n, n = 1, 2, \ldots, \frac{N}{2}, \quad 0 < \varphi_n < \pi, \tag{6}$$

where $\mathbf{A}_n = 2\mathrm{Re}[\mathbf{U}_n]$, $\mathbf{B}_n = -2\mathrm{Im}\,[\mathbf{U}_n]$, q_n is an arbitrary sequence of integers, and we call the sequence $\mathbf{q} = (q_1, q_2, \ldots, q_{N/2})$ the generating sequence (GS) of the FrDCT, which is introduced due to the multiplicity of the roots of the αth power of λ_n. Different choices of q_n lead to different matrices $\mathbf{C}_\alpha$ and, hence, to different FrDCT definitions. So taking the GS $\mathbf{q}$ as secret key can provide a huge key space. Readers can refer to [31] for more information about $\mathbf{q}$. The expansion of the FrDCT for a two-dimensional signal is straightforward and simple through two FrDCTs successively by rows and by columns.

2.2. Concept of true and indexed color images

A true color image can be treated as a three-dimensional (3-D) matrix with each pixel as a triplet corresponding to the values of the primary color components in RGB model, while an indexed color image consists of two 2-D matrices, i.e. an image matrix and a color map matrix. The color map is an $M \times 3$ array of class double containing floating-point values in the range [0, 1], whose length M is equal to the numbers of colors it defines. For example, M is 256 for an 8-bit color system. Each row of the color map specifies the red, green and blue components of a single color. An indexed image directly maps the pixel intensity values to the color map values. The color of each image pixel is determined by using the corresponding value of the image matrix as a pointer into color map [24]. After representing an RGB color image with its indexed format, the encryption of the color image can be simplified. Since the color map is uniquely defined for all color images in the same color system and only an indexed image needs to be encrypted, which is straightforward compared with the multichannel encryption. The color image can be retrieved after adding the color map to the decrypted indexed image [16].

2.3. Chirikov standard map

Chirikov standard map (CSM) [26] is an invertible area-preserving chaotic map for two canonical dynamical variables from a square with side 2π onto itself, i.e.:

$$\begin{cases} x_{i+1} = (x_i + y_i) \bmod 2\pi \\ y_{i+1} = (x_i + \delta \sin(x_i + y_i)) \bmod 2\pi \end{cases} \tag{7}$$

where $\delta > 0$ is the control parameter, and x_i and y_i both take real values in the range $[0, 2\pi)$ for all i. In this paper, the Chirikov standard map will be used twice, which respectively generates the random sequences to be applied to the cyclic shift and the generating sequences.

2.4. Arnold transform

As a simple scrambling method, Arnold transform (AT) commonly known as cat face transform is widely used. The transform is a process of clipping and splicing that realigns the pixel matrix of

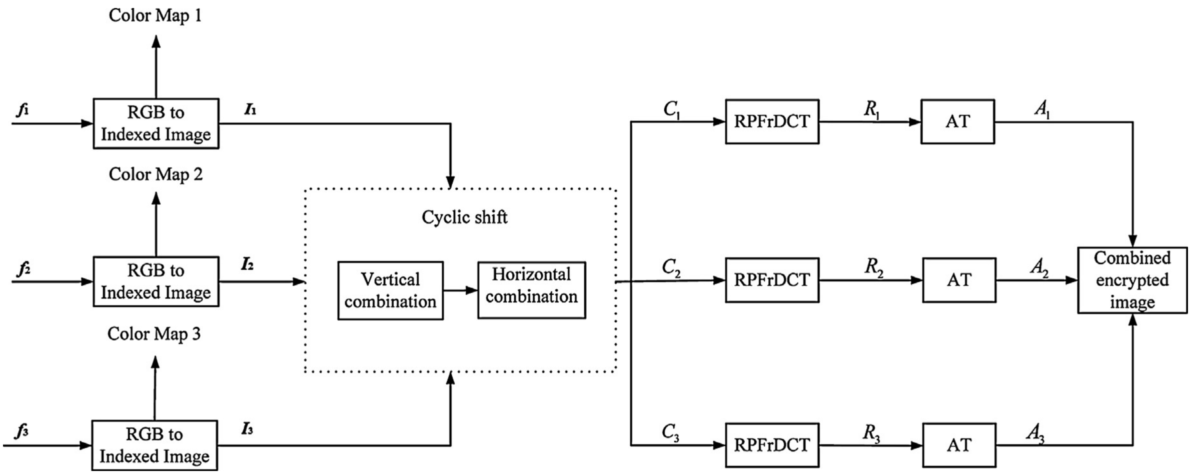


Fig. 1. The flowchart of the proposed encryption algorithm.

digital image. A digital image sized $N \times N$ can be scrambled by the following discrete form [14,20]:

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \bmod N \tag{8}$$

where x, y and x', y' represent the positions of image pixels shifted before and after, respectively. AT is an equal-area transform with periodicity. The period of the transform depends on the size of the image. If an image is scrambled by AT for t times, then the image can be recovered by applying the same AT of $(T - t)$ times, where T is the period. That is, the receiver cannot recover the image correctly without knowing the iteration number t and the period T.

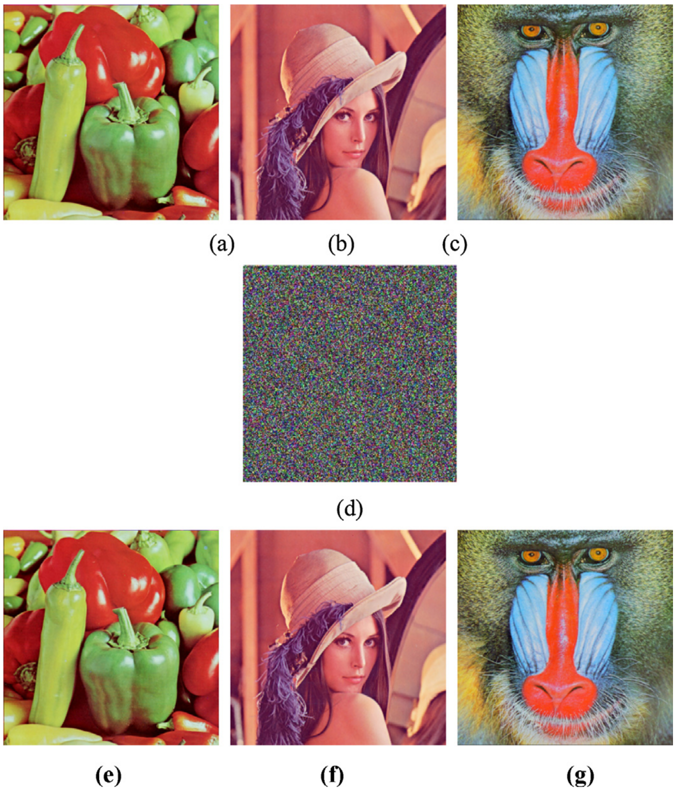


Fig. 2. (a)–(c) Original RGB images (from left to right): Peppers, Lena and Baboon; (d) encrypted color image; (e)–(g) decrypted images with correct keys: Peppers, Lena and Baboon.

2.5. Description of the encryption algorithm

In the design of three color images encryption, both scrambling and changing pixel values are considered and utilized. Fig. 1 gives the flowchart of this proposed encryption algorithm and the details are described as follows:

(1) Generation of indexed color images. Read three color images f_1, f_2 and f_3, and convert these three color images to their indexed formats I_1, I_2 and I_3, which are treated as red, green and blue components of a single color image, respectively.

(2) Cyclic shift. Two scrambling schemes are achieved to make these three components affect each other by scrambling the interims obtained from vertically and horizontally combining the three indexed formats successively, with the help of the chaos-based cyclic shift.

Step 1: Iterate Eq. (7) to generate two random sequences of length max$\{3M + 1000, N + 1000\}$ with x_0, y_0. Discard the previous 1000 values to avoid the harmful effect and then obtain the sequences $\mathbf{x}$ of length $3M$ and $\mathbf{y}$ of length N. Further, two new sequences are generated as:

$$\mathbf{X} = \text{floor}(\mathbf{x} \times 10^{14}) \bmod N, \quad \mathbf{Y} = \text{floor}(\mathbf{y} \times 10^{14}) \bmod 3M \tag{9}$$

where floor(z) rounds z to the nearest integer toward minus infinity.

Step 2: Combine three indexed images I_1, I_2 with I_3 vertically and get a new matrix F of size $3M \times N$. Perform the cyclic shift toward the right for each row and the number of shifts is determined by $\mathbf{X}$. After shifting the entire row, do the cyclic shift determined by $\mathbf{Y}$ toward the bottom for each column.

Step 3: Decompose the scrambled matrix obtained in Step 2 into three matrices, then combine these three matrices horizontally and get a new matrix F' of size $M \times 3N$. Do the same chaos-based cyclic shift for each row and each column of the matrix F'. Decompose the obtained new matrix into three matrices C_1, C_2 and C_3.

(3) RPFrDCT. The interims C_1, C_2 and C_3 are encrypted by the reality-preserving fractional discrete cosine transform, in which two generating sequences are determined by chaotic sequences for each row and each column. The specific procedures of C_i $(i = 1, 2, 3)$ encryption are described as follows:

Step 1: Set the initial values x'_0, y'_0 and iterate Eq. (7) max$\left\{1000 + M/2, 1000 + N/2\right\}$ times to get two random sequences. Then select $\mathbf{x}'$ of length $M/2$ and $\mathbf{y}'$ of length $N/2$ and these two sequences are further modified by dividing π such that they are distributed in [0,2).

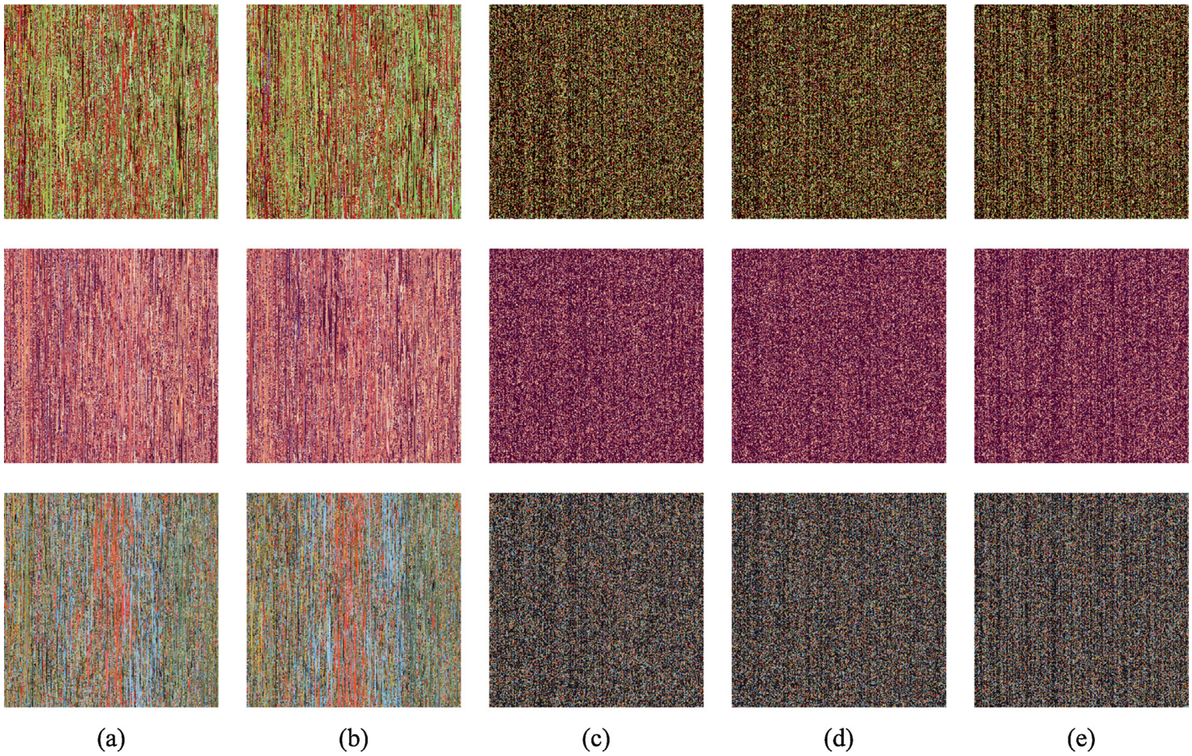


Fig. 3. The decrypted images (each column from top to bottom: Peppers, Lena and Baboon) with incorrect keys: (a) $x_0 = 0.1234 + 10^{-14}$; (b) $y_0 = 0.2345 + 10^{-14}$; (c) $x'_0 = 0.4567 + 10^{-14}$; (d) $y'_0 = 0.5678 + 10^{-14}$; (e) $\delta = 0.3456 + 10^{-14}$.

Step 2: Generate two random generating sequences **q** for the rows and the columns according to (10), respectively,

$$q(n) = \begin{cases} 0, & 0 \leq m(j) \leq 1 \\ 1, & 1 < m(j) < 2 \end{cases}, \quad j = 1, 2, \ldots, L \tag{10}$$

where $m(j)$ is the values of ith state in the random sequence, and L is the length of the random sequence.

Step 3: Set the fractional orders α and β. Then perform two rounds 1-D RPFrDCT using the α, β and corresponding random GS for each row and each column, respectively. The obtained result is denoted as R_i.

(4) Arnold transform. AT is utilized to obtain a scrambled matrix. The iteration numbers are set to be $\mathrm{Num} = \{t_1, t_2, t_3\}$. After AT, combine three results as the red, green and blue components of a color image and get the final cipher color image.

The decryption process is the inverse of the above steps. However, in the final step of decryption, the color maps are added to the segregated images to obtain the original RGB images as the outputs. It is pertinent to mention that the transform fractional orders in the decryption need further modification as $\alpha' = -\alpha$, $\beta' = -\beta$.

3. Simulations and discussion

Numerical simulations are performed to check the validity of the proposed encryption algorithm. Three typical color images sized $256 \times 256 \times 3$ shown in Fig. 2(a)–(c) are chosen as the test plaintexts. The initial values and the control parameters of the Chirikov standard map are set as $x_0 = 0.1234$, $y_0 = 0.2345$, $x'_0 = 0.4567$, $y'_0 = 0.5678$ and $\delta = 0.3456$. The fractional orders and the iteration numbers are set as $\alpha = 0.6867$, $\beta = 0.7278$ and $t_1 = 23$, $t_2 = 45$ and $t_3 = 62$, respectively. The final cipher color image is displayed in Fig. 2(d). The decrypted images with the correct keys are shown in Fig. 2(e)–(g), which demonstrates the lossless decrypted images.

3.1. Key space

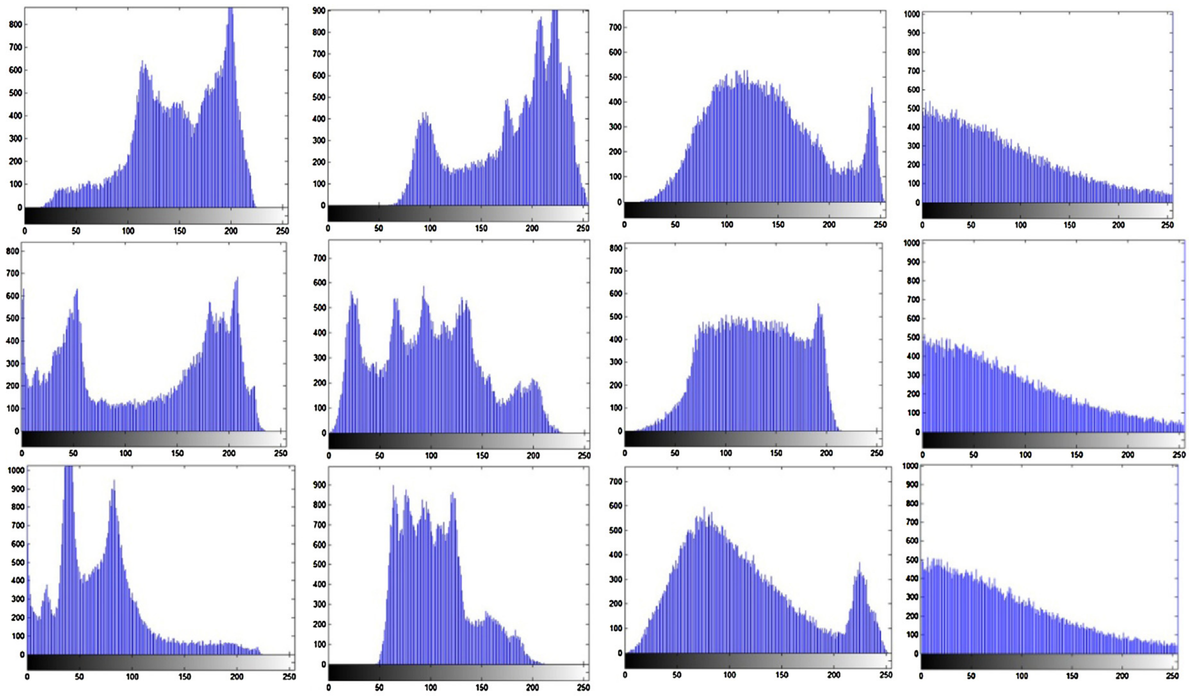
Because of the insensitivity, the fractional orders are not used as the cipher keys. Our encryption algorithm has the following secret keys: (1) given initial values x_0, y_0, x'_0, y'_0 and control parameter δ; (2) iteration numbers t_1, t_2 and t_3. For the initial values and the control parameter of the Chirikov standard map, if the precision is 10^{-14}, then the key space will be 10^{70} and the iteration numbers as well, which is large enough to resist the exhaustive attack.

3.2. Key sensitivity

Fig. 3(a)–(e) illustrates the sensitivity of our algorithm to the corresponding incorrect keys. The decrypted images do not leak any valid information even when the deviation is up to 10^{-14}. Due to the chaotic properties such as the pseudo-randomness and the sensitivity to the initial values and control parameter, a tiny change

Table 1
Correlation coefficients for original images and encrypted image.

	Peppers			Lena			Baboon			Encrypted image		
	R	G	B	R	G	B	R	G	B	R	G	B
Horizontal	0.9686	0.9691	0.9623	0.9603	0.9409	0.9292	0.9488	0.8701	0.9131	0.0200	0.0336	0.0096
Vertical	0.9705	0.9709	0.9640	0.9753	0.9752	0.9560	0.9168	0.8337	0.9173	0.0048	0.0110	−0.0051
Diagonal	0.9319	0.9574	0.9273	0.9349	0.9190	0.8897	0.9065	0.7973	0.8795	−0.0026	−0.0019	0.0143



(a) (b) (c) (d)

Fig. 4. Histograms of the original images and the encrypted image (each column from top to bottom: R channel, G channel and B channel): (a) Peppers; (b) Lena; (c) Baboon; (d) the encrypted image.

of the initial values and control parameter will lead to dramatic change with respect to the sequences of cyclic shift and generating sequences. Thus, the decrypted images with even little mismatched keys are absolutely different from the original plain images.

3.3. *Correlation*

To validate the ability to resist statistical attack, 2000 pairs of two adjacent pixels are randomly selected in horizontal, vertical and diagonal directions of the original images and the encrypted one, respectively. The correlation coefficient is calculated by Eq. (11) and the results are compiled in Table 1.

$$C = \frac{\sum_{i=1}^{N}(x_i-\bar{x})(y_i-\bar{y})}{\sqrt{\left(\sum_{i=1}^{N}(x_i-\bar{x})^2\right)\left(\sum_{i=1}^{N}(y_i-\bar{y})^2\right)}} \qquad (11)$$

where (x_i, y_i) denotes a pair of adjacent pixels, N is the total number of adjacent pixels pairs. $\bar{x} = (1/N)\sum_{i=1}^{N}x_i$ and $\bar{y} = (1/N)\sum_{i=1}^{N}y_i$.

From Table 1, one can see clearly that the correlation coefficients of adjacent pixels in the encrypted image are much lower than those in the original images. That is to say, the attacker cannot obtain any information of the original images though statistical analysis.

3.4. *Histogram*

The histograms of the original images and the encrypted image are displayed in Fig. 4(a)–(d), respectively. It is shown that the histograms of the encrypted image are obviously different from those of the original images, and many tests on the histograms of different encrypted images demonstrate that the histograms are much similar to Fig. 4(d). Thus, the illegal users cannot get any valid information according to the statistical analysis.

4. Conclusion

We have demonstrated a method to encrypt three color images by use of scrambling and the reality-preserving fractional discrete cosine transform, which is a kind of encryption with secrecy of pixel values and pixel positions simultaneously. Each color image is firstly converted to its indexed image. The encryption process is only done to their indexed images, due to the color map is uniquely defined for a given color system. During the encryption, two scrambling schemes are achieved to make these three indexed images affect each other by scrambling the interims obtained from vertically and horizontally combining the three indexed formats with the help of the chaos-based cyclic shift. To strengthen the security of the system, the outputs of the RPFrDCT are further scrambled by the Arnold transform. The designed encryption algorithm fully considers the space domain and the frequency domain, so it is more secure than the pure encryption operation based on the RPFrDCT. The output is real due to the reality property of the RPFrDCT, which makes it convenient to display, store and transfer. The simulation results and discussions demonstrated that this method not only can encrypt and decrypt three color images effectively, but also has large key space to resist the exhaustive attack and sensitivity to the keys thanks to the chaotic properties.

Acknowledgments

This work is supported by the National Natural Science Foundation of China (Grant Nos. 61262084 and 61141007), the Foundation for Young Scientists of Jiangxi Province (Grant No. 20122BCB23002) and the Natural Science Foundation of Jiangxi Province (Grant No. 20122BAB201029).

References

[1] P. Refregier, B. Javidi, Optical image encryption based on input plane and Fourier plane random encoding, Opt. Lett. 20 (1995) 767–769.

[2] G. Unnikrishnan, J. Joseph, K. Singh, Optical encryption by double-random phase encoding in the fractional Fourier domain, Opt. Lett. 25 (2000) 887–889.

[3] S.C. Pei, W.L. Hsue, The multiple-parameter discrete fractional Fourier transform, IEEE Signal Proc. Lett. 13 (2006) 329–332.

[4] Z.J. Liu, S.T. Liu, Random fractional Fourier transform, Opt. Lett. 32 (2007) 2088–2090.

[5] N.R. Zhou, T.J. Dong, J.H. Wu, Novel image encryption algorithm based on multiple-parameter discrete fractional random transform, Opt. Commun. 283 (2010) 3037–3042.

[6] L.F. Chen, D.M. Zhao, Optical image encryption based on fractional wavelet transform, Opt. Commun. 254 (2005) 361–367.

[7] D.M. Zhao, X.X. Li, L.F. Chen, Optical image encryption with redefined fractional Hartley transform, Opt. Commun. 281 (2008) 5326–5329.

[8] R. Tao, J. Lang, Y. Wang, The multiple-parameter discrete fractional Hadamard transform, Opt. Commun. 282 (2009) 1531–1535.

[9] J.H. Wu, L. Zhang, N.R. Zhou, Image encryption based on the multiple-order discrete fractional cosine transform, Opt. Commun. 283 (2010) 1720–1725.

[10] N.R. Zhou, Y.X. Wang, L.H. Gong, Novel optical image encryption scheme based on fractional Mellin transform, Opt. Commun. 284 (2011) 3234–3242.

[11] M. Abuturab, Color image security system based on discrete Hartley transform in gyrator transform domain, Opt. Laser Eng. 51 (2013) 3117–3324.

[12] W. Chen, C. Quan, C.J. Tay, Optical color image encryption based on Arnold transform and interference method, Opt. Commun. 282 (2009) 3680–3685.

[13] N.R. Zhou, Y.X. Wang, L.H. Gong, X.B. Chen, Y.X. Yang, Novel color image encryption algorithm based on the reality preserving fractional Mellin transform, Opt. Laser Technol. 44 (2012) 2270–2281.

[14] L.S. Sui, B. Gao, Color image encryption based on gyrator transform and Arnold transform, Opt. Laser Technol. 48 (2013) 530–538.

[15] H. Liu, H. Nan, Color image security system using chaos-based cyclic shift and multiple-order discrete fractional cosine transform, Opt. Laser Technol. 50 (2013) 1–7.

[16] S.Q. Zhang, M.A. Karim, Color image encryption using double random phase encoding, Microw. Opt. Technol. Lett. 21 (1995) 318–323.

[17] G. Situ, J. Zhang, Multiple-image encryption by wavelength multiplexing, Opt. Lett. 30 (2005) 1306–1308.

[18] M.G. Shan, J. Chang, Z. Zhong, B.G. Hao, Double image encryption based on discrete multiple-parameter fractional Fourier transform and chaotic maps, Opt. Commun. 285 (2012) 4227–4234.

[19] Z. Zhong, J. Chang, M.G. Shan, B.G. Hao, Double image encryption using double pixel scrambling de random phase encoding, Opt. Commun. 285 (2012) 584–588.

[20] X.Y. Shi, D.M. Zhao, Y.B. Huang, J.J. Pan, Multiple color images encryption by triplets recombination combining the phase retrieval technique and Arnold transform, Opt. Commun. 306 (2013) 90–98.

[21] H.J. Li, Y.R. Wang, et al., Double-image encryption by using chaos-based local pixel scrambling technique and gyrator transform, Opt. Laser Eng. 51 (2013) 1327–1331.

[22] Z.J. Liu, J. Dai, X. Sun, S.T. Liu, Triple image encryption scheme in fractional Fourier transform domains, Opt. Commun. 282 (2009) 518–522.

[23] X.Y. Liang, X.Y. Su, et al., Key rotation multiplexing for multiple-image optical encryption in the Fresnel domain, Opt. Laser Technol. 43 (2011) 889–894.

[24] M. Joshi, Chandrashahker, K. Singh, Color image encryption and decryption for twin images in fractional Fourier domain, Opt. Commun. 281 (2008) 5713–5720.

[25] J.H. Wu, X.Z. Luo, N.R. Zhou, Four-image encryption method based on spectrum truncation, chaos and the MODFrFT, Opt. Laser Technol. 45 (2013) 571–577.

[26] Y.S. Zhang, D. Xiao, Double optical image encryption using discrete Chirikov standard map and chaos-based fractional random transform, Opt. Laser Eng. 51 (2013) 472–480.

[27] X.G. Wang, D.M. Zhao, Multiple-image encryption based on nonlinear amplitude-truncation and phase-truncation in Fourier domain, Opt. Commun. 284 (2011) 148–152.

[28] X.G. Wang, D.M. Zhao, Double-image self-encoding and hiding based on phase-truncated Fourier transforms and phase retrieval, Opt. Commun. 284 (2011) 4441–4445.

[29] A.W. Lohmann, D. Mendlovic, Z. Zalevsky, R.G. Dorsch, Some important fractional transforms for signal processing, Opt. Commun. 125 (1996) 18–20.

[30] S.C. Pei, M.H. Yeh, The discrete fractional cosine and sine transforms, IEEE Trans. Signal Proc. 49 (2001) 1198–1207.

[31] G. Cariolaro, T. Erseghe, P. Kraniauskas, The fractional discrete cosine transform, IEEE Trans. Signal Proc. 50 (2002) 902–911.