

# Color image encryption combining a reality-preserving fractional DCT with chaotic mapping in HSI space

Yaru Liang<sup>1</sup> · Guoping Liu<sup>1</sup> · Nanrun Zhou<sup>2</sup> ·  
Jianhua Wu<sup>2</sup>

Received: 10 October 2014 / Revised: 31 January 2015 / Accepted: 30 March 2015 /  
Published online: 19 April 2015  
© Springer Science+Business Media New York 2015

**Abstract** A color image encryption algorithm by combining the reality-preserving fractional DCT (RPFrDCT) with chaotic mapping in HSI space is presented, in which the generating sequence (GS) is introduced and produced by 2D chaotic mapping to ensure the uniqueness of the transform matrix and enlarge the cipher key space of the encryption system. In addition, the color image is converted from standard RGB space into HSI space and the nonlinearity of the spatial transform makes the proposed encryption algorithm more secure than linear ones. Three components, namely H, S and I, are encrypted by the RPFrDCT with fractional orders and GS as cipher keys. Three-dimensional (3D) scrambling is adopted to further enhance the security of the encryption algorithm. The nonlinearity of the spatial transform from RGB to HSI, the real-valued output and the high cipher key-sensitivity guarantee the security and the feasibility of the proposed encryption algorithm. Experimental results demonstrate that the proposed encryption algorithm is sensitive to cipher keys and, to some extent, robust to noise and occlusion attacks.

**Keywords** Reality-preserving fractional DCT · HSI space · Generating sequence · Three-dimensional scrambling · Color image encryption

---

✉ Jianhua Wu  
jhwu@ncu.edu.cn

Yaru Liang  
liangyaru@126.com

Guoping Liu  
liuguoping.ncu@163.com

Nanrun Zhou  
nrzhou@ncu.edu.cn

<sup>1</sup> School of Mechatronic Engineering, Nanchang University, Nanchang 330031, China

<sup>2</sup> Department of Electronic Information Engineering, Nanchang University, Nanchang 330031, China

## 1 Introduction

Nowadays, the Internet and multimedia technology has grown fast and digital information can be acquired and transmitted easily. Digital images, especially color images, can provide more immediate visual information. As the problems of illegally obtaining personal privacy and data information on the Internet become more and more serious, information security is a vital issue in data storage and exchange. Generally, encryption is a good method to ensure the high security and usually implemented in spatial and frequency domains. In spatial domain, the basic principle of encryption includes three major forms: permutation, diffusion and their compound [6, 13, 15]. With the intrinsic features such as high sensibility dependence on initial conditions and control parameters, random-like behavior and low computational complexity, chaos becomes the most suitable candidate to encrypt images in spatial domain. Thus, a variety of chaos-based algorithms were proposed for image encryption [4, 14, 16, 23–25]. An example of image encryption based on chaos can be found in Ref. [2], in which a coupling of chaotic function and xor operator is applied to increase unpredictability in the encrypted image and a large key space is produced to resist brute-force attack. Zhou et al. proposed an image encryption using a new parametric switching chaotic system [27], in which a new parametric switching chaotic system composed of Logistic, Sine, and Tent mappings has more complex chaotic behavior and the encryption algorithm has a high level of security. In addition to the above mentioned spatial domain based methods, various encryption schemes in frequency domain have also been presented for the security of image information so far. In 1995, Refregier and Javidi proposed an optical encryption method in Fourier domain, in which the encrypted image is obtained by random-phase encoding in both the input and the Fourier planes [12]. Later on, Unnikrishnan et al. firstly presented optical image encryption in fractional Fourier domain, in which a primary image is encoded to stationary white noise with the fractional orders as the cipher keys [17]. And on this basis, the fractional Fourier transform (FrFT) and its optical implementation have been studied for many years. In FrFT based image encryption, the fractional orders are used as cipher keys, but the key space was relatively small. Liu and Sheridan proposed an image encryption method by jigsaw and Arnold transforms to scramble an image in the fractional Fourier domain, which provides an enlarged cipher key space and security level due to using the jigsaw permutation indices, Arnold frequencies and fractional Fourier orders as cipher keys [10]. The discrete FrFT has a certain relationship with the discrete fractional cosine and sine transforms. Pei et al. proposed the discrete fractional cosine and sine transforms, which help to reduce the computational load of discrete fractional Fourier transform [11]. After that, a number of scholars studied deeply about the discrete fractional cosine and sine transforms and the fractional Mellin transform are introduced into the field of image information security [21, 26, 28]. Liu and Nan proposed a color image security system using chaos and multiple-order discrete fractional cosine transform [9], which provides a large key space with the help of chaos to generate the transform orders. Yet, the output of most transform-based encryption algorithm is complex, which increases the burden of storage and transmission. In 2004, Venturini and Duhamel [18] proposed a method of reality-preserving treatment for a fractional transform, in which the coefficients of transform are real. Subsequently, Lang proposed the reality-preserving multiple-parameter FrFT [7], with the nature of real-valuedness as well as most properties required for a fractional transform. Zhou et al. proposed an image encryption method based on the reality preserving fractional Mellin transform (RPFrMT), in which the output of transform is real and the transform is nonlinear [29]. The above mentioned reality preserving transforms adopted the same way of transform, i.e., a reality-preserving transform matrix must be constructed and the reality-preserving fractional transform has lost some properties compared with non-reality preserving fractional transform. In view of this, image encryption based

on a reality-preserving fractional DCT is proposed [8], where multiple generating sequences are employed to enlarge the key space of encryption system. In Ref. [20], three color images are firstly converted to three index-format images and then the three index-format images serve as three components, namely R, G, B, of a single color image. This method's advantage is that the amount of data is reduced and the output of encrypted images is real. Yet the output is coded with float-point numbers due to the operation of DCT-based transform, which in turn expands the data amount.

In this paper, we proposed a color image encryption algorithm based on a reality-preserving fractional DCT (RPFrDCT) in HSI space, by taking the advantages of both the reality of RPFrDCT and the nonlinearity of the transform of RGB-to-HSI. First, the original RGB image is converted into HSI space, which is more desirable to human visual properties than RGB space. The RGB model is mostly oriented toward hardware and is not simply synthesized by three primary-color images to one image in practice, while the HSI model corresponds closely with the way humans describe and interpret colors. Human likes to use hue, saturation and intensity to describe objects. The HSI model is an ideal tool for the color image encryption. Its advantage is that it can decouple the color and the gray-scale information in an image in a nonlinear way. Then, each component of the color image in HSI space is transformed with the RPFrDCT. The RPFrDCT has unitary, real orthogonal and a unique orthogonal basis, in which choosing a specific sequence called as a generating sequence (GS) of the RPFrDCT has resolved the nonuniqueness of a fractional operator. In RPFrDCT, only two generating sequences are employed to make the encryption algorithm simpler and more effective. And then a 2D chaotic mapping is employed to generate the random GS. Finally, to further enhance the security of the system, a three-dimensional (3D) scrambling is utilized to scramble the positions of the coefficients in RPFrDCT domain, thus the three components of a color image mutually affect each other. Experimental results demonstrate that the proposed algorithm is feasible, secure, sensitive to keys and, to some extent, robust to noise and occlusion attacks.

The rest of this paper is organized as follows. The theoretical background for RPFrDCT and the chaotic mapping are reviewed in Section 2. The new color image encryption algorithm based on the HSI space, RPFrDCT and chaos is introduced in Section 3. Experimental results and analysis are conducted in Section 4. And finally, the conclusions are drawn in the last section.

## 2 Theoretical background

### 2.1 Reality-preserving fractional DCT

The reality-preserving fractional DCT (RPFrDCT) matrix  $\mathbf{C}_\alpha$  is defined as [1, 8, 19, 20]:

$$\begin{aligned} \mathbf{C}_\alpha &= 2\text{Re} \left[ \sum_{n=1}^{N/2} \mathbf{U}_n \lambda_n^\alpha \right] = 2\text{Re} \left[ \sum_{n=1}^{N/2} \mathbf{U}_n e^{j(\varphi_n + 2\pi q_n)\alpha} \right] \\ &= \sum_{n=1}^{N/2} (\mathbf{A}_n \cos \omega_n \alpha + \mathbf{B}_n \sin \omega_n \alpha) \end{aligned} \quad (1)$$

where  $\alpha$  is the fractional order,  $N$  is an integer multiple of 4,  $\mathbf{U}_n = \mathbf{u}_n \mathbf{u}_n^*$  is unitary matrices,  $\mathbf{u}_n$  is the  $n$ -th eigenvector of the  $N \times N$  DCT matrix,  $\mathbf{A}_n = 2\text{Re}[\mathbf{U}_n]$ ,  $\mathbf{B}_n = -2\text{Im}[\mathbf{U}_n]$ ,  $\omega_n = \varphi_n + 2\pi q_n$ ,  $0 < \varphi_n < \pi$ ,  $n = 1, 2, \dots, N/2$ ,  $q_n$  is an arbitrary integer,  $\mathbf{q} = (q_1, q_2, \dots, q_{N/2})$  is called the generating

sequence (GS) of the RPFrDCT. The RPFrDCT matrix  $C_\alpha$  becomes unique for  $N=4N_0$  with a specific GS. The RPFrDCT inherits all features of DCT, such as having a unique orthonormal basis, the reality preservation and index additivity, except periodicity. Different  $\mathbf{q}$  can result in different matrix  $C_\alpha$ . The detailed derivation of  $C_\alpha$  can be found in Ref. 20.

For an image  $\mathbf{f}$ , its two-dimensional RPFrDCT is given by:

$$\mathbf{F} = \mathbf{C}_\alpha \mathbf{f} \mathbf{C}'_\beta \tag{2}$$

where  $\alpha$  and  $\beta$  are the fractional orders of row and column, respectively, and ' denotes the operation of transposition. The inverse of the two-dimensional RPFrDCT is simply given by:

$$\mathbf{f} = \mathbf{C}_{-\alpha} \mathbf{F} \mathbf{C}'_{-\beta} \tag{3}$$

### 2.2 GS based on the 2D chaotic mapping

The 2D chaotic mapping is exploited to generate the GS, since it has more initial and system parameters than in one dimensional case, thus the space of cipher key is enlarged and the security is enhanced. The 2D chaotic mapping, also called the generalized Arnold mapping, is expressed as [5]:

$$\begin{cases} x_{n+1} = x_n + ay_n \pmod 1 \\ y_{n+1} = bx_n + (1 + ab)y_n \pmod 1 \end{cases} \tag{4}$$

where  $x_n, y_n \in (0, 1)$ ,  $n=0, 1, 2, \dots$  are the random iterative values and  $x_0, y_0$  are the initial values. If  $a > 0$  and  $b > 0$ , the generalized Arnold mapping will exhibit chaotic behavior. Large number of random iterative values limited in  $(0, 1)$  and the desirable properties of non-correlation, pseudo-randomness can be generated through iterating Eq. (4).  $x_0, y_0, a$  and  $b$  are used as the cipher keys. For an image of size  $M \times N$ , two generating sequences of length  $M/2$  and  $N/2$  are necessary for the RPFrDCT. Then, two random sequences are obtained by iterating Eq. (4) and denoted as  $\mathbf{x}$  and  $\mathbf{y}$

$$\begin{aligned} \mathbf{x} &= \{x_n, n = 0, 1, 2, \dots, K + M/2 - 1\} \\ \mathbf{y} &= \{y_n, n = 0, 1, 2, \dots, K + N/2 - 1\} \end{aligned}$$

The previous  $K$  entries are discarded in the calculating process of  $\mathbf{x}$  and  $\mathbf{y}$  for enhancing randomness and confusion, resulting in two new random sequences  $\mathbf{x}$  and  $\mathbf{y}$  of length  $M/2$  and  $N/2$ , respectively.

Since GS is a random integer sequence, a threshold function is defined as follows:

$$\begin{aligned} q_x(n) &= \begin{cases} 0, & 0 < x_n \leq 0.25 \\ 1, & 0.25 < x_n \leq 0.5 \\ 2, & 0.5 < x_n \leq 0.75 \\ 3, & 0.75 < x_n < 1 \end{cases} & n = 1, 2, \dots, M/2 \\ q_y(n) &= \begin{cases} 0, & 0 < x_n \leq 0.25 \\ 1, & 0.25 < x_n \leq 0.5 \\ 2, & 0.5 < x_n \leq 0.75 \\ 3, & 0.75 < x_n < 1 \end{cases} & n = 1, 2, \dots, N/2 \end{aligned} \tag{5}$$

where  $q_x(n)$  is the  $n$ -th entry in  $\mathbf{q}_x$ , and similar to  $q_y(n)$ .  $\mathbf{q}_x$  and  $\mathbf{q}_y$  are specified as the generating sequences for the rows and the columns of RPFrDCT, respectively. In Eq. (5),  $\mathbf{x}$  and

$y$  are mapped into four different values. Of course,  $x$  and  $y$  can also be mapped to more integer values which have better chaotic property. The experiments in Section 4 verify that the decrypted image quality is sensitive to the initial values of the 2D chaotic mapping, if  $x$  and  $y$  are mapped into at least four different integer values.

### 3 Image encryption based on the RPFrDCT and chaos

As shown in Fig. 1, the proposed encryption system consists of four parts, i.e., the RGB-to-HSI model transform, the RPFrDCT, scrambling and quantization.

The specific encryption steps are described as follows:

- (1) The original image is converted from RGB space to HSI space.  
 For an RGB color image, each pixel is represented by the values of three components, but the three components are not independent—they have a strong correlation. The HSI space decouples the three components. In addition, the spatial transform between RGB and HSI is nonlinear and benefits to image encryption.
- (2)  $H_0$ ,  $S_0$  and  $I_0$  are obtained by RPFrDCT with the specific generating sequences  $q_x$  and  $q_y$ . And the fractional orders  $\alpha$  and  $\beta$ , the number  $K$  of discarded entries and the chaotic parameters for generating  $q_x$  and  $q_y$  are cipher keys.
- (3) In the RPFrDCT domain, further scrambling operations are conducted as:
  - (a) Two random matrices  $P_1$  and  $P_2$  are generated as permutation matrices with seeds  $s_1$  and  $s_2$ , the size of the random matrices is the same as the image size.  $P_1$  and  $P_2$  are obtained by the low triangular matrix and the upper triangular matrix (LU) decomposition [29].
  - (b) A 2D scrambling for three components are obtained by:
 
$$\begin{cases} H_1 = (P_1 P_2)H_0(P_2 P_1) \\ S_1 = (P_1 P_2)S_0(P_2 P_1) \\ I_1 = (P_1 P_2)I_0(P_2 P_1) \end{cases} \quad (6)$$
  - (c) A random matrix of size  $3 \times 3$  is produced by the seed  $s_3$ . Then, the permutation matrix  $P_3$  is obtained using the same method as step (a). A 3D scrambling is obtained by confusing  $H_1$ ,  $S_1$  and  $I_1$ :

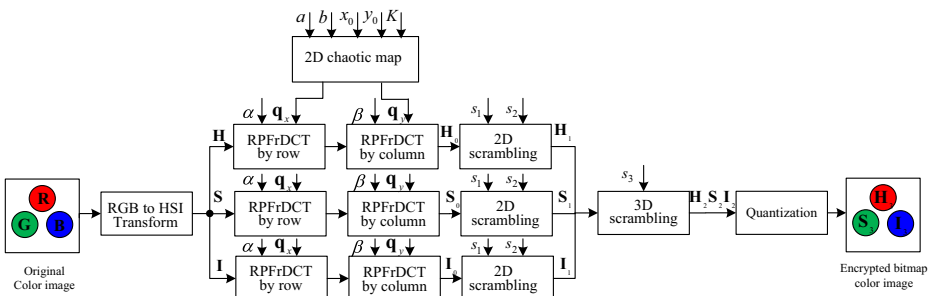


Fig. 1 Diagram of the proposed encryption system

$$\begin{cases} \mathbf{H}_{2A}(i, j) = \mathbf{P}_3(1, :) [\mathbf{H}_{1A}(i, j), \mathbf{S}_{1B}(i, j), \mathbf{I}_{1C}(i, j)]' \\ \mathbf{S}_{2A}(i, j) = \mathbf{P}_3(2, :) [\mathbf{H}_{1D}(i, j), \mathbf{S}_{1A}(i, j), \mathbf{I}_{1B}(i, j)]' \\ \mathbf{I}_{2A}(i, j) = \mathbf{P}_3(3, :) [\mathbf{H}_{1C}(i, j), \mathbf{S}_{1D}(i, j), \mathbf{I}_{1A}(i, j)]' \end{cases} \quad (7)$$

where ' denotes transposition.  $\mathbf{H}_1$ ,  $\mathbf{S}_1$  and  $\mathbf{I}_1$  are respectively divided into four parts as shown in Fig. 2, in which A, B, C, and D represent different parts in matrix. For example,  $\mathbf{H}_{1A}(i, j)$  indicates the entry of the  $i$ -th row and the  $j$ -th column in Part A of  $\mathbf{H}_1$  and similar to the  $\mathbf{S}_{1B}(i, j)$  and  $\mathbf{I}_{1C}(i, j)$ .  $\mathbf{H}_{2A}(i, j)$  represents the entry of the  $i$ -th row and the  $j$ -th column in Part A of the scrambled result  $\mathbf{H}_2$  and similar to the  $\mathbf{S}_{2A}(i, j)$  and  $\mathbf{I}_{2A}(i, j)$ .  $\mathbf{P}_3(i, :)$  represents the  $i$ -th ( $i=1, 2, 3$ ) row of matrix  $\mathbf{P}_3$ . The rest parts of  $\mathbf{H}_2$ ,  $\mathbf{S}_2$  and  $\mathbf{I}_2$  can be obtained similarly from Eq. (7) with combination of three parts of A, B, C and D of  $\mathbf{H}_1$ ,  $\mathbf{S}_1$  and  $\mathbf{I}_1$ . For example,  $\mathbf{H}_{2B}$  can be obtained using  $\mathbf{H}_{1B}$ ,  $\mathbf{S}_{1C}$  and  $\mathbf{I}_{1D}$ .

- (4) Each of the three components,  $\mathbf{H}_2$ ,  $\mathbf{S}_2$  and  $\mathbf{I}_2$ , is uniformly quantized with 8 bits for a pixel, resulting in three components  $\mathbf{H}_3$ ,  $\mathbf{S}_3$  and  $\mathbf{I}_3$ , which can be stored in a bitmap format, the same way like the original image. The three components are not converted back to RGB and comprise directly the encrypted image, as shown in the right-most block in Fig. 1.

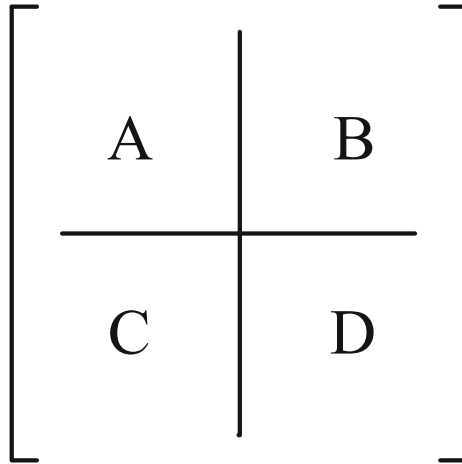
The decryption process is the inverse of encryption with the fractional orders for RPFrDCT  $\alpha' = -\alpha$ ,  $\beta' = -\beta$  and all other cipher parameters unchanged. The near-lossless image reconstruction can be achieved if all cipher keys are correct.

## 4 Experimental results and analysis

Experiments are performed to test the proposed color image encryption method. According to Section 2.1, the length of signal is the integer multiple of 4, the color image, Lena, with the size of  $512 \times 512 \times 3$  (Fig. 3a) is adopted as the original test image. An average value should be subtracted to remove the direct current (DC) component, so that in the quantization process after the RPFrDCT the quantization error can be as small as possible. Since the values of three components range from 0 to 1 after the spatial transform from RGB to HSI, 0.5 is selected as an approximation of the DC value for convenience.  $a$ ,  $b$ ,  $x_0$ ,  $y_0$ ,  $s_1$ ,  $s_2$ ,  $s_3$  and  $K$  are the cipher keys. Since the decrypted image quality is not sufficiently sensitive to the fractional orders  $\alpha$  and  $\beta$ , the fractional orders serve as the auxiliary keys and set to be 0.7689 and 0.4578, respectively. According to Section 2.2, the parameters  $\{a, b, x_0, y_0, K\}$  are randomly chosen within the above specified intervals. In our experiment, they are  $\{3.13, 6.32, 0.348921, 0.456932, 1000\}$ . Certainly, these parameters can be set to be any values satisfying the conditions. Besides, three seeds,  $s_1$ ,  $s_2$  and  $s_3$ , used in three dimensional scrambling are set to be 0.234, 0.345 and 0.5624, respectively. If any other values are chosen, the performance of the algorithm is not affected. All simulations are performed using MATLAB 2007(a) in a computer with Intel Core2 CPU 2.93GHz, 1.96GB of memory. The encrypted and decrypted images are shown in Fig. 3b and c, respectively.

### 4.1 Key space and sensitivity analysis

A secure encryption scheme should be sensitive to its cipher keys, i.e., a slight difference of cipher keys will result in a complete different decrypted image [22]. In this paper, the cipher

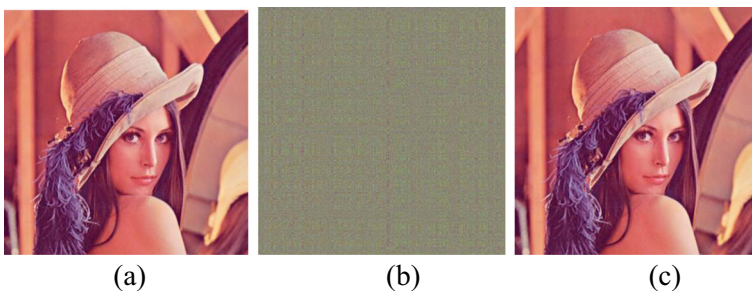


**Fig. 2** Division diagrams of matrix

key parameters are  $\{a, b, x_0, y_0, s_1, s_2, s_3, K\}$ . Figure 4 illustrates the decrypted images with a slight deviation of one cipher key while other cipher keys remain correct.  $s_1, s_2$  and  $s_3$  are seeds of 2D scrambling and 3D scrambling. From Fig. 4, one cannot distinguish the content of the decrypted images even the deviation is as small as  $10^{-15}$ . Thus, the proposed algorithm is sensitive to the cipher keys. If the deviations of  $a, b, x_0, y_0, s_1, s_2$  and  $s_3$  are  $10^{-15}$ , the decrypted images (Fig. 4) are still messy. Then the size of key space comes out to be  $10^{105}$ . In addition,  $K$  can also be used as the cipher keys. Thus, the key space is large enough to resist brute-force attack.

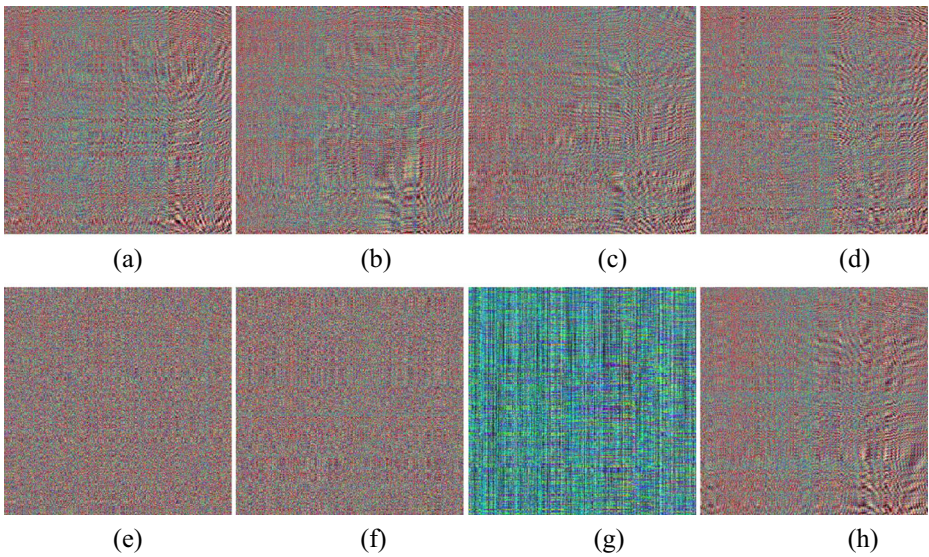
#### 4.2 Statistical analysis

Histograms and correlations of different test images have been considered. Due to the limit of paper length, only Lena, Peppers, Barbara and Baboon images (Fig. 5) are adopted as test images for histogram analysis. As shown in Fig. 6, the histograms of the three components of original images are entirely different, while those of the encrypted images are all like Gaussian distribution and obviously different from those of the corresponding original color images. And experimental results indicate that the histograms of the encrypted images for different



**Fig. 3** Test image and results: (a) Lena, (b) Encrypted Lena and (c) Decrypted Lena





**Fig. 4** Decrypted images with only one wrong cipher key. **a**  $\Delta x_0=10^{-15}$ , **b**  $\Delta y_0=10^{-15}$ , **c**  $\Delta a=10^{-15}$ , **d**  $\Delta b=10^{-15}$ , **e**  $\Delta s_1=10^{-15}$ , **f**  $\Delta s_2=10^{-15}$ , **g**  $\Delta s_3=10^{-15}$ , **h**  $\Delta K=1$

plain-images are all similar to each other, which declares that the attackers could not obtain any valid information about the original images through analyzing the histograms of the encrypted images. Thus, the proposed algorithm is able to resist statistical attacks.

Each pixel is usually correlated with its adjacent pixels in a normal image [22]. Attackers can utilize the correlation of the encrypted image to decode. The expression of the self-correlation coefficient  $r(u, v)$  is shown as:

$$r(u, v) = \frac{\sum_{x,y} [f(x, y) - \bar{f}] [f(x-u, y-v) - \bar{f}]}{\sqrt{\sum_{x,y} [f(x, y) - \bar{f}]^2 \sum_{x,y} [f(x-u, y-v) - \bar{f}]^2}} \tag{8}$$

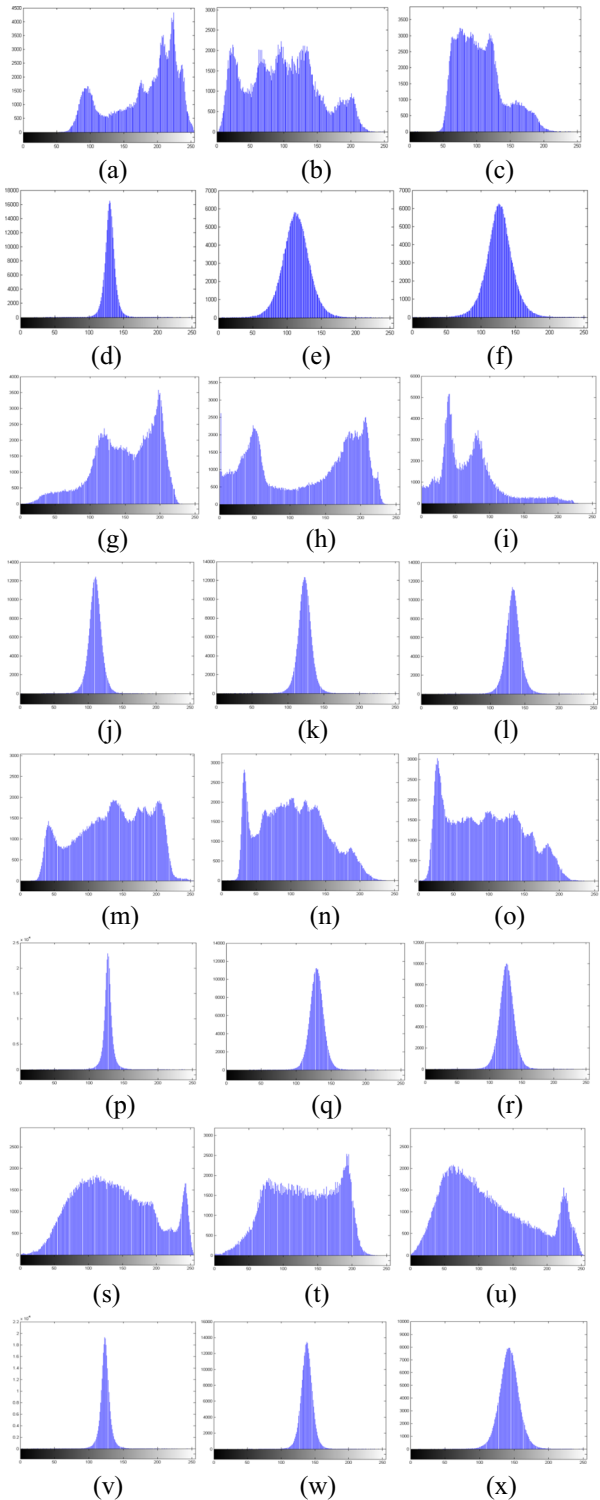
where  $f(x, y)$  is the pixel value of the image at the coordinate  $(x, y)$ ,  $\bar{f}$  is the mean of all pixel values of  $f(x, y)$ , and  $u, v$  are the offsets of  $x$  -direction and  $y$  -direction, respectively.

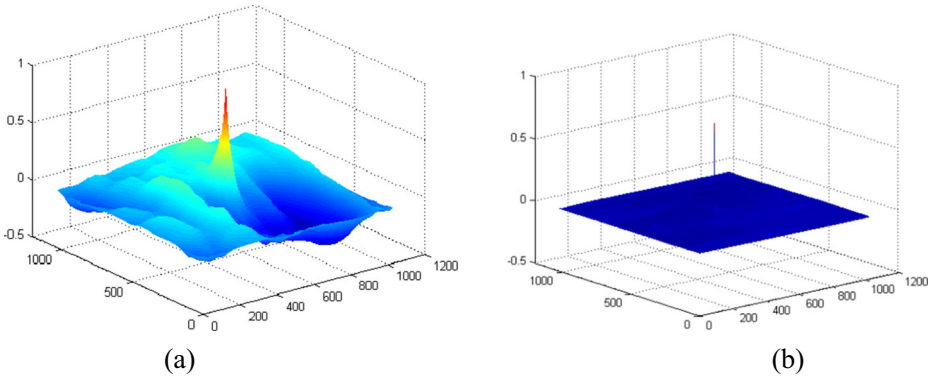


**Fig. 5** Test images for histogram analysis: **(a)** Lena, **(b)** Peppers, **(c)** Barbara and **(d)** Baboon



**Fig. 6** Histograms of the original Lena for (a) R, (b) G, (c) B components, the original Peppers for (g) R, (h) G, (i) B components, the original Barbara for (m) R, (n) G, (o) B components and histograms of the encrypted Lena for (d) R, (e) G, (f) B components, the encrypted Peppers for (j) R, (k) G, (l) B components, the encrypted Barbara for (p) R, (q) G, (r) B components and the encrypted Baboon for (v) R, (w) G, (x) B components





**Fig. 7** Self-correlation of R component for Lena. **a** the original image and **b** the encrypted image

As shown in Fig. 7a, self-correlation coefficients include positive and negative values, and the surface is rough, where the maximum value comes out to be in the center. However, those are almost even except the maximum value after encryption, as shown in Fig. 7b, which shows that the correlation among pixels is weak. The self-correlations of the other components of the original image and the encrypted image have similar behaviors. Therefore, the proposed algorithm has an ability of de-correlation and the attackers cannot obtain any valid information with correlation analysis.

### 4.3 Robustness analysis

The quantization leads to somewhat error between the decrypted and original images even during completely correct decryption. To evaluate the quality of decrypted images, the peak signal-to-noise ratio (PSNR) is adopted:

$$PSNR = 10 \log_{10} \left( \frac{255^2 \times M \times N}{\sum_{i=1}^M \sum_{j=1}^N [\mathbf{O}(i, j) - \mathbf{I}(i, j)]^2} \right) \text{ (dB)} \tag{9}$$

where  $M \times N$  is the size of image,  $\mathbf{I}(i, j)$  and  $\mathbf{O}(i, j)$  are the pixel values of the original image and decrypted image at  $(i, j)$ , respectively. For a color image, the PSNR can be calculated as the mean of PSNRs of three components.

The proposed encryption algorithm is compared with the encryption algorithm based on RPFrMT in Ref. [29]. The output of the encrypted image in Ref. [29] is real, however, the disadvantages are its floating-point output and data expansion with respect to the original

**Table 1** Information of encrypted images

Approach	Size of the encrypted image	Format of the encrypted image
Zhou et al. [29]	1024 × 1024	Float point number
Our method	512 × 512	8-bit integer

**Table 2** PSNRs for different noise intensities  $k$ 

Algorithm\k	0	10	30	50	70	100
RPFrDCT	39.9973 dB	14.0820 dB	9.6838 dB	8.2900 dB	7.6434 dB	7.1805 dB
RPFrMT [29]	36.1655 dB	13.6999 dB	8.0387 dB	6.8191 dB	6.3068 dB	5.9571 dB

image. However, the proposed algorithm in this paper has not any data expansion, as shown in Table 1.

The Gaussian noise is added into the encrypted image as follows:

$$\mathbf{E}' = \mathbf{E} + k\mathbf{N} \quad (10)$$

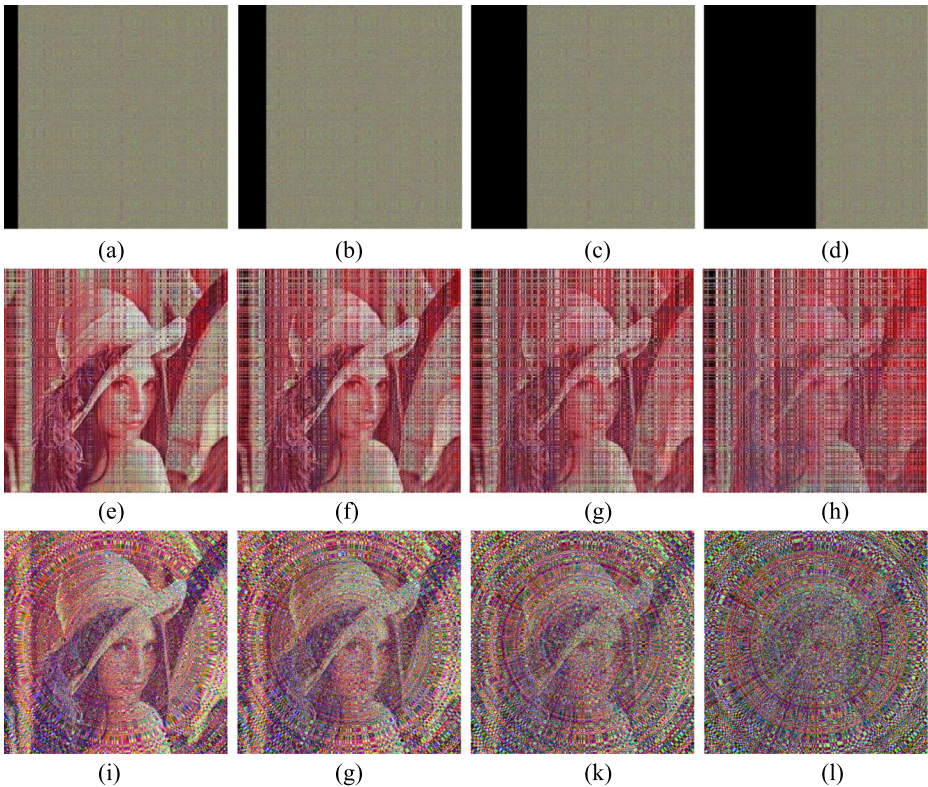
where  $\mathbf{E}'$  and  $\mathbf{E}$  are the encrypted images with and without noise, respectively.  $k$  is a coefficient representing the added noise intensity. The larger the  $k$  is, the stronger the noise is.  $\mathbf{N}$  is the Gaussian noise with zero-mean and unit standard deviation. Three channels of the encrypted image are added noise with the same intensity.

The PSNRs of the decrypted images decoded from encrypted images affected by different intensities of noise are shown in Table 2. The more the noise intensity  $k$  increases, the more the PSNR decreases. By comparison, the PSNRs of the decrypted images are higher than those in Ref. [29]. For example, intuitively, the details of Lena's eyes can be discerned in Fig. 8c while they cannot be identified in Fig. 8g. As a result, the proposed algorithm has the ability of anti-noise to some extent. Furthermore, the ability of anti-noise of the proposed algorithm is stronger than that of the proposed algorithm in Ref. [29].

The encrypted images with an occlusion of ratios of 1/16, 1/4, 1/8 and 1/2 and the corresponding decrypted results are shown in Fig. 9. And the PSNRs of decrypted images



**Fig. 8** Decrypted images by RPFrDCT with different Gaussian noise intensities of (a) 10, (b) 30, (c) 50 and (d) 100; Decrypted images by RPFrMT [29] with different Gaussian noise intensities of (e) 10, (f) 30, (g) 50 and (h) 100



**Fig. 9** Results of anti-occlusion attacks: The encrypted images by RPFrDCT with an occlusion of (a) 1/16, (b) 1/8, (c) 1/4 and (d) 1/2; (e), (f), (g) and (h) are decrypted images from (a), (b), (c) and (d), respectively; (i), (j), (k) and (l) are decrypted images by RPFrMT [29] under the same occlusions as in (a), (b), (c) and (d), respectively

are shown in Table 3. In spite of partial data cropping and a decrease in PSNR, the decrypted images can still be recognized. The PSNRs of decrypted images are higher than those in Ref. [29]. From Table 3 and Fig. 9, the proposed algorithm has a stronger ability of anti-cropping than that in Ref. [29].

#### 4.4 Known/chosen plaintext attack

Practically, there exist four potential types of attacks including cipher only attack, known plaintext attack, chosen plaintext and chosen cipher-text attack [9]. Generally, chosen plaintext is the most powerful attack. If an encryption system is linear, it is vulnerable to the attack of known plaintext and chosen plaintext [3]. In this paper, not only the spatial transform is

**Table 3** PSNRs for different cropped ratios

Algorithm	1/16	1/8	1/4	1/2
RPFrDCT	10.75 dB	9.74 dB	8.78 dB	7.94 dB
RPFrMT [29]	9.06 dB	7.97 dB	7.27 dB	6.57 dB



nonlinear but also the 2D scrambling and 3D scrambling strengthen the nonlinearity of the encryption system. Thus, the proposed algorithm can resist these classical types of attacks.

## 5 Conclusion

An RPFrDCT based color image encryption algorithm is proposed in HSI space. The HSI model is a nonlinear spatial transform and an ideal tool for developing image processing algorithms based on color descriptions that are natural and intuitive to humans. In HSI space, three channel components are encrypted by RPFrDCT, in which the GS is used as main cipher keys and generated by the 2D chaotic mapping. To further enhance the security, scrambling operation is exploited to scramble the three components, which makes the three components of a color image mutually affect each other. Experimental results show that the proposed scheme has a high key-sensitivity, a sufficiently large key space and, to some extent, robustness against noise and occlusion attacks. The advantages of the encryption algorithm is the nonlinearity of the spatial transform RGB-to-HSI, the real-valued output of RPFrDCT for real input, which is beneficial for storage, display and transmission of images.

**Acknowledgments** This work was supported by the National Natural Science Foundation of China (61262084 and 61462061), the Natural Science Foundation of Jiangxi Province (20122BAB201029) and the Science and Technology Program of Jiangxi Provincial Department of Education (GJJ14135).

## References

1. Cariolaro G, Erseghe T, Kraniuskas P (2012) The Fractional discrete cosine transform. *IEEE Trans Signal Process* 50(4):902–911
2. Francois M, Grosgees T, Barchiesi D, Erra R (2012) A new image encryption scheme based on a chaotic function. *Signal Process Image Commun* 27(3):249–259
3. Frauel Y, Castro A, Naughton T, Javid B (2007) Resistance of the double random phase encryption against various attacks. *Opt Express* 15(16):10253–10265
4. Huang XL, Ye GD (2014) An efficient self-adaptive model for chaotic image encryption algorithm. *Commun Nonlinear Sci Numer Simul* 19(10):4094–4104
5. Huang XL, Ye GD (2014) An efficient self-adaptive model for chaotic image encryption algorithm. *Commun Nonlinear Sci Numer Simul* 19(12):4094–4104
6. Kanso A, Ghebleh M (2012) A novel image encryption algorithm based on a 3D chaotic mapping. *Commun Nonlinear Sci Numer Simul* 17(7):2943–2959
7. Lang J (2012) Image encryption based on the reality-preserving multiple-parameter fractional Fourier transform and chaos permutation. *Opt Laser Technol* 50(7):929–937
8. Liang YR, Liu GP, Zhou NR, Wu JH (2014) Image encryption combining multiple generating sequences controlled fractional DCT with dependent scrambling and diffusion. *J Mod Opt*. doi:10.1080/09500340.2014.964342
9. Liu H, Nan H (2013) Color image security system using chaos-based cyclic shift and multiple-order discrete fractional cosine transform. *Opt Laser Technol* 50:1–7
10. Liu S, Sheridan JT (2013) Optical encryption by combining image scrambling techniques in fractional Fourier domains. *Opt Commun* 287:73–80
11. Pei SC, Yeh MH (2001) The discrete fractional cosine and sine transforms. *IEEE Trans Signal Process* 49(6):1198–1207
12. Refregier P, Javid B (1995) Optical image encryption based on input plane and Fourier plane random encoding. *Opt Lett* 20(7):767–769
13. Singh N, Sinha A (2010) Chaos based multiple image encryption using multiple canonical transforms. *Opt Laser Technol* 42(5):724–731

14. Song CY, Qiao YL, Zhang XZ (2013) Image encryption scheme based on new spatiotemporal chaos. *Optik* 124(18):3329–3334
15. Tong X (2010) The novel bilateral-Diffusion image encryption algorithm with dynamical compound chaos. *J Syst Softw* 85(4):850–858
16. Tong X, Cui M (2009) Image encryption scheme based on 3D baker with dynamical compound chaotic sequence cipher generator. *Signal Process* 89(4):480–491
17. Unnikrishnan G, Joseph J, Singh K (2000) Optical encryption by double-random phase encoding in the fractional Fourier domain. *Opt Lett* 25(12):887–889
18. Venturini I, Duhamel P (2004) Reality Preserving Fractional Transforms. *ICASSP IEEE Int Conf Acoust Speech Signal Process Proc* 5:V- 205-V-208
19. Wu JH, Guo FF, Liang YR, Zhou NR (2014) Triple color images encryption algorithm based on scrambling and the reality-preserving fractional discrete cosine transform. *Optik* 125(16):4474–4479
20. Wu JH, Guo FF, Zeng PP, Zhou NR (2013) Image encryption based on a reality-preserving fractional discrete cosine transform and a chaos-based generating sequence. *J Mod Opt* 60(20):1760–1771
21. Wu JH, Zhang L, Zhou NR (2010) Image encryption based on the multiple-order discrete fractional cosine transform. *Opt Commun* 283(9):1720–1725
22. Yoon JW, Kim H (2010) An image encryption scheme with a pseudorandom permutation based on chaotic mappings. *Commun Nonlinear Sci Numer Simul* 15(12):3998–4006
23. Zhang Q, Guo L, Wei XP (2013) A novel image fusion encryption algorithm based on DNA sequence operation and hyper-chaotic system. *Optik* 124(18):3596–3600
24. Zhang LY, Hu XB, Liu YS, Wong KW, Gan J (2014) A chaotic image encryption scheme owning temporal feedback. *Commun Nonlinear Sci Numer Simul* 19:3653–3659
25. Zhang YS, Xiao D (2014) Self-adaptive permutation and combined global diffusion for chaotic color image encryption. *AEU Int J Electron Commun* 68(4):361–368
26. Zhang YS, Xiao D, Wen WY, Tian Y (2013) Edge-based lightweight image encryption using chaos-based reversible hidden transform and multiple-order discrete fractional cosine transform. *Opt Laser Technol* 54:1–6
27. Zhou YC, Chen BL, CLP (2013) Image encryption using a new parametric switching chaotic system. *Signal Process* 93(11):3039–3052
28. Zhou NR, Liu XB, Zhang Y, Yang YX (2013) Image encryption scheme based on fractional Mellin transform and phase retrieval technique in fractional Fourier domain. *Opt Laser Technol* 47:341–346
29. Zhou NR, Wang YX, Gong LH, Chen XB, Yang YX (2012) Novel color image encryption algorithm based on the reality preserving fractional Mellin transform. *Opt Laser Technol* 44(7):2270–2281



**Yaru Liang** Was born in Tieling, Liaoning Province, China, on Apr. 19, 1978. She received a Bachelor's degree in automation from Heilongjiang Institute of Technology in 2002 and a Master's degree in power electronics and power drives from Shenyang University of Technology in 2008. She is now in pursuit of Doctor degree in mechatronic engineering in Nanchang University. Her research interests include image processing, image encryption and information security.





**Guoping Liu** Was born in Linchuan County of Jiangxi Province, China, on Aug. 1, 1964. He received a Master's degree in mechatronic engineering from Zhejiang University in 1993. Now, he is a professor, a doctoral tutor and works in school of mechatronic engineering, Nanchang University, China. His research interests include signal processing, robot technology and intelligent control.



**Nanrun Zhou** Was graduated from Jiangxi Normal University, Nanchang, China and received his Bachelor degree in Physics in 2000. He studied for his Master degree from September 2000 to June 2003 in Theoretical Physics in Jiangxi Normal University and Doctor Degree from March 2003 to September 2005 in Communications & Information Systems in Shanghai Jiao Tong University, Shanghai, China. Now, as a professor, his research focuses on Optical Image Encryption, Algorithm Design and Analyses, Information Security, etc. He has published over 40 papers in academic journals and conferences.



**Jianhua Wu** born in Jinxian County of Jiangxi Province, China, on Sept. 9, was graduated from Harbin Institute of Technology in 1982 and got a Bachelor's degree in information engineering. In 1985, he was graduated from South China University of Technology, Guangzhou, China and got a Master's degree of science majored in communication and electronic systems. In 2005, he got the Ph.D. from the University of Poitiers, Poitiers, France majored in image and signal processing. He is currently a professor with Department of Electronic Information Engineering, Nanchang University, China. He has published more than twenty papers in journals such as Optics Communications, Optics and Laser Technology, etc. His research interests include image and signal processing, image encryption, pattern recognition, etc. Dr. Wu is a member of IEEE.