DOUBLE RANDOM SCRAMBLING ENCODING IN THE RPMPFRHT DOMAIN

Xuejing Kang, Zhao Han, Aiwei Yu, Peiqi Duan

Institute of Sensing Technology and Business, Beijing University of Posts and Telecommunications.

ABSTRACT

In this paper, a novel method of digital image encryption based on the reality-preserving multiple parameter fractional Hartley transform (RPMPFrHT) is proposed. Firstly, we define an RPMPFrHT that make sure the output of cryptosystem is real-value. Then, based on random address sequences generated by coupled logistic function, we propose the double random scrambling encoding scheme which scrambled an image in the spatial domain and the RPMPFrHT domain respectively. Our method can encrypt an original image into noise-like picture with real-value which is convenient for storage and transmission. Numerical simulations have been performed and demonstrated that the proposed image encryption method is effective and sensitive to keys. Moreover, some potential attacks have also been performed to verify the robustness of the proposed method.

Index Terms— Image encryption, Hartley transform, fractional Hartley transform, logistic map, chaos scrambling.

1. INTRODUCTION

With the development of the Internet and communication, the exchange of image data for electronic commerce has been growing up. To protect the confidential images transmitted on Internet, various image encryption techniques have been proposed. Among those methods, the double random phase encoding (DRPE) method was considered to be an effective encryption scheme and have been used widely [1,2]. Moreover, many modified DRPE-based encryption techniques have been put forward and achieved good security [3-5]. Unnikrishnan's [3] first extended DRPE to the fractional Fourier transform (FrFT) domain, which was believed the first usage of the FrFT for image encryption [6]. Since then, researches noticed that fractional transforms have excellent properties and extra parameters which can enlarge the key space and improve the security of cryptosystems. Therefore, the image encryption methods based on fractional transforms have received increasing attention.

Lima [7] studied the performance of image encryption based on FrFT over finite fields. Sui [8] designed an asymmetric multiple-image encryption method based on coupled logistic maps in the FrFT domain and achieved good security. Tao [9] encrypted an image by multi-orders of the FrFT and analyzed its efficiency. To further enlarge the key space and improve the security of cryptosystem, some researchers have proposed multiple parameter FrFT (MPFrFT) [10-14]. In addition, combining with different scrambling technique, some encryption methods based on the fractional Hartley transform [15,16], fractional cosine transform [17,18], and fractional wavelet transform [19] have also been investigated. Although these fractional-transform-based encryption methods have good performance, their outputs are complex-value that is inconvenient for record and transmission. Venturini et al. [20] developed a methodology for obtaining variants of the discrete fractional Cosine (Sine) transform, which share real-valuedness and decentralization as well as most of properties required for a fractional transform. Based on this idea, some researchers have proposed the reality-preserving FrFT [6,21], reality-preserving fractional Mellin transform [22] and used them for image encryption.

So far, the reality-preserving multiple-parameter fractional Hartley transform (RPMPFrHT) has never been defined and its performance on image encryption has never been investigated. In this paper, for the first time to author's knowledge, we defined an RPMPFrHT and proposed a double random scrambling encoding scheme for image encryption. Firstly, we propose a constructed scheme for multiple-parameter fractional Hartley transform (MPFrHT) and its reality-preserving form. Then, we compared the MPFrHT and RPMPFrHT from the storage space and transformation efficiency. Finally, the double random scrambling encoding in the RPMPFrHT domain is performed, which not only have many parameters to serve as keys, but also can obtain real-value output that is convenient for image storage and transmission. Simulation results demonstrate that the proposed algorithm can get noise-like encrypted image and the cryptosystem is secure, sensitive to keys and robust to statistical attack and data loss.

2. PRELIMINARIES

The elements of the discrete Hartley transform matrix $\mathbf{H}$ are computed by

$$H_{mn} = 1/\sqrt{N}\left[\cos\left(2\pi mn/N\right)+\sin\left(2\pi mn/N\right)\right], \quad (1)$$

where $m,n = 0,1,\cdots,N-1$. The eigen-decomposition of the N-point Hartley transform matrix can be expressed by [23]

$$\mathbf{H} = \sum_{k=0}^{N-1}\exp\left[-j\pi k\right]\mathbf{u}_k\mathbf{u}_k^T, \quad (2)$$

where $\mathbf{u}_k$ is an eigenvector corresponding to the eigenvalue $\exp\left[-j\pi k\right]$, and can be obtained from the eigenvector of a real and symmetric matrix $\mathbf{S}$

$$\mathbf{S} = \begin{bmatrix} 2 & 1 & 0 & \cdots & 0 & 1 \\ 1 & 2\cos(2\pi/N) & 1 & \cdots & 0 & 0 \\ 0 & 1 & 2\cos(4\pi/N) & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 2\cos\left[2\pi(N-2)/N\right] & 1 \\ 1 & 0 & 0 & \cdots & 1 & 2\cos\left[2\pi(N-1)/N\right] \end{bmatrix}, \quad (3)$$

Taking the a-th power of eigenvalues for the matrix $\mathbf{H}$, Pei [23] defined the N-point FrHT kernel $\mathbf{H}^a$ as

$$\mathbf{H}^a = \mathbf{U}\mathbf{D}^a\mathbf{U}^T = \sum_{k=0}^{N-1}\exp\left[-j\pi ak\right]\mathbf{u}_k\mathbf{u}_k^T, \quad (4)$$

where $\mathbf{U} = \left[\mathbf{u}_0\middle|\mathbf{u}_1\middle|\cdots\middle|\mathbf{u}_{N-1}\right]$, and $\mathbf{u}_k$ is the same as the eigenvector of the Hartley transform.

3. THE PROPOSED RPMPFRHT

The FrHT is very closely related to the FrFT [23] whose multiplicity has been studied from the mathematical viewpoint [24]. Inspired by the computation methods of the FrFT [25], we will define the MPFrHT and its reality preserving form in this section.

3.1 The MPFrHT

Based on the computation method of the FrFT in [25], the FrHT kernel matrix in (4) can be rewritten as

$$\begin{aligned}\mathbf{H}^a &= \sum_{k=0}^{N-1}\left(\sum_{\ell=0}^{N-1} C_{\ell,a}\exp\left[-j\left(2\pi/N\right)\ell k\right]\right)\mathbf{u}_k\mathbf{u}_k^T \\ &= \sum_{\ell=0}^{N-1} C_{\ell,a}\left(\sum_{k=0}^{N-1}\exp\left[-j\left(2\pi/N\right)\ell k\right]\mathbf{u}_k\mathbf{u}_k^T\right) \\ &= \sum_{\ell=0}^{N-1} C_{\ell,a}\mathbf{H}^{\ell b}\end{aligned} \tag{5}$$

where $b=2/N$, and the weighting coefficients $C_{\ell,a}$ is defined as $C_{\ell,a}=\frac{1}{N}\cdot\frac{1-\exp\left[j\pi\cdot N\cdot\left(\ell b-a\right)\right]}{1-\exp\left[j\pi\left(\ell b-a\right)\right]}$.

Definition 1: Extending the order a to a N-dimensional vector $\bar{a}=\{a_0,a_1,\cdots,a_{N-1}\}\in\mathbb{R}^N$, we can define the MPFrHT as

$$\mathbf{H}^{\bar{a}}=\sum_{\ell=0}^{N-1}C_{\ell,a_\ell}\mathbf{H}^{\ell b},\ b=2/N \tag{6}$$

The weighting coefficients C_{ℓ,a_ℓ} is computed by

$$C_{\ell,a_\ell}=\frac{1}{N}\cdot\frac{1-\exp\left[j\pi\cdot N\cdot\left(\ell b-a_\ell\right)\right]}{1-\exp\left[j\pi\left(\ell b-a_\ell\right)\right]} \tag{7}$$

where $a_\ell,(\ell=0,1,\cdots,N-1)$ is mutual independent parameters.

It can be easily proved that the proposed MPFrHT in (6) possesses most of the desired properties for fractional transforms, such as, the boundary property, linearity, index commutativity, et al. However, it does not always satisfy the index additivity that is an essential property for a fractional operation. To solve this drawback, we give a selection strategy to the vector parameters.

Denote $\mathbf{C}_{\bar{b}}=\left(C_{0,b_0},C_{1,b_1},\cdots,C_{N-1,b_{N-1}}\right)$ as a coefficients vector, and $\mathrm{cir}^p\left(\mathbf{C}_{\bar{b}}\right)$ is the p-right circular shift of $\mathbf{C}_{\bar{b}}$, that is

$$\mathrm{cir}^p\left(\mathbf{C}_{\bar{b}}\right)=\left(C_{N-p,b_{N-p}},C_{N-p+1,b_{N-p+1}},\cdots,C_{N-p-1,b_{N-p-1}}\right),\quad p=0,1,\cdots \tag{8}$$

It can be trivially proof that for satisfying the index additivity, the following equality must be established.

$$\left(\mathrm{cir}^0\left(\mathbf{C}_{\bar{b}}\right),\mathrm{cir}^1\left(\mathbf{C}_{\bar{b}}\right),\cdots,\mathrm{cir}^{N-1}\left(\mathbf{C}_{\bar{b}}\right)\right)\cdot\mathbf{C}_{\bar{a}}=\mathbf{C}_{\bar{a}+\bar{b}} \tag{9}$$

where $\bar{a}$ and $\bar{b}$ are two independent fractional orders. We can easily find that if the elements in $\bar{a}$ and $\bar{b}$ are selected arbitrarily, the equality in (9) is not satisfied. Therefore, we must set some limits to the selection of weighting coefficients to satisfy index additivity property. Here we give a selection strategy to the vector parameters as

$$a_\ell=2a\left(\ell+r_\ell\right)/N\ell \tag{10}$$

where a is the transform order, $\left(r_0,r_1,\cdots,r_{N-1}\right)\in\mathbb{R}^N$. Note this is one but not the only one selection strategy to the vector parameters. So, the weighting coefficients can be computed as

$$\tilde{C}_{\ell,a_\ell}=\frac{1}{N}\sum_{n=0}^{N-1}\exp\left\{-j\frac{2\pi}{N}\left[a\left(n+r_\ell\right)-\ell n\right]\right\}. \tag{11}$$

In this case, the equation (9) will be satisfied. And the MPFrHT in (6) can be revised as

$$\tilde{\mathbf{H}}^{\bar{a}}=\sum_{\ell=0}^{N-1}\tilde{C}_{\ell,a_\ell}\mathbf{H}^{\ell b},\ b=2/N \tag{12}$$

We have $\tilde{\mathbf{H}}^{\bar{a}}\tilde{\mathbf{H}}^{\bar{b}}=\tilde{\mathbf{H}}^{\bar{a}+\bar{b}}$. Based on the index additivity, the inverse transform of revised MPFrHT can be simply given $\left(\tilde{\mathbf{H}}^{\bar{a}}\right)^{-1}=\tilde{\mathbf{H}}^{-\bar{a}}$.

The output of the MPFrHT is complex even if the input data is real. It is inconvenient for data record and transmission. Many practical applications, such as image compression, transmission and watermarking etc, are usually expected that when a transform is applied on real-valued data, we can also obtain real-valued outputs. Next, we define a reality-preserving form for the MPFrHT.

3.2 The RPMPFrHT

In this part, inspired by Venturini's technique [20], a RPMPFrHT are defined. The procedure is listed as follow.

① Let $x=\{x_1,x_2,\cdots,x_N\}^T$ be a real signal of length N, and $\tilde{\mathbf{H}}^{\bar{a}}$ be a MPFrHT matrix with size $N/2$.

② Let $\hat{x}=\{x_1+j\times x_{N/2+1},x_2+j\times x_{N/2+2},\cdots,x_{N/2}+j\times x_N\}^T$. It is a complex vector constructed from x as it is shown.

③ $\hat{y}=\tilde{\mathbf{H}}^{\bar{a}}\hat{x}$, and then construct $y=\left\{\mathrm{Re}(\hat{y}),\mathrm{Im}(\hat{y})\right\}^T$ as the output of the RPMPFrHT.

Rewriting the above procedure in matrix form, we can obtain

$$\begin{aligned}\hat{y}=\tilde{\mathbf{H}}^{\bar{a}}\hat{x} &= \left\{\mathrm{Re}\left(\tilde{\mathbf{H}}^{\bar{a}}\right)+j\times\mathrm{Im}\left(\tilde{\mathbf{H}}^{\bar{a}}\right)\right\}\left\{\mathrm{Re}\left(\hat{x}\right)+j\times\mathrm{Im}\left(\hat{x}\right)\right\} \\ &= \left\{\mathrm{Re}\left(\tilde{\mathbf{H}}^{\bar{a}}\right)\mathrm{Re}\left(\hat{x}\right)-\mathrm{Im}\left(\tilde{\mathbf{H}}^{\bar{a}}\right)\mathrm{Im}\left(\hat{x}\right)\right\} \\ &\quad + j\times\left\{\mathrm{Im}\left(\tilde{\mathbf{H}}^{\bar{a}}\right)\mathrm{Re}\left(\hat{x}\right)+\mathrm{Re}\left(\tilde{\mathbf{H}}^{\bar{a}}\right)\mathrm{Im}\left(\hat{x}\right)\right\}\end{aligned} \tag{13}$$

Therefore,

$$y=\begin{bmatrix}\mathrm{Re}\left(\tilde{\mathbf{H}}^{\bar{a}}\right) & -\mathrm{Im}\left(\tilde{\mathbf{H}}^{\bar{a}}\right)\\ \mathrm{Im}\left(\tilde{\mathbf{H}}^{\bar{a}}\right) & \mathrm{Re}\left(\tilde{\mathbf{H}}^{\bar{a}}\right)\end{bmatrix}\begin{bmatrix}\mathrm{Re}\left(\hat{x}\right)\\ \mathrm{Im}\left(\hat{x}\right)\end{bmatrix}=\mathbf{R}_H^{\bar{a}}x \tag{14}$$

Which means the 1D RPMPFrHT kernel matrix is

$$\mathbf{R}_H^{\bar{a}}=\begin{bmatrix}\mathrm{Re}\left(\tilde{\mathbf{H}}^{\bar{a}}\right) & -\mathrm{Im}\left(\tilde{\mathbf{H}}^{\bar{a}}\right)\\ \mathrm{Im}\left(\tilde{\mathbf{H}}^{\bar{a}}\right) & \mathrm{Re}\left(\tilde{\mathbf{H}}^{\bar{a}}\right)\end{bmatrix} \tag{15}$$

Definition 2: The 1D kernel $\mathbf{R}_H^{\bar{a}}$ can be extended to the 2D case by the tensor product as

$$\mathbf{R}_H^{(\bar{a},\bar{b})}=\mathbf{R}_H^{\bar{a}}\otimes\mathbf{R}_H^{\bar{b}} \tag{16}$$

where $\otimes$ denotes the tensor product, $\bar{a}$ and $\bar{b}$ are the individual fractional orders in two dimensions.

3.3 The Comparison of the MPFrHT and RPMPFrHT

In this part, we compare the differences of outputs between the MPFrHT and RPMPFrHT from the storage space taken up and transmission efficiency.

Suppose $\mathbf{X}$ is a 2D image with size $M\times N$, its MPFrHT is complex-valued and can be expressed as

$$\begin{aligned}\mathbf{X}_{MPFrHT}&=\mathbf{H}^{(\bar{a},\bar{b})}(\mathbf{X})=\tilde{\mathbf{H}}^{\bar{a}}\cdot\mathbf{X}\cdot\tilde{\mathbf{H}}^{\bar{b}}\\ &=\mathbf{X}_{MPFrHT\_real}+j\mathbf{X}_{MPFrHT\_imag}\end{aligned} \tag{17}$$

Here, the size of $\mathbf{X}_{MPFrHT\_real}$ and $\mathbf{X}_{MPFrHT\_imag}$ are both $M\times N$.

The RPMPFrHT of $\mathbf{X}$ is

$$\mathbf{X}_{RPMPFrHT}=\mathbf{R}_H^{(\bar{a},\bar{b})}(\mathbf{X})=\mathbf{R}_H^{\bar{a}}\cdot\mathbf{X}\cdot\mathbf{R}_H^{\bar{b}} \tag{18}$$

The output $\mathbf{X}_{RPMPFrHT}$ is real-valued image with size $M\times N$.

① When being stored on a computer, $\mathbf{X}_{RPMPFrHT}$ just need save the real-valued data. While $\mathbf{X}_{MPFrHT}$ must store both the real and imaginary parts. Therefore, the MPFrHT of a signal takes more storage space compared with that of the RPMPFrHT.

② When transmitting over digital communication channels, $\mathbf{X}_{MPFrHT}$ must transmit its real and imaginary parts simultaneously. Therefore, it is easy to understand that the transmission efficiency of the output of the RPMPFrHT is higher than that of the MPFrHT.

The above mentioned advantages of the RPMPFrHT make it more suitable for image encryption.

4. THE DOUBLE RANDOM SCRAMBLING ENCODING IN THE RPMPFRHT DOMAIN

In this section, we propose the double random scrambling encoding in the RPMPFrHT domain. The flowchart of the encryption scheme is illustrated in Fig.1.

Here, G denotes a plain image with size $M \times N$. $\mathbf{J}_1, \mathbf{J}_2$ are scrambling operators generated by a coupled logistic map that is believed to be a great tool for image encryption [8] and defined as

$$\begin{cases} x_{n+1} = \mu_1 x_n (1 - x_n) + \gamma_1 y_n^2 \\ y_{n+1} = \mu_2 y_n (1 - y_n) + \gamma_2 (x_n^2 + x_n y_n) \end{cases} \tag{19}$$

where $\mu_1, \mu_2, \gamma_1, \gamma_2$ are system parameters. $x_n, y_n \in (0,1)$, $n = 0,1,2,\cdots$ are random iterative values, x_0, y_0 are initial values. When $2.75 < \mu_1 < 3.4$, $2.75 < \mu_2 < 3.45$, $0.15 < \gamma_1 < 0.27$, and $0.13 < \gamma_2 < 0.15$, the 2D logistic map will exhibit chaotic behavior. That is, a large number of random iterative values limited in $(0,1)$ with desirable properties of non-correlation, pseudo-randomness can be generated. Using 2D logistic map, we produce scrambling operators $\mathbf{J}_1, \mathbf{J}_2$. The generation algorithm is shown in table I.

The encryption process can be formulated as follows

$$Q = \mathbf{R}_H^{(\bar{c},\bar{d})}\left\{\mathbf{J}_2\left\{\mathbf{R}_H^{(\bar{a},\bar{b})}\left\{\mathbf{J}_1\{G\}\right\}\right\}\right\} \tag{20}$$

The decryption process is the inverse of the encryption and it can be formulated as

$$G^* = \mathbf{J}_1^{-1}\left\{\mathbf{R}_H^{(-\bar{a},-\bar{b})}\left\{\mathbf{J}_2^{-1}\left\{\mathbf{R}_H^{(-\bar{c},-\bar{d})}\{Q\}\right\}\right\}\right\} \tag{21}$$

where Q denotes the encryption image, and G^* is the decryption image, $\mathbf{J}_i^{-1}$ is obtained by a reversed processing of Step5 in Table I. In our algorithm, the fractional orders $\bar{a}, \bar{b}, \bar{c}, \bar{d}$ and the logistic parameters $\mu_1, \mu_2, \gamma_1, \gamma_2$ and x_0, y_0 are served as keys.

5. EXPERIMENTAL RESULTS AND PERFORMANCE ANALYSIS

5.1 Experimental Results

Simulations are performed to verify the validity of the proposed algorithm in this section. The gray image "Lena" (Fig.2(a)) with size 256×256 is served as the plain image. The fractional orders of the RPMPFrHT $\bar{a}, \bar{b}, \bar{c}, \bar{d}$ are produced from a random number generator in MATLAB. Set the chaotic scrambling keys as $x_0 = 0.7145, y_0 = 0.3452; \mu_1 = 3.2478, \mu_2 = 2.9356; \gamma_1 = 0.2394, \gamma_2 = 0.1453.$

The encrypted image and decrypted image with correct keys are shown in Fig.2(b) and Fig.2(c), respectively. From Fig.2(b), we cannot get any information of the original image, which demonstrate the security of the proposed algorithm.

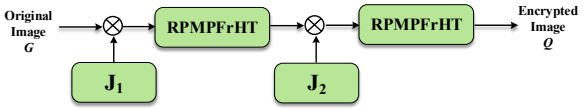


Fig. 1 The flowchart of encryption.

Table I. Random scrambling operator generation algorithm.

Step 1. Set initial values x_0, y_0, integer K_1, K_2;

Step 2. Set system parameters values $\mu_1, \mu_2, \gamma_1, \gamma_2$;

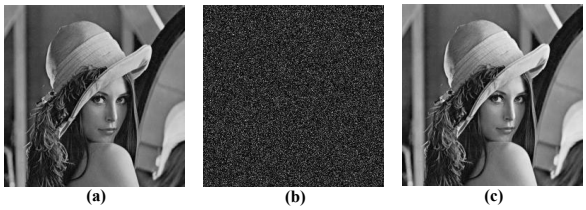
Step 3. Perform (26) and generate two sequences $\{x_{M\times N}\}, \{y_{M\times N}\}$;

Step 4. Sort the sequences in ascending order and obtain $\{x^*_{M\times N}\}, \{y^*_{M\times N}\}$;

Step 5. Generate two address sequences $\mathbf{d}_1, \mathbf{d}_2$, satisfy:

$$x_n^*(m) = x_{M\times N}(d_1(m))$$
$$y_n^*(m) = y_{M\times N}(d_2(m))$$

Step 6. Reshape address sequences $\mathbf{d}_1, \mathbf{d}_2$ to 2D with size $M \times N$, and obtain two random scrambling operator $\mathbf{J}_1, \mathbf{J}_2$



(a) (b) (c)

Fig.2 (a) original image, (b) encrypted image, (c) decrypted image with correct keys.

5.2 Sensitivity to the Keys

For a secure cryptosystems, the encrypted image should be highly sensitive to the variation of keys. Once a marginal difference is changed in the correct keys, the original image cannot be decrypted correctly. Next, we will analyze the sensitivity of the encrypted image to these keys.

To compare decryption examples of the encrypted image to wrong fractional orders, we set $\bar{a}' = \bar{a} + \bar{\delta}$, $\bar{b}' = \bar{b} + \bar{\delta}$, $\bar{c}' = \bar{c}' + \bar{\delta}$, $\bar{d}' = \bar{d}' + \bar{\delta}$, where $\bar{\delta} = 0.05$ is an error vector. The decrypted image is shown in Fig.3(a). We could not visually discern the original image from this result. Fig.3(b) display the MSE with the change of fractional orders. The x-axis δ represents the deviation distance to correct fractional-orders. When fractional-orders are correct, the MSE value approximates to zero. While when they slightly depart from the correct value, the MSE increase sharply. These results indicate that the encrypted image is sensitive to the variations of the fractional orders.

We also test the sensitivity of the encrypted image to logistic parameters and the results are displayed in Fig.4. Fig.4(a) and Fig.4(b) displays the decrypted images using $x_0 = 0.7145 + 1.0e^{-16}$, $y_0 = 0.3452 + 1.0e^{-16}$. Fig.4(c) and Fig.4(d) shows the decryption images using $\mu_1 = 3.2478 + 1.0e^{-15}$, $\mu_2 = 2.9356 + 1.0e^{-15}$. Fig.4(e) and Fig.4(f) are the decryption images using $\gamma_1 = 0.2394 + 1.0e^{-16}$, $\gamma_2 = 0.1453 + 1.0e^{-16}$. From the resultant images, we cannot get any information of the original image, which indicate the sensitivity of the encrypted image to the keys.

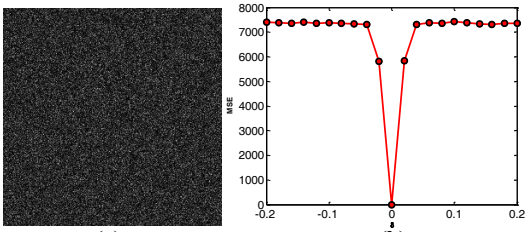


Fig.3 (a) Decryption with wrong fractional orders, (c) The MSE with the change of fractional orders.

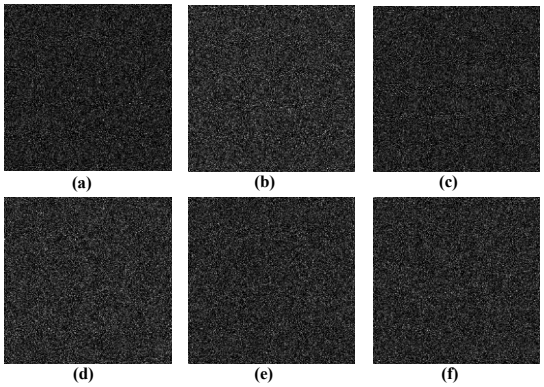


Fig.4 Decrypted images with wrong logistic parameters.

5.3 Robustness to the Statistical Attack

Statistical analysis is a commonly used method to demonstrate the confusion and diffusion properties of the encryption algorithm. This can be done by testing the distribution of pixels of the encrypted image and the correlation among the adjacent pixels.

Here, we randomly select 5000 pairs of adjacent pixels in vertical, horizontal and diagonal directions from the plain image and encrypted image to test the correlation that is computed by

$$CC = \frac{\sum_{i=1}^{N}(x_i-\bar{x})(y_i-\bar{y})}{\sqrt{\left(\sum_{i=1}^{N}(x_i-\bar{x})^2\right)\left(\sum_{i=1}^{N}(y_i-\bar{y})^2\right)}} \tag{22}$$

where $\bar{x} = 1/N\sum_{i=1}^{N} x_i$, $\bar{y} = 1/N\sum_{i=1}^{N} y_i$.

Fig.5 displays the correlation distribution of the plain image and encrypted image. It can be noted that two adjacent pixels of the plain images are significant correlated, while that of the encrypted image are low. This indicates that after encryption the correlation among the image pixels is broken.

Histogram is another tool to analyze the statistical feature of an image. Fig.6 shows the histograms of original image "Lena" and its encrypted image. They are obviously different and demonstrate that the encrypted image does not provide any information regarding the distribution of intensity values to the attacker.

5.4 Robustness to the data loss Attack

When transmitting on insecure communication channels, some information of the encrypted image may be lost. To check the robustness of our algorithm to data loss, we occlude 25%, 50% of the encrypted image pixels. Fig.7 shows the decrypted results. The recovered images are visual recognizable because the algorithm has distributed the energy of original image over the entire output plain. Therefore, our algorithm provides robustness to the distortions due to loss of encrypted data.

5.5 Comparison with Existing Methods

In this part, we compare our proposed algorithm with existing

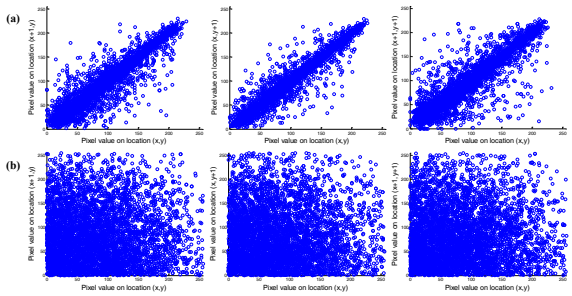


Fig.5 Correlation of adjacent pixels in horizontal, vertical, diagonal direction, (a) original image (b) encrypted image.

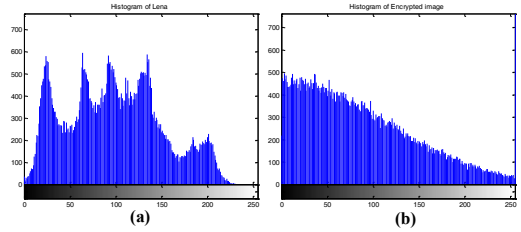


Fig.6 Histogram of images. (a) original image, (b) encrypted image.

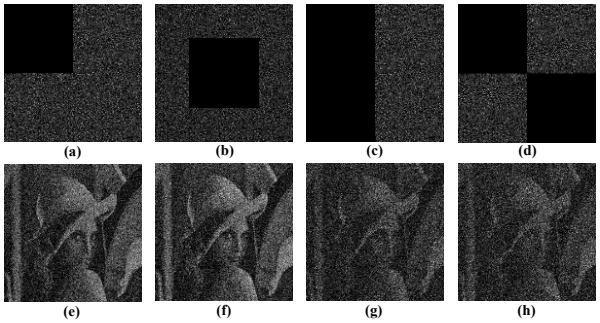


Fig.7 Decrypted image compounding to different data loss.

Table II. Comparison of correlation of encrypted image Lena.

	Original Image	Our Method	Lima's [7]	Liu's [26]	Zhou's [27]
Horizontal	0.9420	0.0017	0.0020	0.0030	0.0846
Vertical	0.9720	0.0028	0.0062	−0.0024	0.0583
Diagonal	0.9180	0.0020	0.0066	−0.0034	0.0931

methods from the aspect of decorrelation ability. Table II shows the results and indicates that the proposed scheme has a good decorrelation ability compared with [7],[26],[27], which imply robust security.

6. CONCLUSION

In this paper, we first define a RPMPFrHT, and then, propose a double random scrambling encoding in the RPMPFrHT domain. Simulation results demonstrate that the proposed algorithm is secure, sensitive to keys and robust to statistical attack and data loss.

7. ACKNOWLEDGEMENT

This research is supported by the Fundamental Research Funds for the Central Universities (2017RC52).

11. REFERENCES

[1] P. Refregier, B. Javidi, "Optical image encryption based on input plane and Fourier plane random encoding," *Optics Letters*, vol. 20, no. 7, pp. 767-769, 1995.

[2] X.X. Li, D.M. Zhao, "Optical color image encryption with redefined fractional Hartley transform," *Optik*, vol. 121, no. 7, pp. 673-677, 2010.

[3] G. Unnikrishnan, J. Joseph, K. Singh, "Optical encryption by double-random phase encoding in the fractional Fourier domain," *Optics Letters*, vol. 25, no. 12, pp. 887-889, 2000.

[4] G. Situ, J. Zhang, "Double random-phase encoding in the Fresnel domain," *Optic Letters*, vol. 29, pp. 1584-1586, 2004.

[5] J. Chen, Z. Zhu, Z. Liu, C. Fu, L. Zhang, H. Yu, "A novel double-image encryption scheme based on cross-image pixel scrambling in gyrator domains," *Optic Express*, vol. 22, pp. 7349-7361, 2014.

[6] Y. Xin, R. Tao, and Y. Wang, "Image encryption based on a novel reality-preserving fractional Fourier transform," *In Proceedings of the first International Conference on Innovative Computing, Information and Control (ICICIC)*, pp. 1-4, 2006.

[7] J.B. Lima, L.F. Novaes, "Image encryption based on the fractional Fourier transform over finite fields," *Signal Processing*, vol. 94, pp. 521-530, 2014

[8] L.S. Sui, K.K. Duan, J.L. Liang, Z.Q. Zhang, H.N. Meng, "Asymmetric multiple-image encryption based on coupled logistic maps in fractional Fourier transform domain," *Optics and Lasers in Engineering*, vol. 62, pp. 139-152, 2014.

[9] R. Tao, X.Y. Meng, and Y. Wang, "Image encryption with multiorders of fractional Fourier transforms," *IEEE Transactions on Information Forensics and Security*, vol. 5, no. 4, pp. 734-738, 2010.

[10] J. Lang, R. Tao, Y. Wang, "Image encryption based on the multiple-parameter discrete fractional Fourier transform and chaos function," *Optics Communications*, vol. 283, no.10, pp. 2092-2096, 2010.

[11] S.C. Pei, W.L. Hsue, "The multiple-parameter discrete fractional Fourier transform," *IEEE Signal Processing Letters*, vol. 13, no. 6, pp. 329-332, 2006.

[12] Q.W. Ran, H.Y. Zhang, J. Zhang, L.Y. Tan, J. Ma, "Deficiencies of the cryptography based on multiple-parameter fractional Fourier transform," *Optics Letters*, vol. 34, no. 11, pp. 1729-1731, 2009.

[13] T.Y. Zhao, Q.W. Ran, L. Yuan, Y.Y. Chi, J. Ma, "Security of image encryption scheme based on multi-parameter fractional Fourier transform," *Optics Communications*, vol. 376, pp. 47-51, 2016.

[14] X.J. Kang, R. Tao, F. Zhang, "Multiple-Parameter Discrete Fractional Transform and its Applications," *IEEE Transactions on Signal Processing*, vol. 64,no. 13, pp. 3402-3417, 2016.

[15] Y. Liu, J. Du, J.H. Fan, and L.H. Gong, "Single-channel color image encryption algorithm based on fractional Hartley transform and vector operation," *Multimedia Tools and Applications*, vol. 74, no. 9, pp. 3171-3182, 2015.

[16] X.X. Li and D.M. Zhao, "Optical color image encryption with redefined fractional Hartley transform," *Optik*, vol. 121, no. 7, pp. 673-677, 2010.

[17] Z.J. Liu, L. Xu, T. Liu, H. Chen, and P.F. Li, "Color image encryption by using Arnold transform and color-blend operation in discrete cosine transform domains," *Optics Communications*, vol. 284, no. 1, pp. 123-128, 2011.

[18] J.H. Wu, F.F. Guo, Y.R. Liang and N.R. Zhou, "Triple color images encryption algorithm based on scrambling and the reality-preserving fractional discrete cosine transform," *Optik*, vol. 125, no. 16, pp. 4474-4479, 2014.

[19] L.F. Chen, D.M. Zhao, "Optical image encryption based on fractional wavelet transform," *Optics Communications*, vol. 254, pp. 361-367, 2005.

[20] I. Venturini and P. Duhamel, "Reality preserving fractional transforms," *In Proc. ICASSP*, pp. 205-208, 2004.

[21] J. Lang, "Color image encryption based on color blend and chaos permutation in the reality-preserving multiple-parameter fractional Fourier transform domain," *Optics Communications*, vol. 338, pp. 181-192, 2015.

[22] N.R. Zhou, Y.X. Wang, L.H. Gong, and X.B. Chen, "Novel color image encryption algorithm based on the reality preserving fractional Mellin transform," *Optics and Lasers in Engineering*, vol. 44, no. 7, pp. 2270-2281, 2012.

[23] S.C. Pei, C.C. Tseng, M.H. Yeh, and J.J. Shyu, "Discrete fractional Hartley and Fourier transforms," *IEEE Transactions on Circuits and Systerms*, vol. 45, no. 6, pp. 665-675, 1998.

[24] G. Cariolaro, T. Erseghe, P. Kraniauskas, and N. Laurenti, "Multiplicity of fractional Fourier transforms and their relationships," *IEEE Transactions on Signal Processing*, vol. 48, no. 1, pp. 227-241, 2000.

[25] M.H. Yeh and S.C. Pei, "A method for the discrete fractional Fourier transform computation," *IEEE Transactions on Signal Processing*, vol. 51, no. 3, pp. 889-891, 2003.

[26] W.H. Liu, K.H. Sun, C.X. Zhu, "A fast image encryption algorithm based on chaotic map," *Optics and Lasers In Engineering*, vol. 84, pp. 26-36, 2016.

[27] N.R. Zhou, A.D. Zhang, F. Zheng, L.H. Gong, " Novel image compression-encryption hybrid algorithm based on key-controlled measurement matrix in compressive sensing," *Optics and Laser Technology*, vol. 62, pp. 152-160, 2014.