Image Encryption With Multiorders of Fractional Fourier Transforms

Ran Tao, *Senior Member, IEEE*, Xiang-Yi Meng, *Student Member, IEEE*, and Yue Wang

***Abstract*—The original information in the existing security system based on the fractional Fourier transform (FRFT) is essentially protected by only a certain order of FRFT. In this paper, we propose a novel method to encrypt an image by multiorders of FRFT. In the image encryption, the encrypted image is obtained by the summation of different orders inverse discrete FRFT of the interpolated subimages. And the original image can be perfectly recovered using the linear system constructed by the fractional Fourier domain analysis of the interpolation. The proposed method can be applied to the double or more image encryptions. Applying the transform orders of the utilized FRFT as secret keys, the proposed method is with a larger key space than the existing security systems based on the FRFT. Additionally, the encryption scheme can be realized by the fast-Fourier-transform-based algorithm and the computation burden shows a linear increase with the extension of the key space. It is verified by the experimental results that the image decryption is highly sensitive to the deviations in the transform orders.**

***Index Terms*—Discrete fractional Fourier transform (DFRFT), fractional Fourier transform (FRFT), image encryption, interpolation, linear system.**

NOMENCLATURE

FT	Fourier transform.
FD	Fourier domain.
FRFT	Fractional Fourier transform.
FRFD	Fractional Fourier domain.
DFRFT	Discrete fractional Fourier transform.
IDFRFT	Inverse discrete fractional Fourier transform.

I. INTRODUCTION

THE fractional Fourier transform (FRFT) is more flexible than the conventional Fourier transform (FT) due to the extra parameter of the transform order. With the transform order gradually varying from 0 to 1, the FRFT of a signal can develop from the original function to its FT [1]–[4]. Thus, it has recently shown its potential in the fields of the image and the optical encryption. Using the transform order to enlarge the key space, the systems based on the FRFT are of a higher security than the corresponding systems based on the FT or cosine transform [5]–[12].

However, the traditional information security systems based on the FRFT are only the rotation of the corresponding Fourier-based systems in the time-frequency plane, i.e., the FT or the Fourier domain (FD) is replaced by the FRFT or the fractional Fourier domain (FRFD) [9]–[11]. Even if some systems are constructed by the cascade of different orders of FRFT, the image is also protected by being transformed into a certain order of FRFD due to the additive property of rotations [5]–[8]. In this paper, we will propose a novel method to encrypt an image by multiorders of FRFT. In the image encryption, the original image is first equally divided into several subimages. Then, the encrypted image is obtained by the summation of different orders of inverse discrete fractional Fourier transform (IDFRFT) of the interpolated subimages. Thus, the original image is protected by multiorders of FRFT. However, in the image decryption, different encrypted subimages cannot be recovered by the corresponding FRFT due to the nonorthogonality among the kernel functions of different orders of FRFT. In order to solve this problem, we propose a decryption algorithm using the linear system constructed by the FRFD analysis of the interpolation, in which the decryption of each subimage needs the whole transform orders of the utilized FRFT. Applying the transform orders as the security keys, the proposed method is with a larger key space than the existing image encryption systems based on the FRFT. Additionally, the proposed method can be applied to the double or more image encryptions. It is also analyzed based on the property of the utilized discrete fractional Fourier transform (DFRFT) that the encryption scheme can be realized by the fast Fourier transform (FFT)-based algorithm and the computation burden shows a linear increase with the extension of the key space. Simulation results demonstrate that the image decryption is highly sensitive to the deviations in the security keys.

The rest of this paper is organized as follows. In Section II, the novel encryption and the decryption principles are proposed. In Section III, we present the detailed performance analysis of the proposed method. In Section IV, the performance of the proposed method is verified by the simulation examples. Finally, in Section V, we make a conclusion.

Notations: The matrices are denoted by boldface capital letters (e.g., $\boldsymbol{S}$). $\boldsymbol{F}_p^N$ expresses the pth-order DFRFT matrix for N-length sequences. Superscripts $(\cdot)^T$ and $(\cdot)^H$ stand for transposition and Hermite transposition, respectively. The

Manuscript received February 04, 2010; revised July 22, 2010; accepted August 05, 2010. Date of publication August 19, 2010; date of current version November 17, 2010. This work was supported in part by the National Science Foundation of China for Distinguished Young Scholars under Grant 60625104 and in part by the Foundation for Beijing excellent Ph.D. thesis under Grant 1320037010901. The associate editor coordinating the review of this manuscript and approving it for publication was Dr. Wenjun Zeng.

The authors are with the Department of Electronic Engineering, Beijing Institute of Technology, Beijing 100081, China (e-mail: rantao@bit.edu.cn; mxy0827@bit.edu.cn).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TIFS.2010.2068289

signal vectors are denoted by boldface small letters with an overbar (e.g., $\vec{\boldsymbol{x}}$). The element in the row m and column n of the matrix $\boldsymbol{A}$ with dimension $M \times N$ is expressed as $[\boldsymbol{A}]_{m,n}$, where $m = 1, 2, \ldots, M$ and $n = 1, 2, \ldots, N$. The nth element in an N-length $\vec{\boldsymbol{x}}$ is expressed as $[\vec{\boldsymbol{x}}]_n$, where $n = 1, 2, \ldots, N$.

II. Principle of Encryption/Decryption

A. FRFT and DFRFT

The pth-order FRFT of a signal is defined as

$$\{F_p[x(t)]\}(u) = \int_{-\infty}^{+\infty} x(t) K_p(u,t) dt$$

where

$$K_p(u,t) = \begin{cases} A_p \exp\left[j\frac{t^2+u^2}{2} \cdot \cot\left(\frac{p\pi}{2}\right) - jut \cdot \csc\left(\frac{p\pi}{2}\right)\right], & p \neq 2n \\ \delta(t-u), & p = 4n \\ \delta(t+u), & p = 4n \pm 2 \end{cases}$$

in which $A_p = \sqrt{[1 - j \cdot \cot(p\pi/2)]/(2\pi)}$ and $n \in \mathbf{Z}$ [1]. Since the FRFT is periodic with the period of 4, the transform order can be limited in the interval $[-2, 2]$. In this paper, the FRFT with $p = 2n$ is not taken into consideration. Additionally, $F_p[x(t)](u) = F_{p+2}[x(t)](-u)$. So it can be assumed that $p \in (0, 2)$, i.e., $\sin(p\pi/2) > 0$, in the derivations.

The algorithms for the DFRFT are divided into sampling discretization-type, eigenvector decomposition-type, linear combination-type, etc. The proposed method in this paper is based on the FRFD analysis of the interpolation. Thus, the sampling discretization-type [13], which can be expressed in a closed form, is utilized. Let $\boldsymbol{F}_p^N \in \mathbb{C}^{N \times N}$ be the matrix expressing the pth-order DFRFT for an N-length sequence; it is written as

$$\boldsymbol{F}_p^N = \boldsymbol{\Lambda}_{p,u}^N \cdot \boldsymbol{W}^N \cdot \boldsymbol{\Lambda}_{p,t}^N \tag{1}$$

where the matrix $\boldsymbol{W}^N \in \mathbb{C}^{N \times N}$ and the diagonal matrices $\Lambda_{p,u}^N, \Lambda_{p,t}^N \in \mathbb{C}^{N \times N}$ are defined as

$$[\boldsymbol{W}^N]_{m,n} = e^{-j\frac{2\pi}{N}(m-1)(n-1)}$$
$$\left[\boldsymbol{\Lambda}_{p,t}^N\right]_{n,n} = e^{j\frac{1}{2}\cot\left(\frac{p\pi}{2}\right)\cdot(n-1)^2\cdot\Delta t^2}$$

and

$$\left[\boldsymbol{\Lambda}_{p,u}^N\right]_{n,n} = e^{j\frac{1}{2}\cot\left(\frac{p\pi}{2}\right)\cdot(n-1)^2\cdot\Delta u_p^2}$$

in which Δt and $\Delta u_p = 2\pi \sin(p\pi/2)/(N\Delta t)$ are the sampling intervals in the time domain and the pth-order FRFD, respectively. Correspondingly, the pth-order IDFRFT for an N-length sequence, which is equivalent to the $-p$th-order DFRFT, can be expressed as the Hermite transposition of $\boldsymbol{F}_p^N$, i.e.,

$$\boldsymbol{F}_{-p}^N = \left(\boldsymbol{F}_p^N\right)^H = \boldsymbol{\Lambda}_{-p,t}^N \cdot (\boldsymbol{W}^N)^H \cdot \boldsymbol{\Lambda}_{-p,u}^N. \tag{2}$$

B. Image Encryption

Considering an original image $\boldsymbol{S}$ with a size of $A \times B$, if the column and row vectors are M-fold and N-fold equally divided, then the original image can be divided into $M \times N$ subimages $\boldsymbol{S}_{a,b}$, $a = 1, 2, \ldots, M$ and $b = 1, 2, \ldots, N$, with a size of $(A/M) \times (B/N)$, which are given by

$$[\boldsymbol{S}_{a,b}]_{m,n} = [\boldsymbol{S}]_{(a-1)A/M+m,(b-1)B/N+n}.$$

In the image encryption, if the column vectors of $\boldsymbol{S}_{a,b}$ are M-fold interpolated and further $p_{a,b,1}$th-order inverse discrete fractional Fourier transformed while the row vectors are N-fold interpolated and further $p_{a,b,2}$th inverse discrete fractional Fourier transformed, then we can obtain the encrypted subimages $\boldsymbol{Y}_{a,b}$ based on the FRFD analysis of the interpolation [14], [15]

$$\boldsymbol{Y}_{a,b} = \begin{bmatrix} \boldsymbol{D}_{p_{a,b,1},0} \\ \boldsymbol{D}_{p_{a,b,1},1} \\ \vdots \\ \boldsymbol{D}_{p_{a,b,1},M-1} \end{bmatrix} \cdot \boldsymbol{X}_{a,b} \cdot \begin{bmatrix} \boldsymbol{E}_{p_{a,b,2},0} & \boldsymbol{E}_{p_{a,b,2},1} & \cdots & \boldsymbol{E}_{p_{a,b,2},N-1} \end{bmatrix} \tag{3}$$

where the matrix $X_{a,b} \in \mathbb{C}^{(A/M)\times(B/N)}$ is the two-dimensional IDFRFT of $\boldsymbol{S}_{a,b}$, which is given by

$$\boldsymbol{X}_{a,b} = \boldsymbol{F}_{-p_{a,b,1}}^{A/M} \cdot \boldsymbol{S}_{a,b} \cdot \left(\boldsymbol{F}_{-p_{a,b,2}}^{B/N}\right)^T$$

and the diagonal matrices $\boldsymbol{D}_{p_{a,b,1},l} \in \mathbb{C}^{(A/M)\times(A/M)}$, $l = 0, 1, \ldots, M-1$, and $\boldsymbol{E}_{p_{a,b,2},k} \in \mathbb{C}^{(B/N)\times(B/N)}$, $k = 0, 1, \ldots, N-1$, are expressed as

$$\left[\boldsymbol{D}_{p_{a,b,1},l}\right]_{n,n} = e^{-j\cdot\frac{1}{2}\cdot\cot\left(\frac{p_{a,b,1}\pi}{2}\right)\cdot\left[2\cdot(n-1)\cdot l\cdot(A/M)+l^2\cdot(A/M)^2\right]\Delta t^2}$$

and

$$\left[\boldsymbol{E}_{p_{a,b,2},k}\right]_{n,n} = e^{-j\cdot\frac{1}{2}\cdot\cot\left(\frac{p_{a,b,2}\pi}{2}\right)\cdot\left[2\cdot(n-1)\cdot k\cdot(B/N)+k^2\cdot(B/N)^2\right]\cdot\Delta t^2}.$$

Furthermore, we can obtain the encrypted image $\boldsymbol{Y}$ by the summation of $\boldsymbol{Y}_{a,b}$, i.e.,

$$\boldsymbol{Y} = \sum_{a=1}^{M}\sum_{b=1}^{N} \boldsymbol{Y}_{a,b}. \tag{4}$$

C. Image Decryption

In the image decryption, the decrypted subimages cannot be derived from the inner product of the encrypted image and the corresponding kernel functions due to the nonorthogonality among the kernel functions of different orders of FRFT. In order to solve this problem, this subsection proposes a method to derive the IDFRFT of the decrypted subimages (i.e., $\hat{\boldsymbol{X}}_{a,b}$) from the encrypted image through the linear system constructed by (3) and (4).

Given the diagonal matrices $\boldsymbol{D}_{p_{a,b,1},l}$ and $\boldsymbol{E}_{p_{a,b,2},k}$, we can derive the relationship between the original image and the encrypted image as shown in the following linear equation from (3) and (4):

$$\sum_{a=1}^{M}\sum_{b=1}^{N}\left[\boldsymbol{D}_{p_{a,b,1},l}\right]_{m,m}\cdot\left[\boldsymbol{X}_{a,b}\right]_{m,n}\cdot\left[\boldsymbol{E}_{p_{a,b,2},k}\right]_{n,n} = [\boldsymbol{Y}]_{l(A/M)+m,k(B/N)+n}. \quad (5)$$

With the selection of l from 0 to $M-1$ and k from 0 to $N-1$, we can obtain a linear system comprised of $M \times N$ linear equations in the form as shown in (5). Furthermore, the pixel (m,n) in $\hat{\boldsymbol{X}}_{a,b}$ can be written as

$$[\hat{\boldsymbol{X}}_{a,b}]_{m,n} = [\vec{\boldsymbol{z}}_{m,n}]_{(a-1)N+b} \quad (6)$$

where $\vec{\boldsymbol{z}}_{m,n} \in \mathbb{C}^{MN\times 1}$ is written as

$$\vec{\boldsymbol{z}}_{m,n} = \boldsymbol{C}_{m,n}^{-1}\cdot\vec{\boldsymbol{r}}_{m,n} \quad (7)$$

in which $\vec{\boldsymbol{r}}_{m,n} \in \mathbb{C}^{MN\times 1}$ and $\boldsymbol{C}_{m,n} \in \mathbb{C}^{MN\times MN}$ are given by

$$[\vec{\boldsymbol{r}}_{m,n}]_{(a-1)N+b} = [\boldsymbol{Y}]_{(a-1)(A/M)+m,(b-1)(B/N)+n}$$
$$[\boldsymbol{C}_{m,n}]_{lN+k+1,(a-1)N+b} = \left[\boldsymbol{D}_{p_{a,b,1},l}\right]_{m,m}\cdot\left[\boldsymbol{E}_{p_{a,b,2},k}\right]_{n,n}.$$

Then, each decrypted subimage $\hat{\boldsymbol{S}}_{a,b}$ can be obtained by the corresponding two-dimensional DFRFT of $\hat{\boldsymbol{X}}_{a,b}$, i.e.,

$$\hat{\boldsymbol{S}}_{a,b} = \boldsymbol{F}_{p_{a,b,1}}^{A/M}\cdot\hat{\boldsymbol{X}}_{a,b}\cdot\left(\boldsymbol{F}_{p_{a,b,2}}^{B/N}\right)^{T}. \quad (8)$$

At last, the decrypted image is reconstructed by the decrypted subimages $\hat{\boldsymbol{S}}_{a,b}$.

III. Analysis and Discussion

A. Feature of Proposed Method

In the proposed method, the original image is first equally divided into $M \times N$ subimages and the encrypted image is obtained by summing the two-dimensional IDFRFT of the interpolated subimages. That is to say, the different parts of the original image are converted into an encrypted image of the same size as the original image. Thus, the proposed method can also be applied to double or more image encryptions by regarding the original images as subimages, which is impossible for most of the traditional methods based on the FRFT [7], [9]–[11]. Even if the methods based on the random phase coding in the FRFD can also realize the double image encryptions [8], these methods cannot deal with the case when the amount of the original images is more than two. It should be noted that the encrypted image is of a larger size than the original images, which is different from the traditional methods, such as the random phase coding.

B. Security

In the image decryption, the transform orders of the IDFRFT are used as the secret keys. Although different parts of the original image are processed by different orders of IDFRFT, it is demonstrated in (6) and (7) that the decryption of each subimage needs the whole transform orders due to the nonorthogonality among the kernel functions of different orders of FRFT. The amount of the keys is equal to two times the amount of the subimages and it can also be set arbitrarily large if and only if the invertibility of the matrix $\boldsymbol{C}_{m,n}$ in (7) is satisfied. In the limit case, for an original image with a size of $A \times B$, the image can be equally divided into the subimages of only one pixel and the amount of secret keys will approach as much as $2 \times A \times B$. Compared with the existing image encryption method based on the FRFT, the proposed method is with a larger key space, i.e., a higher security. We can also combine the proposed algorithm with the other encryption methods to further enhance the security of the system.

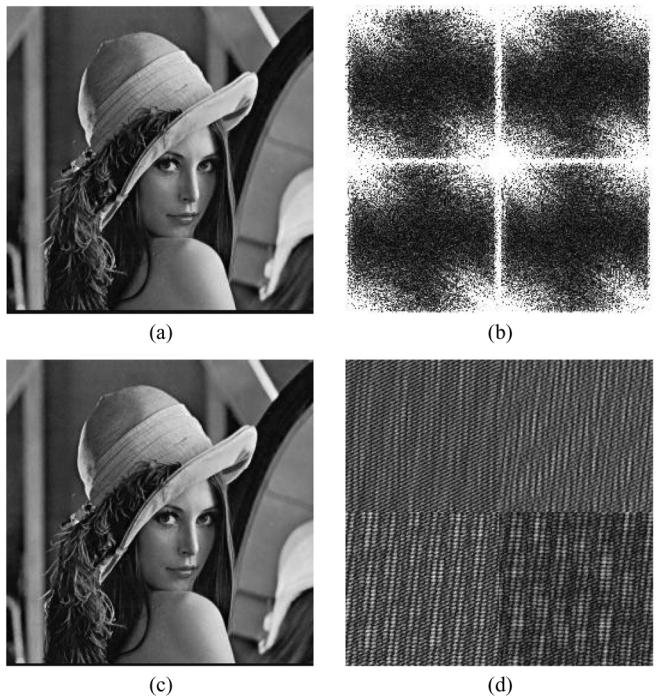


Fig. 1. (a) Original image; (b) encrypted image; (c) correct decrypted image; and (d) decrypted image with incorrect transform orders.

C. Complexity Analysis

The image encryption process with $2 \times M \times N$ secret keys is mainly implemented by $M \times N$ times two-dimensional IDFRFT. The utilized DFRFT and IDFRFT in (1) and (2) can be realized by the FFT and inverse FFT (IFFT). Considering an image with a size of $A \times B$, if the radix-2 FFT is used, the complexity of the proposed encryption process is simply $MN \cdot (AB/2) \cdot [\log_2(AB) + 8]$ complex multiplications. The computational burden of the proposed encryption method shows a linear increase with the extension of the key space.

The image decryption process is mainly carried out by (6), (7), and (8). The computational burden of the decryption mainly consists of the matrices inversions and multiplications in (7) and the two-dimensional DFRFT in (8). Because the complexity of the matrix inversion in (7) is assumed to be $\boldsymbol{O}(M^3N^3/2)$ multiplications [16], the complexity of the proposed decryption

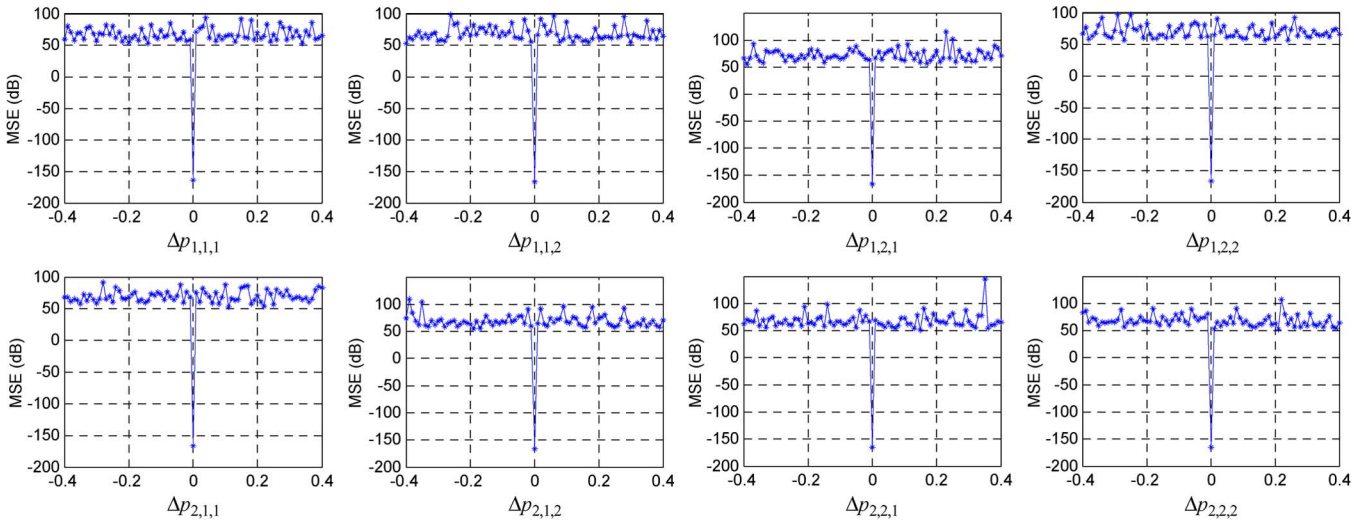


Fig. 2. MSE between the original image and the decrypted image via deviation in transform orders.

process is simply $(AB/2)\cdot\{\log_2[(A/M)(B/N)]+8\}+AB\cdot[\boldsymbol{O}(M^3N^3/2)/(MN)+MN]$ complex multiplications. However, in practice, the inverse matrix of $\boldsymbol{C}_{m,n}$ can be previously restored as the secret keys by the users. Thus, the matrix inversion in (7) can be neglected and the complexity of the decryption will reduce to $(AB/2)\cdot\{\log_2[(A/M)(B/N)]+8+2MN\}$ complex multiplications. So the computational burden of the proposed decryption method also shows a linear increase with the extension of the key space due to the fact that the variation of $\log_2[(A/M)(B/N)]$ can be neglected compared with $2MN$.

In the existing encryption methods based on the FRFT, the eigenvector decomposition-type DFRFT is used. This type of the DFRFT lacks fast algorithms. The encryption and the decryption procedures are both realized by the matrix multiplications. For an image with a size of $A\times B$, the complexity of the encryption and the decryption is about equal to or a small integral multiple of A^2B+AB^2 complex multiplications. Therefore, let $m=2\times M\times N$ be the amount of the secret keys for the proposed method,

if $m\le 4(A+B)/[\log_2(AB)+8]$, the complexity of the proposed encryption scheme is lower than the existing methods;

if $m-\log_2(m/2)\le 2(A+B)-\log_2(AB)-8$, the complexity of the proposed decryption scheme is lower than the existing methods.

Above all, we can find that the proposed algorithm is of a lower complexity than the existing encryption method based on the FRFT when the amount of the secret keys is not so large.

IV. Experimental Results

In this section, we will test the performance of the proposed encryption technique. The performance is measured by the mean square error (MSE) between the original image and the decrypted image, i.e.,

$$\mathrm{MSE}=\frac{1}{AB}\sum_{m=1}^{A}\sum_{n=1}^{B}\left[\hat{\boldsymbol{S}}(m,n)-\boldsymbol{S}(m,n)\right]^2$$

where A and B indicate the size of the image while $\boldsymbol{S}(m,n)$ and $\hat{\boldsymbol{S}}(m,n)$ denote the amplitudes of the original and the decrypted images of the pixel (m,n), respectively.

The grayscale image of "Lena" with a size of 256 × 256, as shown in Fig. 1(a), is serving as the original image. Simply, the column and the row vectors are both two-fold equally divided ($M=2$, $N=2$), i.e., the original image is divided into four subimages with a size of 128 × 128 and the amount of secret keys is $2\times M\times N=8$. The orders of the IDFRFT for the column vectors of each subimage are set as $p_{1,1,1}=0.41$, $p_{1,2,1}=0.43$, $p_{2,1,1}=0.45$, and $p_{2,2,1}=0.47$ while the orders of the IDFRFT for the row vectors of each subimage are set as $p_{1,1,2}=0.42$, $p_{1,2,2}=0.44$, $p_{2,1,2}=0.46$, and $p_{2,2,2}=0.48$. Then, the amplitude of the encrypted image is shown in Fig. 1(b).

The decryption of the image as shown in Fig. 1(b) can be realized using (6), (7), and (8). The transform orders of the utilized IDFRFT are used as the secret keys. Fig. 1(c) shows the decrypted image with the correct transform orders. Fig. 1(d) is the decrypted image with the incorrect $p_{1,1,1}$ ($p_{1,1,1}=0.4$) while the others are correct. The MSE between the original image and the decrypted image is 58.98 dB. From Fig. 1(d), we can find that a little deviation in any secret key will result in the large errors for whole subimages.

In addition, we study the sensitivity of the transform orders. Let $\Delta p_{a,b,i}$ be the deviation in the transform orders $p_{a,b,i}$, $i=1,2$. The curves in Fig. 2 demonstrate the MSE between the original image and the decrypted image as a function of $\Delta p_{a,b,i}$. It is noted from Fig. 2 that a deviation of 0.01 in any secret key will result in the MSE more than 50 dB. The encrypted image can be perfectly decrypted if and only if the transform orders are all matched precisely. For an unauthorized user, he has to test at least $200^{2M\times N}$ combinations of the secret keys to decrypt the image. When M and N are set as the least value of 2 as shown in this section, the amount of the combinations to be tested is more than 2×10^{18}. So the blind image decryption is a sufficiently impossible task for an unauthorized user. Thus, the transform

orders of the utilized DFRFT can be used as the secret keys to protect the original image.

V. Conclusion

In this paper, we have proposed a novel method to encrypt an image by multiorders of FRFT. The encrypted image is obtained by the summation of different orders of IDFRFT of the interpolated subimages. The whole transform orders of the utilized FRFT are used as the secret keys for the decryption of each subimage. It is verified by the experimental results that the image decryption is highly sensitive to the deviations in the transform orders. Compared with the traditional image encryption methods based on the FRFT, the proposed method is with a larger key space and the amount of keys can be set as large as two times the amount of the pixels in the original image. The proposed encryption scheme can also be realized by the FFT-based algorithms and the computation burden shows a linear increase with the extension of the key space. In addition, the proposed method can be applied in the double or more image encryptions. In future work, we can also combine the proposed method with other image encryption methods to enhance the security of the system.

References

[1] H. M. Ozaktas, Z. Zalevsky, and M. A. Kutay, *The Fractional Fourier Transform*. West Sussex, U. K.: Wiley, 2001.

[2] L. B. Almeida, "The fractional Fourier transform and time-frequency representations," *IEEE Trans. Signal Process.*, vol. 42, no. 11, pp. 3084–3091, Nov. 1996.

[3] D. Mustard, "The fractional Fourier transform and the Wigner distribution," *J. Aust. Math. Soc. B*, vol. 38, pp. 209–219, 1996.

[4] R. Tao, B. Deng, and Y. Wang, "Research progress of the fractional Fourier transform in signal processing," *Science in China (Ser.F, Information Science)*, vol. 49, pp. 1–25, Jan. 2006.

[5] G. Unnikrishnan and K. Singh, "Double random fractional Fourier-domain encoding for optical security," *Opt. Eng.*, vol. 39, pp. 2853–2859, 2000.

[6] G. Unnikrishnan, J. Joseph, and K. Singh, "Optical encryption by double random phase encoding in the fractional Fourier domain," *Opt. Lett.*, vol. 25, no. 12, pp. 887–889, 2000.

[7] B. M. Hennelly and J. T. Sheridan, "Image encryption based on the fractional Fourier transform," *Proc. SPIE*, vol. 5202, pp. 76–87, 2003.

[8] R. Tao, Y. Xin, and Y. Wang, "Double image encryption based on random phase encoding in the fractional Fourier domain," *Opt. Express*, vol. 15, no. 24, pp. 16067–16079, 2007.

[9] R. Tao, X. M. Li, and Y. Wang, "Generalization of the fractional Hilbert transform," *IEEE Signal Process. Lett.*, vol. 15, pp. 365–368, 2008.

[10] S. C. Pei and W. L. Hsue, "Random discrete fractional Fourier transform," *IEEE Signal Process. Lett.*, vol. 16, no. 12, pp. 1015–1018, Dec. 2009.

[11] L. J. Yan and J. S. Pan, "Generalized discrete fractional Hadamard transformation and its application on the image encryption," in *Proc. Int. Conf. Intelligent Information Hiding and Multimedia Signal Processing*, 2007, pp. 457–460.

[12] H. Al-Qaheri, A. Mustafi, and S. Banerjee, "Digital watermarking using ant colony optimization in fractional Fourier domain," *J. Inf. Hiding Multimedia Signal Process.*, vol. 1, no. 3, pp. 179–189, Jul. 2010.

[13] S. C. Pei and J. J. Ding, "Closed-form discrete fractional and affine Fourier transforms," *IEEE Trans. Signal Process.*, vol. 48, no. 5, pp. 1338–1353, May 2000.

[14] X. Y. Meng, R. Tao, and Y. Wang, "The fractional Fourier domain analysis of decimation and interpolation," *Science in China, Ser. F*, vol. 50, pp. 521–538, Jul. 2007.

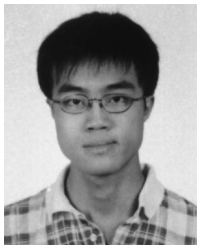
[15] X. Y. Meng, R. Tao, and Y. Wang, "Fractional Fourier domain analysis of cyclic multirate signal processing," *Science in China, Ser. E*, vol. 51, pp. 803–819, Jun. 2008.

[16] M. Bouchard, "Multichannel affine and fast affine projection algorithms for active noise control and acoustic equalization systems," *IEEE Trans. Speech Audio Process.*, vol. 11, no. 1, pp. 54–60, Jan. 2003.

Ran Tao (M'00–SM'04) was born in Nanling County, Anhui Province, China, in 1964. He received the B.S. degree in Hefei College of Electronic Engineering, Hefei, China, in 1985 and the M.S. and Ph.D. degrees from Harbin Institute of Technology, Harbin, China, in 1990 and 1993, respectively.

After completing postdoctoral studies in electronics and communications at the Beijing Institute of Technology (BIT), China, he became an Associate Professor in 1996 and a Professor in 1999. From March 2001 to April 2002, he was a visiting scholar at the University of Michigan, Ann Arbor. He is currently a chief Professor with the Electronic Engineering Department, BIT. His current research interests include fractional Fourier transform with applications, theory, and technology for radar and communication systems.

Dr. Tao is now the Vice-Chair of IEEE China Council. He was a recipient of the National Science Foundation of China for Distinguished Young Scholars in 2006. He also has been a Distinguished Professor of Cheung Kong Scholars Program since 2009. He received the Teaching and Research Award for Outstanding Young Teachers in Higher Education Institutions of MOE, China, in 2000, as well as the Chinese Armament Young Science and Technology Award in 2003. He received the Ministerial Science and Technology First-Grade Awards in 2006 and 2007, respectively. He is also the Vice President of Radar Society and Fellow of Chinese Institute of Electronics.



Xiang-Yi Meng (S'09) was born in Beijing, China, in 1983. He received the B.S. degree in information engineering from the Communication University of China, once called the Beijing Broadcasting Institute, Beijing, China, in 2005. He is currently working toward the Ph.D degree in information and communication engineering at the Beijing Institute of Technology.

His research interests include time-frequency analysis, multirate signal processing, wireless communication, image processing, and parameter estimation.

Mr. Meng is a recipient of the Graduate Research Fellowship Award from Microsoft Research Asia in 2008.

Yue Wang was born in Danyang City, Jiangsu Province, China, in 1932. He received the B.S. degree in radar engineering from Xidian University, Shaanxi, China, in 1956.

He was the President of the Beijing Institute of Technology (BIT), China, from 1993 to 1997. Presently, he is the President Emeritus of BIT. His research interests include information system theory and technology and multiagent theory.

Prof. Wang is a Fellow of the Chinese Academy of Sciences and also a Fellow of the Chinese Academy of Engineering.