The Multiple-Parameter Discrete Fractional FourierTransform

Soo-Chang Pei, *Fellow, IEEE*, and Wen-Liang Hsue

***Abstract*—The discrete fractional Fourier transform (DFRFT) is a generalization of the discrete Fourier transform (DFT) with one additional order parameter. In this letter, we extend the DFRFT to have N order parameters, where N is the number of the input data points. The proposed multiple-parameter discrete fractional Fourier transform (MPDFRFT) is shown to have all of the desired properties for fractional transforms. In fact, the MPDFRFT reduces to the DFRFT when all of its order parameters are the same. To show an application example of the MPDFRFT, we exploit its multiple-parameter feature and propose the double random phase encoding in the MPDFRFT domain for encrypting digital data. The proposed encoding scheme in the MPDFRFT domain significantly enhances data security.**

***Index Terms*—Decryption, discrete fractional Fourier transform (DFRFT), encryption, fractional Fourier transform (FRT).**

I. Introduction

The continuous fractional Fourier transform (FRT) is a generalization of the continuous Fourier transform and has been applied in optics, quantum mechanics, and signal processing areas [1]–[3]. To obtain the discrete version of the continuous FRT, the discrete fractional Fourier transform (DFRFT) was defined [4], [5]. In [4], Pei and Yeh defined the DFRFT based on the eigendecomposition of the DFT matrix. The main features of the eigendecomposition-based DFRFT defined by Pei and Yeh are as follows.

1) It is a generalization of the DFT with one additional order parameter and possesses all of the required properties of being a fractional transform.
2) Its transform outputs are similar to samples of the continuous FRT.

The continuous FRT was successfully used for data security applications. In [6], Refregier and Javidi proposed a double random phase encoding method to encrypt the images. In that encoding scheme, two random phase encodings in the input plane and the Fourier plane are used to encrypt the input image, and the encoded output image is shown to be stationary white. Unnikrishnan and Singh [7] replaced the conventional Fourier transform with the FRT for the conventional double random phase encoding method originally proposed by Refregier and Javidi. The resulting keys for decryption are the fractional order parameters of the FRT and the random phase codes used in the encryption process. Therefore, the continuous FRT can be used for the double random phase encoding method to enhance its data security.

Manuscript received October 4, 2005; revised December 12, 2005. This work was supported by the National Science Council, R. O. C., under Contract NSC93-2219-E-002-004 and Contract NSC93-2752-E-002-006-PAE. The associate editor coordinating the review of this manuscript and approving it for publication was Dr. Xiang-Gen Xia.

S.-C. Pei is with the Department of Electrical Engineering, National Taiwan University, Taipei 10617, Taiwan, R.O.C. (e-mail: pei@cc.ee.ntu.edu.tw).

W.-L. Hsue is with the Graduate Institute of Communication Engineering, National Taiwan University, Taipei 10617, Taiwan, R.O.C., and also with the Department of Electronic Engineering, Lan-Yang Institute of Technology, I-Lan 261, Taiwan, R.O.C. (e-mail: d92942015@ntu.edu.tw).

Digital Object Identifier 10.1109/LSP.2006.871721

II. Preliminaries

The ath-order continuous FRT of $x(t)$ is [2]

$$X_a(u) = \int_{-\infty}^{+\infty} x(t) K_a(u,t)\,dt \tag{1}$$

where the transform kernel $K_a(u,t)$ is

$$\begin{aligned} K_a(u,t) &= \sqrt{1 - j\cot\alpha} \cdot e^{j\pi\left(t^2\cot\alpha - 2tu\csc(\alpha) + u^2\cot\alpha\right)} \\ &= \sum_{n=0}^{\infty} \exp\left(-\frac{jna\pi}{2}\right) \cdot \Psi_n(t)\Psi_n(u) \end{aligned} \tag{2}$$

with $\alpha = a\pi/2$ and $\Psi_n(t)$ being the nth-order continuous Hermite–Gaussian function [2].

The $N \times N$ DFT matrix $\mathbf{F}$ is defined as

$$\mathbf{F}_{kn} = \frac{1}{\sqrt{N}} e^{-j\frac{2\pi}{N}kn}, \quad 0 \le k, n \le N-1. \tag{3}$$

The DFT matrix $\mathbf{F}$ has only four distinct eigenvalues: 1, -1, j, and $-j$ [8]. Let us define an $N \times N$ nearly tridiagonal matrix $\mathbf{S}$ whose nonzero entries are [9]

$$\begin{aligned} \mathbf{S}_{n,n} &= 2\cos\left(\frac{2\pi}{N} \cdot n\right), \quad 0 \le n \le (N-1) \\ \mathbf{S}_{n,n+1} &= \mathbf{S}_{n+1,n} = 1, \quad 0 \le n \le (N-2) \\ \mathbf{S}_{N-1,0} &= \mathbf{S}_{0,N-1} = 1. \end{aligned} \tag{4}$$

Since $\mathbf{S}$ commutes with $\mathbf{F}$, i.e., $\mathbf{SF} = \mathbf{FS}$, matrix $\mathbf{F}$ and $\mathbf{S}$ will have the same eigenvectors but different eigenvalues. Based on the eigendecomposition of $\mathbf{F}$, Pei and Yeh [4] defined the ath-order $N \times N$ DFRFT matrix as

$$\begin{aligned} \mathbf{F}^a &= \mathbf{V}\boldsymbol{\Lambda}^a\mathbf{V}^T \\ &= \begin{cases} \sum_{k=0}^{N-1} e^{-j\frac{\pi}{2}ka}\mathbf{v}_k\mathbf{v}_k^T, & \text{for } N \text{ odd} \\ \sum_{k=0}^{N-2} e^{-j\frac{\pi}{2}ka}\mathbf{v}_k\mathbf{v}_k^T + e^{-j\frac{\pi}{2}Na}\mathbf{v}_N\mathbf{v}_N^T, & \text{for } N \text{ even} \end{cases} \end{aligned} \tag{5}$$

where T denotes the matrix transpose, the matrix $\mathbf{V} = [\mathbf{v}_0|\mathbf{v}_1|\cdots|\mathbf{v}_{N-2}|\mathbf{v}_{N-1}]$ for odd N and $\mathbf{V} = [\mathbf{v}_0|\mathbf{v}_1|\cdots|\mathbf{v}_{N-2}|\mathbf{v}_N]$ for even N, $\mathbf{\Lambda}$ is a diagonal matrix with its diagonal entries corresponding to the eigenvalues for each column eigenvectors $\mathbf{v}_k$ in $\mathbf{V}$, and $\mathbf{v}_k$ is the normalized kth-order discrete Hermite–Gaussian-like eigenvector of $\mathbf{S}$.

III. Definition of the MPDFRFT and Its Properties

From the definition of the ath-order DFRFT matrix $\mathbf{F}^a$ given in (5), we can see that $\mathbf{F}^a$ degenerates to the DFT matrix $\mathbf{F}$ in (3) when $a = 1$ [4]. Therefore, the DFRFT is a generalization of the DFT. From (5), we can further generalize the DFRFT if we take different fractional powers for the eigenvalues $\lambda_k = \exp(-j\pi k/2)$ of the DFT matrix. This results in the definition of the N-point $N \times N$ MPDFRFT matrix

$$\mathbf{F}^{\overline{a}} = \begin{cases} \mathbf{V}\cdot diag\Big(\big(e^{-j\frac{\pi}{2}0}\big)^{a_0}, \big(e^{-j\frac{\pi}{2}1}\big)^{a_1}, \cdots \\ \quad \big(e^{-j\frac{\pi}{2}(N-1)}\big)^{a_{N-1}}\Big)\cdot \mathbf{V}^T, & \text{for } N \text{ odd} \\ \mathbf{V}\cdot diag\Big(\big(e^{-j\frac{\pi}{2}0}\big)^{a_0}, \big(e^{-j\frac{\pi}{2}1}\big)^{a_1}, \cdots \\ \quad \big(e^{-j\frac{\pi}{2}(N-2)}\big)^{a_{N-2}}, \big(e^{-j\frac{\pi}{2}N}\big)^{a_N}\Big)\cdot \mathbf{V}^T, & \text{for } N \text{ even} \end{cases} \tag{6}$$

where $diag(r_1, r_2, \cdots, r_N)$ represents the $N \times N$ diagonal matrix whose diagonal elements are $r_1, r_2, \cdots, r_N$. In (6), $\overline{a}$ is a $1 \times N$ parameter vector consisting of the N independent order parameters of the MPDFRFT

$$\overline{a} = \begin{cases} (a_0, a_1, \cdots, a_{N-1}), & \text{for } N \text{ odd} \\ (a_0, a_1, \cdots, a_{N-2}, a_N), & \text{for } N \text{ even.} \end{cases} \tag{7}$$

To simplify the presentations, let us define

$$\mathbf{\Lambda}^{\overline{a}} = \begin{cases} diag\left(\big(e^{-j\frac{\pi}{2}0}\big)^{a_0}, \big(e^{-j\frac{\pi}{2}1}\big)^{a_1}, \cdots \\ \quad \big(e^{-j\frac{\pi}{2}(N-1)}\big)^{a_{N-1}}\right), & \text{for } N \text{ odd} \\ diag\left(\big(e^{-j\frac{\pi}{2}0}\big)^{a_0}, \big(e^{-j\frac{\pi}{2}1}\big)^{a_1}, \cdots \\ \quad \big(e^{-j\frac{\pi}{2}(N-2)}\big)^{a_{N-2}}, \big(e^{-j\frac{\pi}{2}N}\big)^{a_N}\right), & \text{for } N \text{ even} \end{cases} \tag{8}$$

where the vector $\overline{a}$ is given in (7), and $\mathbf{\Lambda}$ is the $N \times N$ diagonal matrix of the DFT eigenvalues

$$\mathbf{\Lambda} = \begin{cases} diag\left(e^{-j\frac{\pi}{2}0}, e^{-j\frac{\pi}{2}1}, \cdots, e^{-j\frac{\pi}{2}(N-1)}\right), & \text{for } N \text{ odd} \\ diag\left(e^{-j\frac{\pi}{2}0}, e^{-j\frac{\pi}{2}1}, \cdots \\ \quad e^{-j\frac{\pi}{2}(N-2)}, e^{-j\frac{\pi}{2}N}\right), & \text{for } N \text{ even.} \end{cases} \tag{9}$$

Then, (6) can be rewritten as

$$\mathbf{F}^{\overline{a}} = \mathbf{V}\mathbf{\Lambda}^{\overline{a}}\mathbf{V}^T. \tag{10}$$

The MPDFRFT $\mathbf{X}_{\overline{a}}$ of the $N \times 1$ data vector $\mathbf{x}$ with the parameter vector $\overline{a}$ can be computed by

$$\mathbf{X}_{\overline{a}} = \mathbf{F}^{\overline{a}}\mathbf{x}. \tag{11}$$

The main features of the definition of MPDFRFT in (6) are as follows.

1) If $\overline{a} = (a, a, \cdots, a)$, the MPDFRFT in (6) degenerates to the DFRFT definition in (5). That is, the DFRFT is a special case of the MPDFRFT.
2) The N-point MPDFRFT can have up to N independent and possibly different order parameters, whereas the DFRFT has only one order parameter.
3) The computation complexity for the MPDFRFT is $O(N^2)$, which is the same as that for the DFRFT. This can be seen from definitions (5) and (6).

We show below that the MPDFRFT possesses all of the following desired properties for fractional transforms.

1) Unitarity: From (10), we have

$$\begin{aligned}(\mathbf{F}^{\overline{a}})^H(\mathbf{F}^{\overline{a}}) &= (\mathbf{V}\mathbf{\Lambda}^{\overline{a}}\mathbf{V}^T)^H(\mathbf{V}\mathbf{\Lambda}^{\overline{a}}\mathbf{V}^T) \\ &= (\mathbf{V}\mathbf{\Lambda}^{-\overline{a}}\mathbf{V}^T)(\mathbf{V}\mathbf{\Lambda}^{\overline{a}}\mathbf{V}^T) = \mathbf{V}\mathbf{V}^T = \mathbf{I}\end{aligned} \tag{12}$$

where H denotes the conjugate transpose operation. Similarly, we have $(\mathbf{F}^{\overline{a}})(\mathbf{F}^{\overline{a}})^H = \mathbf{I}$.
2) Identity matrix: If $\overline{a} = \overline{0} = (0, 0, \cdots, 0)$, $\mathbf{F}^{\overline{a}} = \mathbf{V}\mathbf{\Lambda}^{\overline{0}}\mathbf{V}^T = \mathbf{V}\mathbf{V}^T = \mathbf{I}$ reduces to an identity operator.
3) Fourier transform: If the parameter vector $\overline{a} = \overline{1} = (1, 1, \cdots, 1)$, $\mathbf{F}^{\overline{a}} = \mathbf{V}\mathbf{\Lambda}^{\overline{1}}\mathbf{V}^T = \mathbf{V}\mathbf{\Lambda}\mathbf{V}^T = \mathbf{F}$.
4) Index additivity: If $\overline{a}_1$ and $\overline{a}_2$ are two parameter vectors of the same size of the MPDFRFT, then

$$\mathbf{F}^{\overline{a}_1}\cdot\mathbf{F}^{\overline{a}_2} = (\mathbf{V}\mathbf{\Lambda}^{\overline{a}_1}\mathbf{V}^T)(\mathbf{V}\mathbf{\Lambda}^{\overline{a}_2}\mathbf{V}^T) = \mathbf{V}\mathbf{\Lambda}^{\overline{a}_1+\overline{a}_2}\mathbf{V}^T = \mathbf{F}^{\overline{a}_1+\overline{a}_2}. \tag{13}$$

5) Index commutativity:

$$\mathbf{F}^{\overline{a}_1}\cdot\mathbf{F}^{\overline{a}_2} = \mathbf{V}\mathbf{\Lambda}^{\overline{a}_1+\overline{a}_2}\mathbf{V}^T = \mathbf{V}\mathbf{\Lambda}^{\overline{a}_2+\overline{a}_1}\mathbf{V}^T = \mathbf{F}^{\overline{a}_2}\cdot\mathbf{F}^{\overline{a}_1}. \tag{14}$$

6) Inverse transform: The inverse transform of the MPDFRFT of parameter vector $\overline{a}$ can be simply given by $(\mathbf{F}^{\overline{a}})^{-1} = \mathbf{F}^{-\overline{a}}$, which can be obtained from properties 2) and 4).
7) Parameter periodicity: The MPDFRFT $\mathbf{F}^{\overline{a}}$ is periodic in parameter a_k with period $4/k$ if k is nonzero, and $\mathbf{F}^{\overline{a}}$ is the same for different a_0. This can be seen from (6), and the facts that

$$e^{-j\frac{\pi}{2}k\cdot\left(a_k+\frac{4}{k}\right)} = e^{-j\frac{\pi}{2}k\cdot a_k}, \text{ if } k\neq 0, \text{ and } \left(e^{-j\frac{\pi}{2}0}\right)^{a_0} = 1, \ \forall a_0. \tag{15}$$

Then $\mathbf{F}^{\overline{a}}$ is periodic in a_k with period 4 for all k.
8) From (6), we have

$$\mathbf{F}^{\overline{a}}\mathbf{v}_k = e^{-j\frac{\pi}{2}k\cdot a_k}\mathbf{v}_k. \tag{16}$$

Thus, the kth-order discrete Hermite–Gaussian-like DFT eigenvector $\mathbf{v}_k$ is also an eigenvector of $\mathbf{F}^{\overline{a}}$, and its corresponding eigenvalue is $\exp(-j\pi k a_k/2)$.

We want to point out that the idea of taking different fractional powers for different eigenvalues to achieve the multiple-parameter property of an eigendecomposition-based fractional transform can also be applied to the continuous FRT in (1) as well as the discrete fractional cosine and sine transforms in [10]. For example, the transform kernel of the multiple-parameter continuous FRT with infinite order parameters $a_0, a_1, \cdots$ is

$$K(u,t) = \sum_{n=0}^{\infty}\exp\left(-\frac{jna_n\pi}{2}\right)\cdot\Psi_n(t)\Psi_n(u). \tag{17}$$

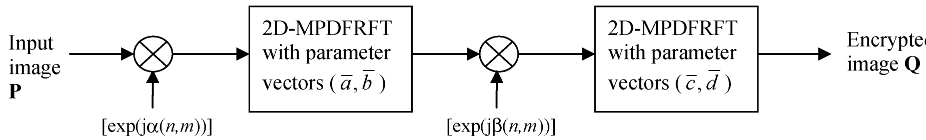

Fig. 1. Encryption process of the double random phase encoding in the MPDFRFT domain.

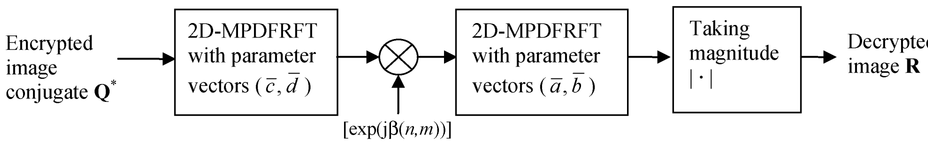

Fig. 2. Decryption process of the double random phase encoding in the MPDFRFT domain.

IV. Image Encryption Application of the MPDFRFT

By replacing FRT with MPDFRFT in the double random fractional Fourier domain encoding introduced by Unnikrishnan and Singh [7], we propose the double random phase encoding in the MPDFRFT domain to encrypt digital images, of which the encryption and decryption processes are depicted in Figs. 1 and 2. This encryption method significantly improves data security because the order parameters of the 2D-MPDFRFT can be exploited as extra keys for decryption.

The 1D-MPDFRFT in (11) can be extended to the two-dimensional case. For an $N \times M$ image $\mathbf{P}$, the 2D-MPDFRFT of $\mathbf{P}$ with parameter vectors $(\overline{a}, \overline{b})$ is given by

$$\mathbf{P}_{(\overline{a},\overline{b})} = \mathbf{F}^{\overline{a}} \cdot \mathbf{P} \cdot \mathbf{F}^{\overline{b}} \tag{18}$$

where $\mathbf{F}^{\overline{a}}$

and $\mathbf{F}^{\overline{b}}$ are the N-point and M-point MPDFRFT matrices, respectively, and $\overline{a}$ and $\overline{b}$ are the parameter vectors of sizes $1 \times N$ and $1 \times M$, respectively.

Let $[\exp(j\alpha(n,m))]$ and $[\exp(j\beta(n,m))]$ denote the two $N \times M$ random phase matrices in Fig. 1, where $\alpha(n,m)$ and $\beta(n,m)$ as well as $1 \leqq n \leqq N$ and $1 \leqq m \leqq M$ are both white and uniformly distributed in $[0, 2\pi]$. $\alpha(n,m)$ and $\beta(n,m)$ are independent of each other. From Fig. 1, the relationship between the encrypted output image $\mathbf{Q}$ and the input image $\mathbf{P}$ in the encryption process is

$$\mathbf{Q} = \mathbf{F}^{\overline{c}} \left\{ \left(\mathbf{F}^{\overline{a}} \left(\mathbf{P} \otimes \left[e^{j\alpha(n,m)} \right] \right) \mathbf{F}^{\overline{b}} \right) \otimes \left[e^{j\beta(n,m)} \right] \right\} \mathbf{F}^{\overline{d}} \tag{19}$$

where $\mathbf{C} = \mathbf{A} \otimes \mathbf{B}$ denotes the element-by-element multiplication operation of matrices $\mathbf{A}$ and $\mathbf{B}$, and the result is a matrix $\mathbf{C}$ whose (n,m)th element $\mathbf{C}_{n,m}$ is $C_{n,m} = \mathbf{A}_{n,m}\mathbf{B}_{n,m}$. From (10), $(\mathbf{F}^{\overline{a}})^* = \mathbf{F}^{-\overline{a}}$. The complex conjugate of the encrypted image in (19) is

$$\mathbf{Q}^* = \mathbf{F}^{-\overline{c}} \left(\left(\mathbf{F}^{-\overline{a}} \left(\mathbf{P} \otimes \left[e^{-j\alpha(n,m)} \right] \right) \mathbf{F}^{-\overline{b}} \right) \otimes \left[e^{-j\beta(n,m)} \right] \right) \mathbf{F}^{-\overline{d}} \tag{20}$$

where the input image for encryption $\mathbf{P}$ is assumed to be real and nonnegative. Thus, the decrypted image $\mathbf{R}$ in Fig. 2 is

$$\begin{aligned} \mathbf{R} &= \left| \mathbf{F}^{\overline{a}} \left\{ \left(\mathbf{F}^{\overline{c}} \mathbf{Q}^* \mathbf{F}^{\overline{d}} \right) \otimes \left[e^{j\beta(n,m)} \right] \right\} \mathbf{F}^{\overline{b}} \right| \\ &= \left| \mathbf{P} \otimes \left[e^{-j\alpha(n,m)} \right] \right| = \mathbf{P} \end{aligned} \tag{21}$$

in which $\mathbf{P}$ is the desired decryption output. In (21), the (n,m)th element of the magnitude operation $|\mathrm{A}|$ of matrix $\mathbf{A}$ is defined as $(|\mathbf{A}|)_{n,m} = |\mathbf{A}_{n,m}|$.

From the above discussions, the parameter vectors and the random phase codes constitute the keys for decryption of the double random phase encoding in the MPDFRFT domain. If we replace 2D-MPDFRFTs with 2D-DFRFTs in Figs. 1 and 2, the double random phase encoding in the MPDFRFT domain will degenerate to that in the DFRFT domain. The double random phase encoding in the DFRFT domain is the digital implementation of the double random fractional Fourier domain encoding in [7].

V. Computer Experiments

In all of the following computer experiments, we use the same random phase matrices for encryptions and decryptions. Let $\overline{a}'$, $\overline{b}'$, $\overline{c}'$, and $\overline{d}'$ denote the parameter vectors employed in the decryption process. Fig. 3(a) is the 256 $\times$ 256 original image to be encrypted. Fig. 3(b) shows the magnitude image of its encryption output using the double random phase encoding in the MPDFRFT domain, where the elements of the 1 $\times$ 256 encryption parameter vectors $\overline{a}$, $\overline{b}$, $\overline{c}$, and $\overline{d}$ are independent and randomly chosen from the interval [0,2]. Then, we use the correct parameter vectors for decryption, and the decrypted output is shown in Fig. 3(c), which is the same as the original image. To give a decryption example of the previous encrypted image with the wrong parameter vectors, we use

$$\overline{a}' = \overline{a}, \quad \overline{b}' = \overline{b}, \quad \overline{c}' = \overline{c} + \overline{\delta}_1, \quad \text{and} \quad \overline{d}' = \overline{d} + \overline{\delta}_2. \tag{22}$$

Error vectors $\overline{\delta}_1$ and $\overline{\delta}_2$ are independent, and the elements of both $\overline{\delta}_1$ and $\overline{\delta}_2$ are independent and uniformly distributed over the two-element set $\{-0.006, 0.006\}$. That is, elements of both

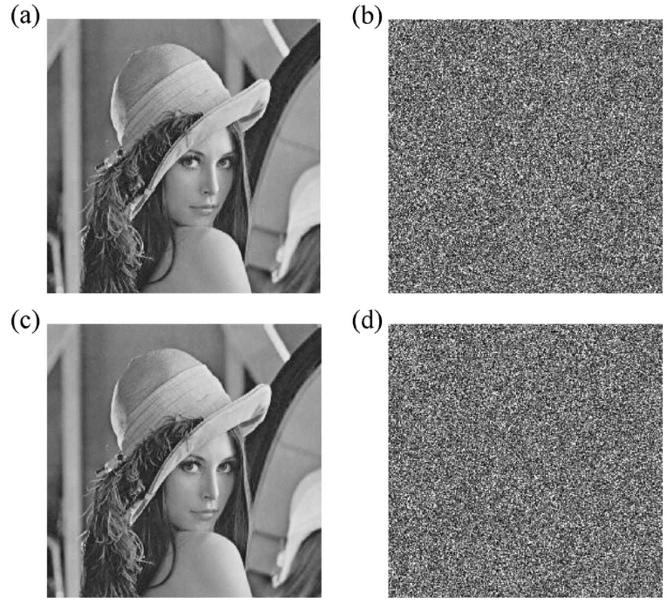

Fig. 3. The double random phase encoding in the MPDFRFT domain. (a) Original image. (b) Encrypted image. (c) Decrypted image with the correct parameter vectors. (d) Decrypted image with the element errors of two decryption parameter vectors uniformly distributed over the set $\{-0.006, 0.006\}$.

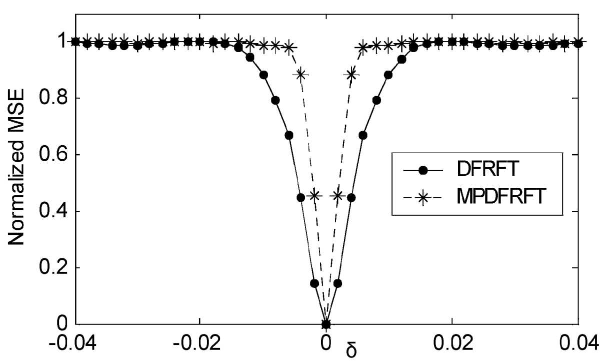

Fig. 4. Normalized MSEs of decrypted images of the double random phase encodings in the MPDFRFT domain and the DFRFT domain.

$\overline{\delta}_1$ and $\overline{\delta}_2$ take values either -0.006 or 0.006 with equal probability. Fig. 3(d) is the decrypted image, which shows that the original image is successfully protected.

Next, we perform another computer experiment to illustrate the effects of decryption parameter vector errors on the double random phase encoding in the MPDFRFT domain. Again, the relations of the parameter vectors used for decryption and encryption are given by (22). Error vectors $\overline{\delta}_1$ and $\overline{\delta}_2$ are independent, and the elements of both $\overline{\delta}_1$ and $\overline{\delta}_2$ are now independent and uniformly distributed over the set $\{-\delta, \delta\}$. Fig. 4 plots the normalized mean squared errors (MSEs) of the resulting decrypted images for various values of δ, where the maximum MSE is normalized to be 1. For comparison, Fig. 4 also plots the normalized MSEs of the decrypted images for the double random phase encoding in the DFRFT domain, where the encryption and decryption order parameters are (0.75,0.9,1.25,1.1) and $(0.75, 0.9, 1.25 + \delta, 1.1 + \delta)$, respectively. In Fig. 4, all of the normalized MSEs are the averaged results of ten realizations. We also perform many other experiments using different images and different keys. For example, we also perform experiments to compute the MSEs of the decrypted images with errors in the decryption parameter vectors $\overline{a}'$ and $\overline{b}'$. Experiment results all show that the double random phase encoding in the MPDFRFT domain is much more sensitive to the decryption parameter error than that in the DFRFT domain.

Finally, assume that the errors for all elements of decryption parameter vectors $\overline{c}'$ and $\overline{d}'$ are uniformly distributed. From computer experiment, in order to have a successful brute-force cracking, all of these parameter errors should be very small and within -0.012 to 0.012, even though both of the other two encryption parameter vectors $\overline{a}$ and $\overline{b}$ and the random phase keys are known. For the kth element of both $\overline{c}'$ and $\overline{d}'$, each of its probability is $\min(0.024/(4/k), 1)$ from the parameter periodicity property of the MPDFRFT. Thus, the probability of a successful cracking is smaller than $p = [1/(4/0.024)]^2[2/(4/0.024)]^2, \ldots, [166/(4/0.024)]^2$. Therefore, it takes $3.1/p$ s to have a successful brute-force cracking, where 3.1 s is the time required for a PC (Pentium 4, 2.4-GHz CPU) to decrypt an image. This is equivalent to 5.46×10^{134} years!

VI. Conclusion

In this letter, a new MPDFRFT is defined from the eigen-decomposition-based DFRFT by taking different fractional powers for different eigenvalues. The MPDFRFT is much more flexible than the DFRFT because it has N order parameters, where N is the number of input data points. The MPDFRFT is shown to have all of the desired properties for fractional transforms. To give an application example, we propose the double random phase encoding in the MPDFRFT domain to encrypt digital images. This new encryption method significantly enhances data security, because the order parameters of the MPDFRFT can be exploited as extra keys for decryption.

References

[1] L. B. Almeida, "The fractional Fourier transform and time-frequency representations," *IEEE Trans. Signal Process.*, vol. 42, no. 12, pp. 3084–3091, Nov. 1994.

[2] H. M. Ozaktas, Z. Zalevsky, and M. A. Kutay, *The Fractional Fourier Transform with Applications in Optics and Signal Processing*. New York: Wiley, 2000.

[3] V. Namias, "The fractional order Fourier transform and its application to quantum mechanics," *J. Inst. Math. Appl.*, vol. 25, pp. 241–265, 1980.

[4] S. C. Pei and M. H. Yeh, "Improved discrete fractional Fourier transform," *Opt. Lett.*, vol. 22, pp. 1047–1049, 1997.

[5] C. Candan, M. A. Kutay, and H. M. Ozaktas, "The discrete fractional Fourier transform," *IEEE Trans. Signal Process.*, vol. 48, no. 5, pp. 1329–1337, May 2000.

[6] P. Refregier and B. Javidi, "Optical image encryption based on input plane and Fourier plane random encoding," *Opt. Lett.*, vol. 20, pp. 767–769, 1995.

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

[8] J. H. McClellan and T. W. Parks, "Eigenvalue and eigenvector decomposition of the discrete Fourier transform," *IEEE Trans. Audio. Electroacoust.*, vol. AU-20, no. 1, pp. 66–74, Mar. 1972.

[9] B. W. Dickinson and K. Steiglitz, "Eigenvectors and functions of the discrete Fourier transform," *IEEE Trans. Acoust., Speech, Signal Process.*, vol. ASSP-30, no. 1, pp. 25–31, Jan. 1982.

[10] S. C. Pei and M. H. Yeh, "The discrete fractional cosine and sine transforms," *IEEE Trans. Signal Process.*, vol. 49, no. 6, pp. 1198–1207, Jun. 2001.