The Multiple-Parameter Discrete Fractional Fourier Transform and Its Application

Wen-Liang Hsue and Soo-Chang Pei

Department of Electrical Engineering, National Taiwan University, Taipei, Taiwan, R.O.C.

Email address: pei@cc.ee.ntu.edu.tw

ABSTRACT

The discrete fractional Fourier transform (DFRFT) is a generalization of the discrete Fourier transform (DFT) with one additional order parameter. In this paper, 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.

1. 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: 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.

In this paper, we first briefly review the continuous FRT and the DFRFT. Then we define the new MPDFRFT from the eigendecomposition-based DFRFT. Properties of the proposed MPDFRFT are also described. To give an application example, we propose the double random phase encoding in the MPDFRFT domain to enhance security of digital images. Related computer experiments are also included and show its advantages.

2. PRELIMINARIES

The a^{th} -order continuous FRT of x(t) is [2]

$$X_{a}(u) = \int_{-\infty}^{+\infty} x(t) K_{a}(t, u) dt, \qquad (1)$$

where the transform kernel $K_a(t, u)$ can be expressed as

$$K_{a}(t,u) = \sqrt{1 - j \cot \phi \cdot e^{j\pi(t^{-} \cot \phi - 2tu \csc(\phi) + u^{-} \cot \phi)}}$$
$$= \sum_{n=0}^{\infty} \exp(-jna\pi/2) \cdot \Psi_{n}(t)\Psi_{n}(u),$$
(2)

with $\phi = a\pi/2$ and $\Psi_n(t)$ being the n^{th} -order continuous Hermite-Gaussian function [2].

The $N \times N$ DFT matrix **F** is defined as

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

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

$$S_{n,n} = 2\cos(\frac{2\pi}{N} \cdot n), \quad 0 \le n \le (N-1)$$

$$S_{n,n+1} = S_{n+1,n} = 1, \quad 0 \le n \le (N-2)$$

$$S_{N-1,0} = S_{0,N-1} = 1.$$
(4)

Since **S** commutes with **F**, that is, **SF=FS**, matrix **F** and **S** will have the same eigenvectors but different eigenvalues. Therefore, the Hermite-Gaussian like eigenvectors of **F** can be computed from those of **S**. Based on the eigendecomposition of **F**, Pei and Yeh [4] defined the a^{th} -order $N \times N$ DFRFT matrix as

$$\mathbf{F}^{a} = \mathbf{V} \mathbf{\Lambda}^{a} \mathbf{V}^{T} = \begin{cases} \sum_{k=0}^{N-1} e^{-j\frac{\pi}{2}ka} \mathbf{v}_{k} \mathbf{v}_{k}^{T}, \text{ for } N \text{ odd} \\ \sum_{k=0}^{N-2} e^{-j\frac{\pi}{2}ka} \mathbf{v}_{k} \mathbf{v}_{k}^{T} + e^{-j\frac{\pi}{2}Na} \mathbf{v}_{N} \mathbf{v}_{N}^{T}, \\ \text{ for } N \text{ even,} \end{cases}$$
(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 k^{th} -order discrete Hermite-Gaussian like eigenvector of \mathbf{S} with the *k* zero-crossings.

3. DEFINITION OF THE MPDFRFT AND ITS PROPERTIES

From the definition of the a^{th} -order DFRFT matrix \mathbf{F}^{a} given in (5), we can see that \mathbf{F}^{a} degenerates to the DFT matrix **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:

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

. . .

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

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

To simplify the presentations, let us define

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

where the vector \overline{a} is given in (7) and Λ is the N×N diagonal matrix of the DFT eigenvalues:

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

Then, (6) can be rewritten as

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

The N-point MPDFRFT $\mathbf{X}_{\overline{a}}$ of the N×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: 1. If $\overline{a} = (a, a, ..., a)$, 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 the same as that for the DFRFT, which can be seen from definitions (5) and (6).

In the following discussions, we show that the MPDFRFT possesses all of the desired properties for fractional transforms:

1. Unitarity: From (10), we have

$$(\mathbf{F}^{\bar{a}})^{H} (\mathbf{F}^{\bar{a}}) = (\mathbf{V} \boldsymbol{\Lambda}^{\bar{a}} \mathbf{V}^{T})^{H} (\mathbf{V} \boldsymbol{\Lambda}^{\bar{a}} \mathbf{V}^{T})$$
$$= (\mathbf{V} \boldsymbol{\Lambda}^{-\bar{a}} \mathbf{V}^{T}) (\mathbf{V} \boldsymbol{\Lambda}^{\bar{a}} \mathbf{V}^{T}) = \mathbf{V} \mathbf{V}^{T} = \mathbf{I},$$
(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 the parameter vector $\overline{a} = \overline{0} = (0, 0, ..., 0)$, $\mathbf{F}^{\overline{a}} = \mathbf{V} \mathbf{\Lambda}^{\overline{0}} \mathbf{V}^{T} = \mathbf{V} \mathbf{V}^{T} = \mathbf{I}$ reduces to an identity operator.

3. Fourier transform: If the parameter vector $\overline{a} = (1, 1, ..., 1)$, $\mathbf{F}^{\overline{a}} = \mathbf{V} \mathbf{\Lambda}^{\overline{1}} \mathbf{V}^{T} = \mathbf{V} \mathbf{\Lambda} \mathbf{V}^{T} = \mathbf{F}$ reduces to the DFT operator, where $\overline{1}$ denotes the all 1 vector.

4. Index additivity:

$$\mathbf{F}^{\overline{a}_1} \cdot \mathbf{F}^{\overline{a}_2} = (\mathbf{V} \boldsymbol{\Lambda}^{\overline{a}_1} \mathbf{V}^T) (\mathbf{V} \boldsymbol{\Lambda}^{\overline{a}_2} \mathbf{V}^T)$$

= $\mathbf{V} \boldsymbol{\Lambda}^{\overline{a}_1 + \overline{a}_2} \mathbf{V}^T = \mathbf{F}^{\overline{a}_1 + \overline{a}_2},$ (13)

where \overline{a}_1 and \overline{a}_2 are two parameter vectors of the same size of the MPDFRFT.

5. Index commutativity:

$$\mathbf{F}^{\overline{a}_1} \cdot \mathbf{F}^{\overline{a}_2} = \mathbf{V} \mathbf{\Lambda}^{\overline{a}_1 + \overline{a}_2} \mathbf{V}^T = \mathbf{V} \mathbf{\Lambda}^{\overline{a}_2 + \overline{a}_1} \mathbf{V}^T = \mathbf{F}^{\overline{a}_2} \cdot \mathbf{F}^{\overline{a}_1} .$$
(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: MPDFRFT $\mathbf{F}^{\overline{a}}$ is periodic in parameter a_k with period 2 when k is even, and is periodic in a_k with period 4 when k is odd. This can be seen from (6), and the facts that

$$e^{-j\frac{\pi}{2}k \cdot (a_k + 2)} = e^{-j\frac{\pi}{2}k \cdot a_k}, \text{ if } k \text{ is even}, \text{ and} \\ e^{-j\frac{\pi}{2}k \cdot (a_k + 4)} = e^{-j\frac{\pi}{2}k \cdot a_k}, \text{ if } k \text{ is odd.}$$
(15)

Then $\mathbf{F}^{\overline{a}}$ is periodic in parameter a_k with period 4 whenever k is even or odd.

We want to point out that the idea of taking different fractional powers for different eigenvalues to achieve the multipleparameter property of a fractional transform can also be applied to the continuous FRT in (1), and 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, \ldots is:

$$K(t,u) = \sum_{n=0}^{\infty} \exp(-jna_n\pi/2) \cdot \Psi_n(t)\Psi_n(u).$$
(16)



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.

4. IMAGE ENCRYPTION APPLICATION OF THE MPDFRFT

In this section, we apply the 2D-MPDFRFT to encrypt digital images for enhancing data security. The proposed encryption method is termed as the double random phase encoding in the MPDFRFT domain. This encryption method significantly improves data security because the order parameters of the MPDFRFT can be exploited as extra keys for decryption.

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.

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

$$\mathbf{P}_{(\bar{a},\bar{b})} = \mathbf{F}^{\bar{a}} \cdot \mathbf{P} \cdot \mathbf{F}^{\bar{b}}$$
(17)

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. In (17), we can use different MPDFRFT parameter vectors \overline{a} and \overline{b} for transforming column vectors and row vectors of **P** to increase the key numbers for decryption.

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 $\beta(n,m)$, $1 \le n \le N$ and $1 \le m \le M$, are both white and uniformly distributed in $[0,2\pi].\alpha(n,m)$ and $\beta(n,m)$ are independent each other. From Fig. 1, the relationship between the encrypted output image **Q** and the input image **P** in the encryption process is given by

$$\mathbf{Q} = \mathbf{F}^{\bar{c}} \{ (\mathbf{F}^{\bar{a}} (\mathbf{P} \otimes [e^{j\alpha(n,m)}]) \mathbf{F}^{\bar{b}}) \otimes [e^{j\beta(n,m)}] \} \mathbf{F}^{\bar{d}}, \qquad (18)$$

where $C=A \otimes B$ denotes the element-by-element multiplication operation of matrices A and B, and the result is a matrix C whose $(n,m)^{th}$ element $C_{n,m}$ is $C_{n,m}=A_{n,m}B_{n,m}$. From (10), $(\mathbf{F}^{\overline{a}})^* = \mathbf{F}^{-\overline{a}}$. The complex conjugate of the encrypted image in (18) can be written as $\mathbf{Q}^* = \mathbf{F}^{-\bar{c}} \left((\mathbf{F}^{-\bar{a}} \left(\mathbf{P} \otimes [e^{-j\alpha(n,m)}] \right) \mathbf{F}^{-\bar{b}} \right) \otimes [e^{-j\beta(n,m)}] \right) \mathbf{F}^{-\bar{d}}, (19)$ where the input image for encryption **P** is assumed to be real and nonnegative. Thus the decrypted image **R** in Fig. 2 is $\mathbf{R} = \left| \mathbf{F}^{\bar{a}} \left\{ (\mathbf{F}^{\bar{c}} \mathbf{Q}^* \mathbf{F}^{\bar{d}}) \otimes [e^{j\beta(n,m)}] \right\} \mathbf{F}^{\bar{b}} \right| = \left| \mathbf{P} \otimes [e^{-j\alpha(n,m)}] \right| = \mathbf{P}, (20)$ in which **P** is the desired decryption output. In (20), the (n,m)th

element of the magnitude operation $|\mathbf{A}|$ 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 Fig. 1 and Fig. 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].

5. 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 256×256 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 1×256 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

$$\overline{a}' = \overline{a}, \ \overline{b}' = \overline{b}, \ \overline{c}' = \overline{c} + \overline{\delta}_1, \ \text{and} \ \overline{d}' = \overline{d} + \overline{\delta}_2.$$
 (21)

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 $\overline{\delta}_1$ 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.



Fig. 3. The double random phase encoding in the MPDFRFT domain. (a) Original image to be encrypted. (b) The 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. MSEs of decrypted images of the double random phase encodings in the MPDFRFT domain and the DFRFT domain.

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 (21). 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 $\{-\delta, \delta\}$. Thus all of the absolute values of elements of error vectors $\overline{\delta}_1$ and $\overline{\delta}_2$ are $|\delta|$. Fig. 4 plots the mean squared errors (MSEs) of the resulting decrypted images for various values of δ . For comparison, Fig. 4 also plots the 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 MSEs are the averaged results of 10 realizations. From Fig. 4, we can see 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.

6. CONCLUSION

In this paper, a new MPDFRFT is defined from the eigendecomposition-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. Moreover, from the computer experiments, we show that the decrypted output of the double random phase encoding in the MPDFRFT domain is much more sensitive to the decryption parameter error than that in the DFRFT domain.

7. REFERENCES

- L. B. Almeida, "The fractional Fourier transform and timefrequency representations," *IEEE Trans. Signal Processing*, vol. 42, pp. 3084-3091, Nov. 1994.
- [2] H. M. Ozaktas, Z. Zalevsky, and M. A. Kutay, *The Frac*tional Fourier Transform with Applications in Optics and Signal Processing. New York, John Wiley & Sons, 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 Processing*, vol. 48, 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, pp. 66-74, 1972.
- [9] B. W. Dickinson and K. Steiglitz, "Eigenvectors and functions of the discrete Fourier transform," *IEEE Trans. Acoust., Speech, Signal Processing*, vol. ASSP-30, pp. 25-31, Jan. 1982.
- [10] S. C. Pei and M. H. Yeh, "The discrete fractional cosine and sine transforms," *IEEE Trans. Signal Processing*, vol. 49, no. 6, pp. 1198-1207, Jun. 2001.