Hindawi
Mathematical Problems in Engineering
Volume 2019, Article ID 4789194, 10 pages
https://doi.org/10.1155/2019/4789194

Review Article

The Weighted Fractional Fourier Transform and Its Application in Image Encryption

Tieyu Zhao [1] **and Qiwen Ran** [2]

[1] *Information and Computational Science, Northeastern University at Qinhuangdao, Qinhuangdao 064000, China*
[2] *State Key Laboratory of Tunable Laser Technology Research, Institute of Optic-Electronics, Harbin Institute of Technology, Harbin 150001, China*

Correspondence should be addressed to Tieyu Zhao; zty03y3213@163.com

Received 15 February 2019; Revised 11 April 2019; Accepted 28 April 2019; Published 12 May 2019

Academic Editor: Nazrul Islam

With the rapid development of information, the requirements for the security and reliability of cryptosystems have become increasingly difficult to meet, which promotes the development of the theory of a class of fractional Fourier transforms. In this paper, we present a review of the development and applications of the weighted fractional Fourier transform (WFRFT) in image encryption. Relationships between the algorithms are established using the generalized permutation matrix group in theoretical analysis. In addition, the advantages and potential weaknesses of each algorithm in image encryption are analyzed and discussed. It is expected that this review will provide a clear picture of the current developments of the WFRFT in image encryption and may shed some light on future developments.

1. Introduction

In 1995, Refregier and Javidi proposed an optical image encryption scheme based on the 4f system [1], which attracted researchers' attention. Later, the scheme was extended to the fractional Fourier transform (FRFT) domain by Unnikrishnan et al. [2]. The transform order was also used as the encryption key in addition to the random phase matrix, which improved the security of the system. The FRFT was a generalized Fourier transform (FT) and had more flexibility and research value. In 1995, Shih first proposed the WFRFT, a new version of the FRFT [3]. Zhu et al. proposed the optical image encryption method based on multifractional Fourier transforms (MFRFT) [4], a generalized WFRFT, which allowed the cycle to also be used as a key. Before long, Ran et al. generalized the definition of the WFRFT by extending it [3–5], which was called the high-order generalized permutational fractional Fourier transform (HGPFRFT) [6]. They then proposed the general MFRFT method based on the generalized permutation matrix group [7]. In the years that followed, new theories based on the FRFT were presented for image encryption. Pei et al. proposed an image encryption method based on the multiple-parameter discrete fractional Fourier transform (MPDFRFT) [8], and this new encryption method significantly enhanced data security since it exploited the order parameters of the MPDFRFT as extra keys for decryption. Liu et al. proposed a random fractional Fourier transform (RFRFT) by using random phase modulations, and the optical implementation of the RFRFT was based on the Lohmann-type FRFT configuration [9]. However, these two definitions [8, 9] are not variants of the WFRFT. Prior to 2008, Tao et al. proposed an image encryption scheme based on the multiparameter fractional Fourier transform (MPFRFT) [10], which greatly improved the security of the system without increasing hardware costs. Then, Ran et al. analyzed the security and the reliability of the encryption schemes based on the MPFRFT, and the modified multiparameter fractional Fourier transform (m-MPFRFT) was proposed [11]. Hence, image encryption schemes were proposed based on the m-MPFRFT, which greatly enriched image encryption research [12–21]. Recently, Ran and Zhao et al. proposed the vector power multiparameter fractional Fourier transform (VPMPFRFT) [22, 23], which can widen the key space and

has greater security; this method widened the research and application of the generalized WFRFT.

In conclusion, the WFRFT has been widely applied in image encryption, and researchers have continuously proposed new transformation theories to improve security. This paper reviews the existing WFRFT methods and analyzes the correlation and diversity among the algorithms.

2. Theoretical Analysis

There are multiple different variants of the FRFT, and we analyze a class of the WFRFT. Its earliest definition was proposed by Shih [3], after which various types of WFRFTs emerged. In the theoretical analysis, we will establish the correlation between the various WFRFTs using the generalized permutation matrix.

2.1. Shih's Weighted Fractional Fourier Transform. In 1987, McBride and Kerr perfected and generalized the concept of Namias [24] and defined the integral form of the FRFT [25]. In the space $L^2(\mathrm{R})$, the FRFT of any signal $f(t)$ is

$$\left(F^a f\right)(t) = \int_{-\infty}^{+\infty} f(t)\, K_\alpha(u,t)\, dt. \tag{1}$$

The integral kernel is

$$K_\alpha(u,t) = \begin{cases} \sqrt{\dfrac{(1 - i\cot t\phi)}{2\pi}} \cdot e^{i(u^2 \cot\phi - 2ut\csc\phi + t^2\cot\phi)} & \phi \neq n\pi \\ \delta\left(u - (-1)^n t\right) & \phi = n\pi. \end{cases} \tag{2}$$

In 1995, Shih proposed the WFRFT by using a superposition method of the state function [3], and it was simply referred to as the SWFRFT. It can be defined as a linear combination of the four state functions, namely, the primitive function and the first-, second-, and third-order FTs. Based on this logic, it is independent of the previous various definitions. The definition is as follows:

$$\left(F^\alpha f\right)(t) = \sum_{l=0}^{3} A_l(\alpha)\, f_l(t). \tag{3}$$

Here, $f_0(t) = f(t)$, $f_1(t) = (Ff_0)(t)$, $f_2(t) = (Ff_1)(t)$, and $f_3(t) = (Ff_2)(t)$.

$$A_l(\alpha) = \cos\left(\frac{(\alpha - l)\pi}{4}\right)\cos\left(\frac{2(\alpha - l)\pi}{4}\right) \cdot \exp\left(-\frac{3(\alpha - l)i\pi}{4}\right). \tag{4}$$

In Figure 1, the gate function is selected as an original function, which is different from the weighted fractional order Fourier transform. When the order is 1, the SWFRFT equates to the Fourier transform of the signal.

After that, Liu et al. proposed the generalized WFRFT (GWFRFT) [5] by expanding Shih's definition. It is shown to have k-periodic eigenvalues with respect to the order of the Hermite–Gaussian functions.

2.2. Multifractional Fourier Transforms. Zhu et al. proposed the MFRFT, which is mainly used in image encryption [4]. It is defined as follows:

$$F_M^\alpha\left[f(x)\right] = \sum_{l=0}^{M-1} A_l(\alpha)\, f_l(x). \tag{5}$$

Here, $f_l(x) = F^{4l/M}[f(x)]$, and the weighting coefficient is

$$A_l(\alpha) = \frac{1}{M}\sum_{k=0}^{M-1} \exp\left[-\frac{2\pi ik(\alpha - l)}{M}\right], \tag{6}$$

so the MFRFT can be represented as

$$F_M^\alpha\left[f(x)\right] = \frac{1}{M}\sum_{l=0}^{M-1}\sum_{k=0}^{M-1} \exp\left[-\frac{2\pi ik(\alpha - l)}{M}\right] f_l(x). \tag{7}$$

Compared with the previous GWFRFT, the image encryption based on the MFRFT is more secure because it added to the key M.

The encryption keys are M=5 and $\alpha = \sqrt{2}$. Figures 2(a) and 2(b) show the original image and the encrypted image, respectively, and Figure 2(c) shows the intensity distribution of the encrypted image.

Next, Ran et al. proposed the generalized multifractional Fourier transform (GMFRFT) [7] and explained the SWFRFT using the generalized permutation matrix group. The weighting coefficient $A_l(\alpha)$ can be expressed as

$$\begin{pmatrix} B_0(\alpha) \\ B_1(\alpha) \\ \vdots \\ B_{M-1}(\alpha) \end{pmatrix} = \begin{pmatrix} W^{0\times 0} & W^{0\times 1} & \cdots & W^{0\times(M-1)} \\ W^{1\times 0} & W^{1\times 1} & \cdots & W^{1\times(M-1)} \\ \vdots & \vdots & \ddots & \vdots \\ W^{(M-1)\times 0} & W^{(M-1)\times 1} & \cdots & W^{(M-1)\times(M-1)} \end{pmatrix} \begin{pmatrix} A_0(\alpha) \\ A_1(\alpha) \\ \vdots \\ A_{M-1}(\alpha) \end{pmatrix}, \tag{8}$$

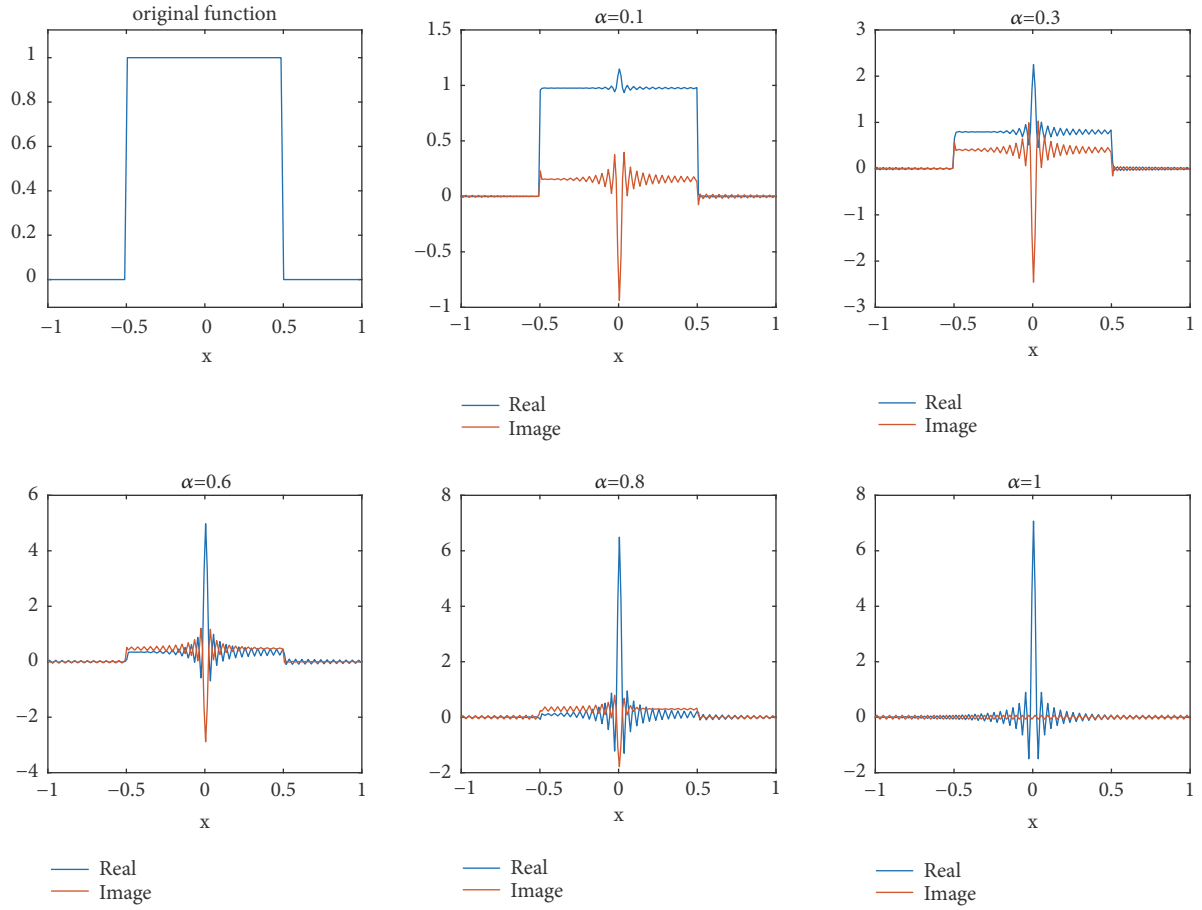


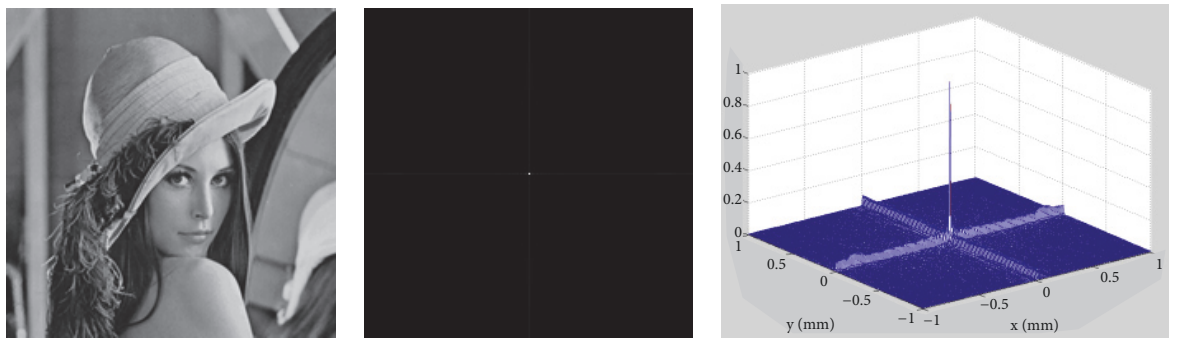
Figure 1: Different orders of WFRFT.

where $W = \exp(-2\pi i/M)$ and $B_l(\alpha) = \exp(-2\pi i\alpha l/M)$. When $M = 4$, the following equation is obtained. That is to say, SWFRFT is a special case.

$$\begin{pmatrix} B_0(\alpha) \\ B_1(\alpha) \\ B_2(\alpha) \\ B_3(\alpha) \end{pmatrix} = \begin{pmatrix} W^{0\times0} & W^{0\times1} & W^{0\times2} & W^{0\times3} \\ W^{1\times0} & W^{1\times1} & W^{1\times2} & W^{1\times3} \\ W^{2\times0} & W^{2\times1} & W^{2\times2} & W^{2\times3} \\ W^{3\times0} & W^{3\times1} & W^{3\times2} & W^{3\times3} \end{pmatrix} \begin{pmatrix} A_0(\alpha) \\ A_1(\alpha) \\ A_2(\alpha) \\ A_3(\alpha) \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{pmatrix} \begin{pmatrix} A_0(\alpha) \\ A_1(\alpha) \\ A_2(\alpha) \\ A_3(\alpha) \end{pmatrix}. \tag{9}$$

From (8), we obtain

$$\begin{pmatrix} A_0(\alpha) \\ A_1(\alpha) \\ \vdots \\ A_{M-1}(\alpha) \end{pmatrix} = \frac{1}{M} \begin{pmatrix} U^{0\times0} & U^{0\times1} & \cdots & U^{0\times(M-1)} \\ U^{1\times0} & U^{1\times1} & \cdots & U^{1\times(M-1)} \\ \vdots & \vdots & \ddots & \vdots \\ U^{(M-1)\times0} & U^{(M-1)\times1} & \cdots & U^{(M-1)\times(M-1)} \end{pmatrix} \begin{pmatrix} B_0(\alpha) \\ B_1(\alpha) \\ \vdots \\ B_{M-1}(\alpha) \end{pmatrix}, \tag{10}$$



(a) (b) (c)

Figure 2: The encryption based on the WFRFT: (a) original image, (b) encrypted image, and (c) intensity distribution of (b).

where $U = \exp(2\pi i/M) = \overline{W}$. Therefore, the weighted coefficient $A_l(\alpha)$ is

$$A_l(\alpha) = \frac{1}{M}\sum_{k=0}^{M-1}\exp\left[-\frac{2\pi ik(\alpha-l)}{M}\right]. \quad (11)$$

The definitions (SWFRFT [3], GWFRFT [5], and MFRFT [4]) are demonstrated using the generalized permutation matrix group and are also further explained in [7].

2.3. Multiparameter Fractional Fourier Transform. Here, if $B_l(\alpha) = B_l(\alpha, m_l, n_l) = \exp[-2\pi i(m_lM+1)\alpha(n_lM+l)/M]$, the weighted coefficient $A_l(\alpha)$ is obtained using (10) as

$$A_l(\alpha, \mathfrak{M}, \mathfrak{N}) = \frac{1}{M}\sum_{k=0}^{M-1}\exp\left\{\frac{-2\pi i}{M}\left[(m_kM+1)\alpha(k+n_kM)-lk\right]\right\}, \quad (12)$$

$\mathfrak{M} = (m_0, m_1, \ldots, m_{M-1}) \in \mathbb{Z}^M$. $\mathfrak{N} = (n_0, n_1, \ldots, n_{M-1}) \in \mathbb{Z}^M$.

Therefore, a new generalized WFRFT is obtained—the MPFRFT [10] and its definition can be written as

$$F_M^{\alpha}(\mathfrak{M}, \mathfrak{N})[f(x)] = \sum_{l=0}^{M-1} A_l(\alpha, \mathfrak{M}, \mathfrak{N}) f_l(x). \quad (13)$$

The algorithm is applied to image encryption and the parameters $(\mathfrak{M}, \mathfrak{N})$ can be used as the encryption keys, which greatly improves the security of the system.

In 2009, Ran et al. studied the function $B_l(\alpha, m_l, n_l) = \exp[-2\pi i(m_lM+1)\alpha(n_lM+l)/M]$ and proposed the equivalent definition function $B_l(\alpha, r_l) = \exp[-2\pi i\alpha(r_lM+l)/M]$. Then, the new weighted coefficient $A_l(\alpha, \mathfrak{R})$ can be obtained using (10) as

$$A_l(\alpha, \mathfrak{R}) = \frac{1}{M}\sum_{k=0}^{M-1}\exp\left\{\frac{-2\pi i}{M}\left[\alpha(k+r_kM)-lk\right]\right\}, \quad (14)$$

so the modified MPFRFT (m-MPFRFT) is obtained [11] as

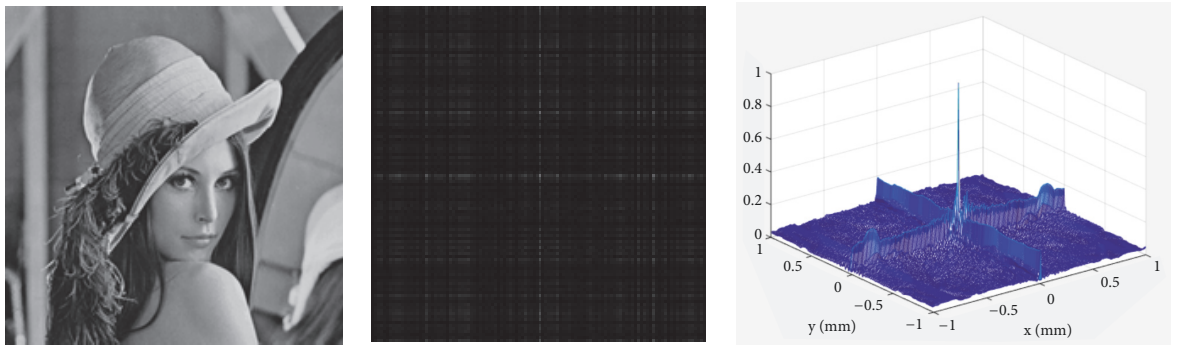
$$F_M^{\alpha}(\mathfrak{R})[f(x)] = \frac{1}{M}\sum_{l=0}^{M-1}\sum_{k=0}^{M-1}\exp\left\{\frac{-2\pi i}{M}\left[\alpha(k+r_kM)-lk\right]\right\} f_l(x). \quad (15)$$

The modified MPFRFT has the same basis function $f_l(x) = F^{4l/M}[f(x)]$, where $\mathfrak{R} = (r_0, r_1, \ldots, r_{(M-1)}) \in \mathbb{R}^M$.

The m-MPFRFT overcame the periodicity by extending the parameter range to the real number field, which had higher security. Hence, many image encryption schemes were proposed based on the m-MPFRFT [12–21]. In Figure 3, the simulation results are presented, and the parameters $K = (M, \alpha, \mathfrak{R}) = [4, \sqrt{5}, (\sqrt{13}, 5.2, \sqrt{3.4}, \sqrt{67})]$ are selected as the encryption keys. Figures 3(a) and 3(b) show the original image and the encrypted image, respectively, and Figure 3(c) shows the intensity distribution of the encrypted image.

2.4. Vector Power Multiparameter Fractional Fourier Transform. Recently, a new generalized WFRFT is proposed, which is called the VPMPFRFT [22]. First of all, the function $B_l(\alpha_l, r_l) = \exp[-2\pi i\alpha_l(r_lM+l)/M]$, where $l = 0, 1, \ldots, (M-1)$ is defined by the arguments $\overline{\alpha} = (\alpha_0, \alpha_1, \ldots, \alpha_{M-1}) \in \mathbb{R}^M$ and $\mathfrak{R} = (r_0, r_1, \ldots, r_{M-1}) \in \mathbb{R}^M$. According to the inverse transformation of the discrete Fourier transform, we have

$$\begin{pmatrix} A_0(\overline{\alpha}, \mathfrak{R}) \\ A_1(\overline{\alpha}, \mathfrak{R}) \\ \vdots \\ A_{M-1}(\overline{\alpha}, \mathfrak{R}) \end{pmatrix} = \frac{1}{M}\begin{pmatrix} U^{0\times0} & U^{0\times1} & \cdots & U^{0\times(M-1)} \\ U^{1\times0} & U^{1\times1} & \cdots & U^{1\times(M-1)} \\ \vdots & \vdots & \ddots & \vdots \\ U^{(M-1)\times0} & U^{(M-1)\times1} & \cdots & U^{(M-1)\times(M-1)} \end{pmatrix}\begin{pmatrix} B_0(\alpha_0, r_0) \\ B_1(\alpha_1, r_1) \\ \vdots \\ B_{M-1}(\alpha_{(M-1)}, r_{(M-1)}) \end{pmatrix}, \quad (16)$$



(a) (b) (c)

Figure 3: The encryption scheme of the m-MPFRFT: (a) original image, (b) encrypted image, and (c) intensity distribution of (b).

where $U = \exp(2\pi i/M)$. The $A_l(\overline{\alpha}, \mathfrak{R})$ expression is

$$A_l(\overline{\alpha}, \mathfrak{R}) = \frac{1}{M}\sum_{k=0}^{M-1} \exp\left\{\frac{-2\pi i}{M}\left[\alpha_k\left(k + r_k M\right) - lk\right]\right\}, \quad (17)$$

and then the VPMPFRFT is

$$F_M^{\overline{\alpha}}(\mathfrak{R})\left[f(x)\right] = \sum_{l=0}^{M-1} A_l(\overline{\alpha}, \mathfrak{R})\, f_l(x). \quad (18)$$

The basis function is $f_l(x) = F^{4l/M}[f(x)]$, where $l = 0, 1, \ldots, M-1$.

In Figure 4, the simulation results are presented, and the parameters $K = (M, \overline{\alpha}, \mathfrak{R}) = [4, (\sqrt{11}, \sqrt{5}, 7.56, \sqrt{8}), (\sqrt{23}, 5.2, \sqrt{3.4}, \sqrt{71})]$ are selected as the encryption keys. Figures 4(a) and 4(b) show the original image and the encrypted image, respectively, and Figure 4(c) shows the intensity distribution of the encrypted image.

The VPMPFRFT retains the parameter $\mathfrak{R}$, and the order α is extended from real numbers to real vectors. It overcomes the deficiency that a group of encryption keys has many different groups of decryption keys. The algorithm is a generalized WFRFT, which is of great theoretical significance and application value.

In short, the diversity of the WFRFT is essentially the difference in the eigenvalues. A complete set of eigenfunctions of the FRFT are produced by the Hermite-Gaussian function:

$$\psi_n(x) = \frac{1}{\sqrt{2^n n!\sqrt{\pi}}} H_n(t) \exp\left(-\frac{t^2}{2}\right), \quad (19)$$

where $H_n(x)$ is the n-th order Hermite polynomial. The diversity between each algorithm's eigenvalue is shown in Table 1.

3. Security Analysis

Image encryption has 4 periodicities based on the SWFRFT [3] and its key space is limited to $\alpha \in (0, 4)$. As such, the encryption key is $\alpha = \sqrt{5}$, and the ciphertext is shown in Figure 5(b). The decryption key can be $\alpha = -\sqrt{5}$ or $\alpha = -\sqrt{5} + 4n, (n \in \mathbb{Z})$, and the decryption results are shown in Figures 5(c) and 5(d), respectively.

Next, we provide some theoretical elaboration. From formula (4), we obtain

$$\begin{aligned} A_l(\alpha) &= \cos\left(\frac{(\alpha - l)\pi}{4}\right)\cos\left(\frac{2(\alpha - l)\pi}{4}\right) \\ &\cdot \exp\left(-\frac{3(\alpha - l)i\pi}{4}\right) = \frac{1}{2} \times \left[\exp\left(\frac{(\alpha - l)\pi i}{4}\right)\right. \\ &\left. + \exp\left(\frac{-(\alpha - l)\pi i}{4}\right)\right] \times \frac{1}{2} \times \left[\exp\left(\frac{2(\alpha - l)\pi i}{4}\right)\right. \\ &\left. + \exp\left(\frac{-2(\alpha - l)\pi i}{4}\right)\right] \times \exp\left(-\frac{3(\alpha - l)i\pi}{4}\right) \\ &= \frac{1}{4}\left(1 + \exp\left(-\frac{2(\alpha - l)\pi i}{4}\right)\right. \\ &\left. + \exp\left(-\frac{4(\alpha - l)\pi i}{4}\right) + \exp\left(-\frac{6(\alpha - l)\pi i}{4}\right)\right) \\ &= \frac{1}{4}\sum_{k=0}^{3} \exp\left(-\frac{2\pi i}{4}(\alpha - l)k\right). \end{aligned} \quad (20)$$

Then, for $n \in \mathbb{Z}$, we have

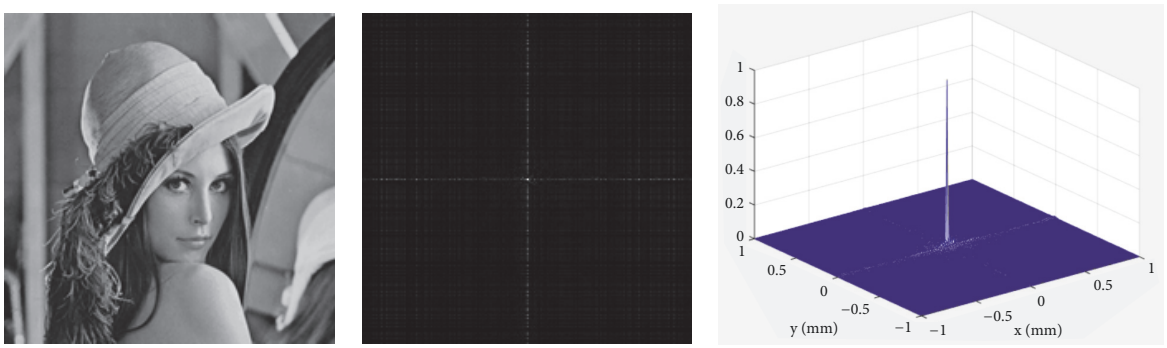
$$\begin{aligned} A_l(\alpha + 4n) &= \frac{1}{4}\sum_{k=0}^{3} \exp\left(-\frac{2\pi i}{4}(\alpha + 4n - l)k\right) \\ &= \frac{1}{4}\sum_{k=0}^{3} \exp\left(-\frac{2\pi i}{4}(\alpha - l)k\right)\exp\left(-\frac{8n\pi i}{4}\right) \\ &= A_l(\alpha). \end{aligned} \quad (21)$$

It turns out that the SWFRFT has 4 periodicities.

Then, the MFRFT was proposed [4]. It expands the key space $\alpha \in (0, M)$, where $M \geq 4$, $M \in \mathbb{Z}$, and improves the security. However, the algorithm still has periodicity (the period is M), which means that, for the encryption key $\alpha = \sqrt{5}$, the decryption keys can be $\alpha = -\sqrt{5}$ and $\alpha = -\sqrt{5} + M$.

Table 1: The algorithm's eigenvalue.

Type	Eigenvalues	Period
FRFT [25]	$\exp\left(\frac{-2\pi i\alpha}{4}n\right)$	∞
SWFRFT [3]	$\exp\left[\frac{-2\pi i\alpha}{4}\bmod(n,4)\right]$	4
GWFRFT [5]	$\exp\left[\frac{-2\pi i\alpha}{4l}\bmod(n,4l)\right]$	$4l$
MFRFT [4]	$\exp\left[\frac{-2\pi i\alpha}{M}\bmod(n,M)\right]$	M
MPFRFT [10]	$\exp\left\{\frac{-2\pi i\alpha}{M}\left[\bmod(n,M)+Mn_{\bmod(n,M)}\right]\left(Mm_{\bmod(n,M)}+1\right)\right\}$	M $\left(m_{\bmod(n,M)}\in\mathbb{Z}^n,\ n_{\bmod(n,M)}\in\mathbb{Z}^n\right)$
m-MPFRFT [11]	$\exp\left\{\frac{-2\pi i\alpha}{M}\left[Mn_{\bmod(n,M)}+\bmod(n,M)\right]\right\}$	∞ $\left(n_{\bmod(n,M)}\in\mathbb{R}^n\right)$
VPMPFRFT [22]	$\exp\left\{\frac{-2\pi i\alpha_{\bmod(n,M)}}{M}\left[Mn_{\bmod(n,M)}+\bmod(n,M)\right]\right\}$	∞ $\left(n_{\bmod(n,M)}\in\mathbb{R}^n\right)$



(a) (b) (c)

Figure 4: The encryption scheme of the VPMPFRFT: (a) original image, (b) encrypted image, and (c) intensity distribution of (b).

(a) (b) (c) (d)

Figure 5: The periodicity of the SWFRFT: (a) original image, (b) encrypted image with the key $\alpha=\sqrt{5}$, (c) image decrypted with the correct key $\alpha=-\sqrt{5}$, and (d) image decrypted with the wrong key $\alpha=-\sqrt{5}+8$.

Conversely, the MPFRFT [10] is presented with two vector parameters that are added as keys, and it has higher security than the previous algorithms. However, in another study, it was found that the algorithm has potential security flaws (due to periodicity and parameter redundancy).

In terms of the periodicity for the encryption key $(M,\alpha,\mathfrak{M},\mathfrak{N})$, the decryption keys can be $(M,-\alpha,\mathfrak{M},\mathfrak{N})$ or $(M,-\alpha+M,\mathfrak{M},\mathfrak{N})$. From weighted coefficient formula (12), we find

$$A_l(\alpha+M,\mathfrak{M},\mathfrak{N}) = \frac{1}{M}\sum_{k=0}^{M-1}\exp\left\{\frac{-2\pi i}{M}\left[\left(m_k M\right.\right.\right.$$

(a) (b) (c) (d)

Figure 6: The parameter redundancy of the MPFRFT: (a) original image, (b) encrypted image, (c) image decrypted by the correct key D, and (d) image decrypted with the wrong key D'.

$$
\begin{aligned}
&+1)(\alpha+M)(k+n_kM)-lk]\Big\}\\
&=\frac{1}{M}\sum_{k=0}^{M-1}\exp\left\{\frac{-2\pi i}{M}\left[(m_kM\right.\right.\\
&+1)\alpha(k+n_kM)-lk]\Big\}\exp\left(\frac{-2\pi i}{M}M(m_kM+1)\right.\\
&\left.\cdot(k+n_kM)\right),
\end{aligned}
\tag{22}
$$

where $m_k \in \mathbb{Z}^m$ and $n_k \in \mathbb{Z}^m$. Then, we obtain

$$
\begin{aligned}
&\exp\left(\frac{-2\pi i}{M}M(m_kM+1)(k+n_kM)\right)\\
&\quad=\exp\left(-2\pi i(m_kM+1)(k+n_kM)\right)=1.
\end{aligned}
\tag{23}
$$

Therefore,

$$
A_l(\alpha+M,\mathfrak{M},\mathfrak{N})=A_l(\alpha,\mathfrak{M},\mathfrak{N}).
\tag{24}
$$

This proves that the MPFRFT is periodic.

On the other hand, the MPFRFT has the potential risk of parameter redundancy in image encryption. For example, the encryption key is

$$
\begin{aligned}
E&=(M,\alpha,\mathfrak{M},\mathfrak{N})\\
&=\left[4,\sqrt{5},(6,5,13,7),(4,8,3,12)\right].
\end{aligned}
\tag{25}
$$

Therefore, the decryption keys can be

$$
\begin{aligned}
D&=(M,-\alpha,\mathfrak{M},\mathfrak{N})\\
&=\left[4,-\sqrt{5},(6,5,13,7),(9,8,3,12)\right]\\
\text{or } D'&=(M,-\alpha,\mathfrak{M},\mathfrak{N})\\
&=\left[4,-\sqrt{5},(0,0,0,0),(225,173,185,369)\right].
\end{aligned}
\tag{26}
$$

The simulation results are shown in Figure 6.

Formula (12) leads to

$$
\begin{aligned}
&A_l(\alpha,\mathfrak{M},\mathfrak{N})\\
&\quad=\frac{1}{M}\sum_{k=0}^{M-1}\exp\left\{\frac{-2\pi i}{M}\left[(m_kM\right.\right.\\
&\quad+1)\alpha(k+n_kM)-lk]\Big\}\\
&\quad=\frac{1}{M}\sum_{k=0}^{M-1}\exp\left\{\frac{-2\pi i}{M}\left[\left(m_kMk\right.\right.\right.\\
&\quad\left.\left.\left.+m_kn_kM^2+k+n_kM\right)\alpha-lk\right]\right\}\\
&\quad=\frac{1}{M}\sum_{k=0}^{M-1}\exp\left\{\frac{-2\pi i}{M}\left[\left(k\right.\right.\right.\\
&\quad\left.\left.\left.+n_k'M\right)\alpha-lk\right]\right\},
\end{aligned}
\tag{27}
$$

where $n_k' = m_kk + m_kn_kM + n_k$ and the two parameters m_k and n_k can be replaced by one parameter n_k'.

Therefore, the modified MPFRFT is proposed, which can overcome parameter redundancy. Furthermore, when the parameter $\mathfrak{R} = (r_0, r_1, \ldots, r_{(M-1)}) \in \mathbb{R}^M$, it overcomes the periodicity risk in image encryption. The theoretical analysis of formula (14) is as follows:

$$
\begin{aligned}
A_l(\alpha+M,\mathfrak{R})&=\frac{1}{M}\\
&\cdot\sum_{k=0}^{M-1}\exp\left\{\frac{-2\pi i}{M}\left[(\alpha+M)(k+r_kM)-lk\right]\right\}=\frac{1}{M}\\
&\cdot\sum_{k=0}^{M-1}\exp\left\{\frac{-2\pi i}{M}\left[\alpha(k+r_kM)-lk\right]\right\}\\
&\cdot\exp\left(\frac{-2\pi i}{M}M(k+r_kM)\right),
\end{aligned}
\tag{28}
$$

where $r_k \in \mathbb{R}^m$. Therefore, $\exp(-2\pi i(k + r_kM)) \neq 1$, and we have $A_l(\alpha + M, \mathfrak{R}) \neq A_l(\alpha, \mathfrak{R})$.

Since then, the m-MPFRFT has been widely used in image encryption, and it can be combined with other encryption methods to obtain higher security [12–21].

(a) (b) (c) (d)

Figure 7: The security vulnerability of the m-MPFRFT: (a) original image, (b) encrypted image, (c) image decrypted with the correct key D, and (d) image decrypted with the wrong key $D(\sqrt{7})$.

With further research, we find that the transformation has a security vulnerability that one group of encryption keys can result in many different groups of keys correctly decrypting the encrypted image. For example, take the encryption key

$$E = (M, \alpha, \mathfrak{R}) = \left[4, \sqrt{6}, \left(\sqrt{11}, \frac{5}{3}, \sqrt{14}, \sqrt{51}\right)\right]. \quad (29)$$

The decryption keys can be

$$\begin{aligned} D &= (M, -\alpha, \mathfrak{R}) = \left[4, -\sqrt{6}, \left(\sqrt{11}, \frac{5}{3}, \sqrt{14}, \sqrt{51}\right)\right] \\ \text{or } D(b) &= (M, -\alpha, \mathfrak{R} + b) \\ &= \left[4, -\sqrt{6}, \left(\sqrt{11} + b, \frac{5}{3} + b, \sqrt{14} + b, \sqrt{51} + b\right)\right], \\ & \qquad b \in \mathbb{R}. \end{aligned} \quad (30)$$

The simulation results are shown in Figure 7. The original image and the encrypted image are shown in Figures 7(a) and 7(b), respectively. The decrypted images are shown in Figures 7(c) and 7(d), which use the decryption keys D and $D(\sqrt{7})$, respectively.

Next, we analyze weighted coefficient formula (14). Let $y_k = k + r_k M$. Then, we obtain

$$\begin{aligned} A_l(\alpha, \mathfrak{R}) &= \frac{1}{M} \sum_{k=0}^{M-1} \exp\left\{\frac{-2\pi i}{M} \left[\alpha\left(k + r_k M\right) - lk\right]\right\}, \\ &= \frac{1}{M} \left(\exp\left(\frac{-2\pi i\alpha}{M} y_0\right), \exp\left(\frac{-2\pi i\alpha}{M} y_1\right), \ldots, \right. \\ &\quad \left. \exp\left(\frac{-2\pi i\alpha}{M} y_{M-1}\right)\right) \begin{pmatrix} \exp\left(\frac{2\pi il}{M} \cdot 0\right) \\ \exp\left(\frac{2\pi il}{M} \cdot 1\right) \\ \vdots \\ \exp\left(\frac{2\pi il}{M} \cdot (M-1)\right) \end{pmatrix}. \end{aligned} \quad (31)$$

We observe that

$$\begin{aligned} A_l(\alpha, \mathfrak{R} + b) &= \frac{1}{M} \\ &\cdot \sum_{k=0}^{M-1} \exp\left\{\frac{-2\pi i}{M} \left[\alpha\left(k + \left(r_k + b\right) M\right) - lk\right]\right\} \\ &= \frac{1}{M} \left(\exp\left(\frac{-2\pi i\alpha}{M} y_0\right) \exp\left(-2\pi i\alpha b\right), \right. \\ &\quad \exp\left(\frac{-2\pi i\alpha}{M} y_1\right) \exp\left(-2\pi i\alpha b\right), \ldots, \\ &\quad \left. \exp\left(\frac{-2\pi i\alpha}{M} y_{M-1}\right) \exp\left(-2\pi i\alpha b\right)\right) \\ &\quad \times \begin{pmatrix} \exp\left(\frac{2\pi il}{M} \cdot 0\right) \\ \exp\left(\frac{2\pi il}{M} \cdot 1\right) \\ \vdots \\ \exp\left(\frac{2\pi il}{M} \cdot (M-1)\right) \end{pmatrix} \\ &= \frac{\exp\left(-2\pi i\alpha b\right)}{M} \left(\exp\left(\frac{-2\pi i\alpha}{M} y_0\right), \right. \\ &\quad \left. \exp\left(\frac{-2\pi i\alpha}{M} y_1\right), \ldots, \exp\left(\frac{-2\pi i\alpha}{M} y_{M-1}\right)\right) \\ &\quad \cdot \begin{pmatrix} \exp\left(\frac{2\pi il}{M} \cdot 0\right) \\ \exp\left(\frac{2\pi il}{M} \cdot 1\right) \\ \vdots \\ \exp\left(\frac{2\pi il}{M} \cdot (M-1)\right) \end{pmatrix} = \exp\left(-2\pi i\alpha b\right) \\ &\quad \cdot A_l(\alpha, \mathfrak{R}). \end{aligned} \quad (32)$$

Thus,

$$F_M^{\alpha}(\mathfrak{R} + b)\left[f(x)\right] = \exp\left(-2\pi i\alpha b\right) \cdot F_M^{\alpha}(\mathfrak{R})\left[f(x)\right]. \quad (33)$$

Then,

$$F_M^{\alpha}(\mathfrak{R}) F_M^{-\alpha}(\mathfrak{R})\left[f(x)\right] = f(x). \quad (34)$$

(a) (b) (c) (d)

Figure 8: (a) Original image, (b) encrypted image, (c) image decrypted with the correct key D, and (d) image decrypted with the wrong key $D(\sqrt{5})$.

Therefore,

$$F_M^{\alpha}(\mathfrak{R})\,F_M^{-\alpha}(\mathfrak{R}+b)\left[f(x)\right]=\exp(2\pi i\alpha b)\,f(x). \tag{35}$$

This results in

$$\begin{aligned}\left|F_M^{\alpha}(\mathfrak{R})\,F_M^{-\alpha}(\mathfrak{R}+b)\left[f(x)\right]\right| &= \left|\exp(2\pi i\alpha b)\,f(x)\right| \\ &= f(x).\end{aligned} \tag{36}$$

For the amplitude plaintext $\sqrt{f(x,y)}$, this security risk will always exist.

Recently, the VPMPFRFT was proposed to overcome this security problem [23]. The principle is that the order is transformed from a real number to a set of real vectors.

From formula (17), we obtain

$$\begin{aligned}A_l(\overline{\alpha},\mathfrak{R}+b) &= \frac{1}{M} \\ &\cdot\sum_{k=0}^{M-1}\exp\left\{\frac{-2\pi i}{M}\left[\alpha_k\left(k+(r_k+b)M\right)-lk\right]\right\} \\ &= \frac{1}{M}\left(\exp\left(\frac{-2\pi i\alpha_0}{M}y_0\right)\right. \\ &\cdot\exp\left(-2\pi i\alpha_0 b\right),\exp\left(\frac{-2\pi i\alpha_1}{M}y_1\right) \\ &\cdot\exp\left(-2\pi i\alpha_1 b\right),\ldots,\exp\left(\frac{-2\pi i\alpha_{M-1}}{M}y_{M-1}\right) \\ &\left.\cdot\exp\left(-2\pi i\alpha_{M-1}b\right)\right) \\ &\times\begin{pmatrix}\exp\left(\frac{2\pi il}{M}\cdot 0\right)\\ \exp\left(\frac{2\pi il}{M}\cdot 1\right)\\ \vdots\\ \exp\left(\frac{2\pi il}{M}\cdot(M-1)\right)\end{pmatrix},\end{aligned} \tag{37}$$

where $y_k = k + r_kM$, $k = 0, 1, \cdots M-1$. When $\overline{\alpha} = (\alpha_0, \alpha_1, \ldots, \alpha_{M-1})$, this transformation overcomes the risk of parameter translation in image encryption.

We select the encryption key

$$\begin{aligned}E &= (M,\overline{\alpha},\mathfrak{R}) \\ &= \left[4,\left(5.3,\sqrt{7},8,\sqrt{11}\right),\left(\sqrt{23},13.6,35,\sqrt{31}\right)\right].\end{aligned} \tag{38}$$

Then, the decryption keys are

$$\begin{aligned}D &= (M,-\overline{\alpha},\mathfrak{R}) = \left[4,-\left(5.3,\sqrt{7},8,\sqrt{11}\right),\right. \\ &\left.\left(\sqrt{23},13.6,35,\sqrt{31}\right)\right], \\ D\left(\sqrt{5}\right) &= \left(M,-\overline{\alpha},\mathfrak{R}+\sqrt{5}\right) = \left[4,\right. \\ &-\left(5.3,\sqrt{7},8,\sqrt{11}\right), \\ &\left.\left(\sqrt{23}+\sqrt{5},13.6+\sqrt{5},35+\sqrt{5},\sqrt{31}+\sqrt{5}\right)\right].\end{aligned} \tag{39}$$

The simulation results are shown in Figure 8. The original image and the encrypted image are shown in Figures 8(a) and 8(b), respectively. The decrypted images are shown in Figures 8(c) and 8(d), respectively. As seen from Figure 8(d), the VPMPFRFT overcomes the security risk of parameter translation.

At this point, we analyze the diversity of the WFRFT with respect to the image encryption security. The security demands of the system promote the continuous development of WFRFT theory; however, the application of the algorithms in other fields requires further study.

4. Conclusions

The FT is widely used in many fields. The FRFT is a generalized form of the FT that has become the focus of researchers' attention. We presented a review of the applications of the WFRFT in image encryption. Via theoretical analysis, the relationship between the generalized WFRFTs is established using the generalized permutation matrix group, and a simulation verification is presented for image encryption. The significant advantages and potential weaknesses of each generalized WFRFT are being analyzed and illustrated with respect to their security. It is expected that, through these comparisons, a clear picture of the current developments in image encryption has been presented and some light has been shed on future developments.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

The authors would like to thank the reviewers for their valuable comments. This study was supported by the National Natural Science Foundation of China (no. 61702088), the Central University Basic Research Service Fees of China, (no. N172303014), and the School Ph.D. Fund of Northeastern University, Qinhuangdao, China (XNB201708).

References

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

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

[3] C.-C. Shih, "Fractionalization of Fourier transform," *Optics Communications*, vol. 118, no. 5-6, pp. 495–498, 1995.

[4] B. Zhu, S. Liu, and Q. Ran, "Optical image encryption based on multi-fractional Fourier transforms," *Optics Expresss*, vol. 25, no. 16, pp. 1159–1161, 2000.

[5] S. Liu, J. Jiang, Y. Zhang, and J. Zhang, "Generalized fractional Fourier transforms," *Journal of Physics A: Mathematical and General*, vol. 30, no. 3, pp. 973–981, 1997.

[6] Q.-W. Ran, L. Yuan, L.-Y. Tan, J. Ma, and Q. Wang, "High order generalized permutational fractional Fourier transforms," *Chinese Physics*, vol. 13, no. 2, pp. 0178–0186, 2004.

[7] Q. Ran, D. S. Yeung, E. C. Tsang, and Q. Wang, "General multifractional Fourier transform method based on the generalized permutation matrix group," *IEEE Transactions on Signal Processing*, vol. 53, no. 1, pp. 83–98, 2005.

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

[9] Z. Liu and S. Liu, "Random fractional Fourier transform," *Optics Expresss*, vol. 32, no. 15, pp. 2088–2090, 2007.

[10] T. Ran, L. Jun, and W. Yue, "Optical image encryption based on the multiple-parameter fractional Fourier transform," *Optics Expresss*, vol. 33, no. 6, pp. 581–583, 2008.

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

[12] N. Zhou, T. Dong, and J. Wu, "Novel image encryption algorithm based on multiple-parameter discrete fractional random transform," *Optics Communications*, vol. 283, no. 15, pp. 3037–3042, 2010.

[13] 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.

[14] J. Lang, R. Tao, and 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.

[15] J. Lang, "Image encryption based on the reality-preserving multiple-parameter fractional Fourier transform," *Optics Communications*, vol. 285, no. 10-11, pp. 2584–2590, 2012.

[16] M. Shan, J. Chang, Z. Zhong, and B. Hao, "Double image encryption based on discrete multiple-parameter fractional Fourier transform and chaotic maps," *Optics Communications*, vol. 285, no. 21-22, pp. 4227–4234, 2012.

[17] J. Lang, "A no-key-exchange secure image sharing scheme based on Shamir's three-pass cryptography protocol and the multiple-parameter fractional Fourier transform," *Optics Express*, vol. 20, no. 3, pp. 2386–2398, 2012.

[18] J. Lang, "Image encryption based on the reality-preserving multiple-parameter fractional Fourier transform and chaos permutation," *Optics and Lasers in Engineering*, vol. 50, no. 7, pp. 929–937, 2012.

[19] X. Luo, J. Fan, and J. Wu, "Single-channel color image encryption based on the multiple-order discrete fractional Fourier transform and chaotic scrambling," in *Proceedings of the IEEE International Conference on Information Science and Technology (ICIST)*, pp. 780–784, IEEE, China, 2012.

[20] J. Lang and Z. Hao, "Novel image fusion method based on adaptive pulse coupled neural network and discrete multi-parameter fractional random transform," *Optics and Lasers in Engineering*, vol. 52, no. 1, pp. 91–98, 2014.

[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] Q. Ran, T. Zhao, L. Yuan, J. Wang, and L. Xu, "Vector power multiple-parameter fractional Fourier transform of image encryption algorithm," *Optics and Lasers in Engineering*, vol. 62, pp. 80–86, 2014.

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

[24] V. Namias, "The fractional order Fourier transform and its application to quantum mechanics," *Journal of Applied Mathematics*, vol. 25, no. 3, pp. 241–265, 1980.

[25] A. C. McBride and F. H. Kerr, "On Namias's fractional Fourier transforms," *IMA Journal of Applied Mathematics*, vol. 39, no. 2, pp. 159–175, 1987.