Key Validity Using the Multiple-parameter Fractional Fourier Transform for Image Encryption

Tieyu Zhao (✉ zhaotieyu@neuq.edu.cn)

Northeastern University

Yingying Chi

Northeastern University

Research Article

Keywords: Multiple-parameter fractional Fourier transform, image encryption, weighted fractional Fourier transform, information security

Posted Date: May 13th, 2021

DOI: <https://doi.org/10.21203/rs.3.rs-504295/v1>

License: © ⓘ This work is licensed under a Creative Commons Attribution 4.0 International License.

[Read Full License](#)

Key validity using the multiple-parameter fractional Fourier transform for image encryption

Tieyu Zhao,^{1*} and Yingying Chi¹

¹Information Science Teaching and Research Section, Northeastern University at Qinhuangdao,
Qinhuangdao, 066004, China.

*Corresponding author: zhaotieyu@neuq.edu.cn

Abstract

Multiple-parameter fractional Fourier transform (MPFRFT) is proposed and applied to image encryption. The MPFRFT with two vector parameters has better security, which becomes the main technical means to protect information security. However, our study found that many keys of the MPFRFT are invalid, which greatly reduces its security. Theoretical analysis and numerical simulation verify our point of view.

Keywords: Multiple-parameter fractional Fourier transform; image encryption; weighted fractional Fourier transform; information security

1. Introduction

Tao et al. proposed an image encryption method based on multiple-parameter fractional Fourier transform (MPFRFT) [1]. In the encryption process, multiple keys are used to expand the key space of the system and thus have better security. Since then, the MPFRFT has become an important means to protect information security, and many research results have been proposed [2-16]. The MPFRFT is an extended definition of multifractional Fourier transform [17]. Compared with previous encryption schemes [17,18], the MPFRFT not only uses the period and the transformation order as the keys, but also introduces two vector parameters, and vector parameters increase with the increase of the period, so it has better security. The existing encryption schemes mainly focus on two aspects: One is to use the MPFRFT combined with other encryption methods to ensure security [2-7]. For example, its combination with chaos is currently the most used encryption strategy [2-5], and its combination with other scrambling techniques [6,7], and so on. The second is the improvement of the algorithm. The two vector parameters introduced by the MPFRFT are integers, which will face security risks in applications [8,9]. Therefore, some improved schemes have been proposed [8-16], for example, Ran et al. proposed a modified MPFRFT, which overcomes the security risk of parameter redundancy [8]; Zhao et al. proposed the vector power MPFRFT to overcome the security risk of parameter translation [14]; and Kang et al. presented a unified framework for the MPFRFT and proposed new type of transforms in signal processing and information security [15].

However, our research shows that many parameter keys of either the MPFRFT or its modified schemes are invalid, and it cannot obtain a larger key space with the increase of the period. This is determined by the periodicity of the basis function itself, and we will present a detailed analysis.

2. Reformulation of the MPFRFT

In order to demonstrate our point of view, we propose a new reformulation of the MPFRFT. Firstly, Tao et al. proposed the MPFRFT [1], which is defined as

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

where the basic functions can be expressed as $f_l(t) = F^{4l/M}[f(t)]$; $l = 0, 1, 2, \dots, M-1$. The

weighting coefficient $A_l^\alpha(\mathfrak{M}, \mathfrak{N})$ is expressed as

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

where $\mathfrak{M} = (m_0, m_1, \dots, m_{M-1}) \in \mathbb{Z}^M$, $\mathfrak{N} = (n_0, n_1, \dots, n_{M-1}) \in \mathbb{Z}^M$. According to Shih's definition [19],

the weighting coefficient A_l^α can also be expressed as

$$\begin{pmatrix} A_0^\alpha \\ A_1^\alpha \\ \vdots \\ A_{M-1}^\alpha \end{pmatrix} = \frac{1}{M} \begin{pmatrix} u^{0 \times 0} & u^{0 \times 1} & \dots & u^{0 \times (M-1)} \\ u^{1 \times 0} & u^{1 \times 1} & \dots & u^{1 \times (M-1)} \\ \vdots & \vdots & \ddots & \vdots \\ u^{(M-1) \times 0} & u^{(M-1) \times 1} & \dots & u^{(M-1) \times (M-1)} \end{pmatrix} \begin{pmatrix} B_0^\alpha \\ B_1^\alpha \\ \vdots \\ B_{M-1}^\alpha \end{pmatrix}, \quad (3)$$

where $u = \exp(-2\pi i/M)$, and

$$B_k^\alpha = \exp\left[\frac{2\pi i \alpha (m_k M + 1)(n_k M + k)}{M}\right], \quad (4)$$

where $k = 0, 1, 2, \dots, M-1$, $m_k \in \mathfrak{M}$ and $n_k \in \mathfrak{N}$.

Next, we will present a new reformulation of the MPFRFT, and Eq. (1) can be re-expressed as

$$\begin{aligned} F_M^\alpha(\mathfrak{M}, \mathfrak{N})[f(t)] &= A_0^\alpha(\mathfrak{M}, \mathfrak{N}) f_0(t) + A_1^\alpha(\mathfrak{M}, \mathfrak{N}) f_1(t) + \dots + A_{M-1}^\alpha(\mathfrak{M}, \mathfrak{N}) f_{M-1}(t) \\ &= A_0^\alpha F^{\frac{0}{M}}[f(t)] + A_1^\alpha F^{\frac{4}{M}}[f(t)] + \dots + A_{M-1}^\alpha F^{\frac{4(M-1)}{M}}[f(t)] \\ &= \left(A_0^\alpha I + A_1^\alpha F^{\frac{4}{M}} + \dots + A_{M-1}^\alpha F^{\frac{4(M-1)}{M}} \right) f(t) \\ &= \left(I, F^{\frac{4}{M}}, \dots, F^{\frac{4(M-1)}{M}} \right) \begin{pmatrix} A_0^\alpha \\ A_1^\alpha \\ \vdots \\ A_{M-1}^\alpha \end{pmatrix} f(t). \end{aligned} \quad (5)$$

From Eqs. (3) and (5), we can obtain

$$F_M^\alpha(\mathfrak{M}, \mathfrak{N})[f(t)] = \frac{1}{M} \left(I, F^{\frac{4}{M}}, \dots, F^{\frac{4(M-1)}{M}} \right) \begin{pmatrix} u^{0 \times 0} & u^{0 \times 1} & \dots & u^{0 \times (M-1)} \\ u^{1 \times 0} & u^{1 \times 1} & \dots & u^{1 \times (M-1)} \\ \vdots & \vdots & \ddots & \vdots \\ u^{(M-1) \times 0} & u^{(M-1) \times 1} & \dots & u^{(M-1) \times (M-1)} \end{pmatrix} \begin{pmatrix} B_0^\alpha \\ B_1^\alpha \\ \vdots \\ B_{M-1}^\alpha \end{pmatrix} f(t), \quad (6)$$

where $u = \exp(-2\pi i/M)$ and B_k^α is Eq. (4). Here, we let

$$\begin{cases} Y_0 = u^{0 \times 0} I + u^{1 \times 0} F^{\frac{4}{M}} + \dots + u^{(M-1) \times 0} F^{\frac{4(M-1)}{M}} \\ Y_1 = u^{0 \times 1} I + u^{1 \times 1} F^{\frac{4}{M}} + \dots + u^{(M-1) \times 1} F^{\frac{4(M-1)}{M}} \\ Y_2 = u^{0 \times 2} I + u^{1 \times 2} F^{\frac{4}{M}} + \dots + u^{(M-1) \times 2} F^{\frac{4(M-1)}{M}} \\ \vdots \\ Y_{M-1} = u^{0 \times (M-1)} I + u^{1 \times (M-1)} F^{\frac{4}{M}} + \dots + u^{(M-1) \times (M-1)} F^{\frac{4(M-1)}{M}} \end{cases} \quad (7)$$

Therefore, a new reformulation of the MPFRFT is obtained

$$\begin{aligned} F_M^\alpha(\mathfrak{M}, \mathfrak{N})[f(t)] &= \frac{1}{M} (Y_0, Y_1, \dots, Y_{M-1}) \begin{pmatrix} B_0^\alpha \\ B_1^\alpha \\ \vdots \\ B_{M-1}^\alpha \end{pmatrix} f(t) \\ &= \frac{1}{M} \sum_{k=0}^{M-1} Y_k B_k^\alpha f(t). \end{aligned} \quad (8)$$

where B_k^α is Eq. (4).

3. Security analysis

We know that the MPFRFT and the multifractional Fourier transform have the same basis function $F^{4l/M}$; $l = 0, 1, \dots, M-1$. Fractional Fourier transform (FRFT) has diversity, so we will discuss the eigendecomposition type FRFT and linear weighted type FRFT as basis functions respectively.

3.1 Eigendecomposition type FRFT as basis function

In [1], the basis function involved for the MPFRFT is defined as

$$F^\alpha[f(t)] = \int_{-\infty}^{\infty} K_\alpha(u, t) f(t) dt, \quad (9)$$

where the transform kernel is given by

$$K_\alpha(u, t) = \begin{cases} A_\alpha e^{i \frac{u^2 + t^2}{2} \cot \phi - i u t \csc \phi} & \alpha \neq k\pi \\ \delta(u - t) & \alpha = 2k\pi \\ \delta(u + t) & \alpha = (2k+1)\pi \end{cases}, \quad (10)$$

where $\phi = \alpha\pi/2$ is interpreted as a rotation angle in the phase plane and

$$A_\alpha = \sqrt{(1 - i \cot \alpha)/2\pi}.$$

As we all know, Eq. (9) is a continuous FRFT, and a discrete FRFT is used for numerical simulation. At present, the discrete definition [20] closest to the continuous FRFT is

$$F^\alpha(m, n) = \sum_{k=0}^{N-1} v_k(m) e^{-i\frac{\pi}{2}k\alpha} v_k(n), \quad (11)$$

where $v_k(n)$ are an arbitrary orthonormal eigenvectors set of the $N \times N$ discrete Fourier transform (DFT). Eq. (11) can be written as

$$F^\alpha = VD^\alpha V^H, \quad (12)$$

where $V = (v_0, v_1, \dots, v_{N-1})$, v_k is the k th order DFT Hermite eigenvector, and D^α is a diagonal matrix defined as

$$D^\alpha = \text{diag}\left(1, e^{-i\frac{\pi}{2}\alpha}, \dots, e^{-i\frac{\pi}{2}(N-2)\alpha}, e^{-i\frac{\pi}{2}(N-1)\alpha}\right), \quad \text{for } N \text{ odd}, \quad (13)$$

and

$$D^\alpha = \text{diag}\left(1, e^{-i\frac{\pi}{2}\alpha}, \dots, e^{-i\frac{\pi}{2}(N-2)\alpha}, e^{-i\frac{\pi}{2}(N)\alpha}\right), \quad \text{for } N \text{ even}. \quad (14)$$

We only prove that N is odd (when N is even, the proof process is the same). In [21,22], the eigenvalues of the DFT can be expressed as $\lambda_n = e^{n\pi i/2}$. Then, the possible values of the eigenvalue are $\lambda_n = \{1, -1, i, -i\}$. Therefore, there is

$$D^\alpha = \text{diag}\left((1)^\alpha, (-i)^\alpha, (-1)^\alpha, (i)^\alpha, (1)^\alpha, (-i)^\alpha, (-1)^\alpha, (i)^\alpha, \dots, (1 \text{ or } -1)^\alpha\right). \quad (15)$$

Thus, Eq. (7) can be written as

$$Y_k = u^{0 \times k} \times I + u^{1 \times k} \times F^{\frac{4}{M}} + \dots + u^{(M-1) \times k} \times F^{\frac{4(M-1)}{M}}, \quad (16)$$

where $u = \exp(-2\pi i/M)$ and $k = 0, 1, \dots, M-1$. The eigendecomposition type FRFT is used as the basis function, and Eq. (17) is obtained

$$\begin{aligned} Y_k &= u^{0 \times k} \times F^0 + u^{1 \times k} \times F^{\frac{4}{M}} + \dots + u^{(M-1) \times k} \times F^{\frac{4(M-1)}{M}} \\ &= u^{0 \times k} V D^0 V^H + u^{1 \times k} V D^{\frac{4}{M}} V^H + \dots + u^{(M-1) \times k} V D^{\frac{4(M-1)}{M}} V^H \\ &= u^{0 \times k} V \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & (-i)^0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & (1 \text{ or } -1)^0 \end{pmatrix} V^H + u^{1 \times k} V \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & (-i)^{\frac{4}{M}} & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & (1 \text{ or } -1)^{\frac{4}{M}} \end{pmatrix} V^H + \dots + u^{(M-1) \times k} V \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & (-i)^{\frac{4(M-1)}{M}} & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & (1 \text{ or } -1)^{\frac{4(M-1)}{M}} \end{pmatrix} V^H. \end{aligned} \quad (17)$$

Therefore, we obtain Eq. (18)

$$Y_k = V \begin{pmatrix} S^{(1)}(k) & 0 & \cdots & 0 \\ 0 & S^{(-i)}(k) & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & S^{(1 \text{ or } -1)}(k) \end{pmatrix} V^H. \quad (18)$$

From Eq. (18), the diagonal matrix only contains $S^{(1)}(k)$, $S^{(i)}(k)$, $S^{(-1)}(k)$, and $S^{(-i)}(k)$.

When the eigenvalue is 1, $S^{(1)}(k)$ can be expressed as

$$\begin{aligned} S^{(1)}(k) &= u^{0 \times k} 1^0 + u^{1 \times k} 1^{4/M} + \cdots + u^{(M-1) \times k} 1^{4(M-1)/M} \\ &= 1 + e^{-2\pi i k/M} + e^{-2\pi i 2k/M} + \cdots + e^{-2\pi i (M-1)k/M} \\ &= \frac{1 - \left(e^{-2\pi i k/M}\right)^M}{1 - e^{-2\pi i (k-0)/M}}. \end{aligned} \quad (19)$$

Therefore, we obtain

$$S^{(1)}(k) = \begin{cases} 0 & k \not\equiv 0 \pmod{M} \\ M & k \equiv 0 \pmod{M} \end{cases}. \quad (20)$$

When the eigenvalue is i , $S^{(i)}(k)$ can be expressed as

$$\begin{aligned} S^{(i)}(k) &= u^{0 \times k} (i)^0 + u^{1 \times k} (i)^{4/M} + \cdots + u^{(M-1) \times k} (i)^{4(M-1)/M} \\ &= 1 + e^{-2\pi i 1(k-1)/M} + e^{-2\pi i 2(k-1)/M} + \cdots + e^{-2\pi i (M-1)(k-1)/M} \\ &= \frac{1 - \left(e^{-2\pi i (k-1)/M}\right)^M}{1 - e^{-2\pi i (k-1)/M}}. \end{aligned} \quad (21)$$

Therefore, there is

$$S^{(i)}(k) = \begin{cases} 0 & k \not\equiv 1 \pmod{M} \\ M & k \equiv 1 \pmod{M} \end{cases}. \quad (22)$$

When the eigenvalue is -1, $S^{(-1)}(k)$ can be expressed as

$$\begin{aligned} S^{(-1)}(k) &= u^{0 \times k} (-1)^0 + u^{1 \times k} (-1)^{4/M} + \cdots + u^{(M-1) \times k} (-1)^{4(M-1)/M} \\ &= 1 + e^{-2\pi i 1(k-2)/M} + e^{-2\pi i 2(k-2)/M} + \cdots + e^{-2\pi i (M-1)(k-2)/M} \\ &= \frac{1 - \left(e^{-2\pi i (k-2)/M}\right)^M}{1 - e^{-2\pi i (k-2)/M}}. \end{aligned} \quad (23)$$

Then, we can obtain

$$S^{(-1)}(k) = \begin{cases} 0 & k \not\equiv 2 \pmod{M} \\ M & k \equiv 2 \pmod{M} \end{cases}. \quad (24)$$

When the eigenvalue is $-i$, $S^{(-i)}(k)$ can be expressed as

$$\begin{aligned}
S^{(-i)}(k) &= u^{0 \times k} (-i)^0 + u^{1 \times k} (-i)^{4/M} + \dots + u^{(M-1) \times k} (-i)^{4(M-1)/M} \\
&= 1 + e^{-2\pi i 1(k-3)/M} + e^{-2\pi i 2(k-3)/M} + \dots + e^{-2\pi i (M-1)(k-3)/M} \\
&= \frac{1 - \left(e^{-2\pi i (k-3)/M} \right)^M}{1 - e^{-2\pi i (k-3)/M}}.
\end{aligned} \tag{25}$$

Therefore, there is

$$S^{(-i)}(k) = \begin{cases} 0 & k \not\equiv 3 \pmod{M} \\ M & k \equiv 3 \pmod{M} \end{cases}. \tag{26}$$

From Eqs. (20), (22), (24) and (26), then Eq. (18) can be written as

$$Y_k = \begin{cases} Y_k & k = 0, 1, 2, 3 \\ 0 & k = 4, 5, \dots, M-1. \end{cases} \tag{27}$$

Thus, for Eq. (8), the MPFRFT is expressed as

$$\begin{aligned}
F_M^\alpha(\mathfrak{M}, \mathfrak{N})[f(t)] &= \frac{1}{M} (Y_0, Y_1, \dots, Y_{M-1}) \begin{pmatrix} B_0^\alpha \\ B_1^\alpha \\ \vdots \\ B_{M-1}^\alpha \end{pmatrix} f(t) \\
&= \frac{1}{M} (Y_0, Y_1, Y_2, Y_3, 0, \dots, 0) \begin{pmatrix} B_0^\alpha \\ B_1^\alpha \\ \vdots \\ B_{M-1}^\alpha \end{pmatrix} f(t) \\
&= \frac{1}{M} (Y_0 B_0^\alpha + Y_1 B_1^\alpha + Y_2 B_2^\alpha + Y_3 B_3^\alpha) f(t).
\end{aligned} \tag{28}$$

From Eq. (28), we find that there are only four effective weighted terms. That is, for the vector parameters $(\mathfrak{M}, \mathfrak{N})$ of the MPFRFT, only $(m_0, m_1, m_2, m_3; n_0, n_1, n_2, n_3)$ can be used as valid encryption keys, and the other keys $(m_4, m_5, \dots, m_{M-1}; n_4, n_5, \dots, n_{M-1})$ are invalid. This leads to the security of the MPFRFT is impaired.

3.2 Weighted type FRFT as basis function

The MPFRFT is a generalized multifractional Fourier transform, which has the same basis function $F^{4l/M}$. The multifraction Fourier transform is a generalized definition of the weighted fractional Fourier transform (WFRFT) [19]. The basis functions of the WFRFT are I, F, F^2, F^3 . Therefore, we can determine the time-frequency representation of the basis function, as shown in **Figure 1**. We consider using the WFRFT as the basis function of the MPFRFT.

Figure 1. Time-frequency denotation

Shih proposed the WFRFT [19], which is defined as

$$F^\alpha [f(t)] = \sum_{l=0}^3 A_l^\alpha f_l(t), \quad (29)$$

with

$$A_l^\alpha = \cos\left(\frac{(\alpha-l)\pi}{4}\right) \cos\left(\frac{2(\alpha-l)\pi}{4}\right) \exp\left(\frac{3(\alpha-l)i\pi}{4}\right), \quad (30)$$

where $f_l(t) = F^l[f(t)]$; $l=0,1,2,3$, (F denotes Fourier transform). Shih's WFRFT with **period 4** is also called 4-weighted type fractional Fourier transform (4-WFRFT). Eq. (29) can also be expressed as

$$\begin{aligned} F^\alpha [f(t)] &= (A_0^\alpha \cdot I + A_1^\alpha \cdot F + A_2^\alpha \cdot F^2 + A_3^\alpha \cdot F^3) f(t) \\ &= (I, F, F^2, F^3) \begin{pmatrix} A_0^\alpha \\ A_1^\alpha \\ A_2^\alpha \\ A_3^\alpha \end{pmatrix} f(t). \end{aligned} \quad (31)$$

According to the definition of the weighting coefficient A_l^α [19], then Eq. (31) can be expressed

as

$$F^\alpha [f(t)] = \frac{1}{4} (I, F, F^2, F^3) \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -i & -1 & i \\ 1 & -1 & 1 & -1 \\ 1 & i & -1 & -i \end{pmatrix} \begin{pmatrix} B_0^\alpha \\ B_1^\alpha \\ B_2^\alpha \\ B_3^\alpha \end{pmatrix} f(t), \quad (32)$$

where $B_k^\alpha = \exp\left(\frac{2\pi i k \alpha}{4}\right)$, $k=0,1,2,3$. Here, we let

$$\begin{cases} P_0 = I + F + F^2 + F^3 \\ P_1 = I - F * i - F^2 + F^3 * i \\ P_2 = I - F + F^2 - F^3 \\ P_3 = I + F * i - F^2 - F^3 * i. \end{cases} \quad (33)$$

Therefore, the WFRFT can be represented as

$$F^\alpha [f(t)] = \frac{1}{4} (P_0, P_1, P_2, P_3) \begin{pmatrix} B_0^\alpha \\ B_1^\alpha \\ B_2^\alpha \\ B_3^\alpha \end{pmatrix} f(t). \quad (34)$$

From Eqs. (7) and (34), we can obtain

$$\begin{aligned} Y_k &= u^{0 \times k} \times F^0 + u^{1 \times k} \times F^{\frac{4}{M}} + \dots + u^{(M-1) \times k} \times F^{\frac{4(M-1)}{M}} \\ &= \frac{1}{4} (P_0, P_1, P_2, P_3) \left(u^{0 \times k} \times \begin{pmatrix} B_0^0 \\ B_1^0 \\ B_2^0 \\ B_3^0 \end{pmatrix} + u^{1 \times k} \times \begin{pmatrix} B_0^{\frac{4}{M}} \\ B_1^{\frac{4}{M}} \\ B_2^{\frac{4}{M}} \\ B_3^{\frac{4}{M}} \end{pmatrix} + \dots + u^{(M-1) \times k} \times \begin{pmatrix} B_0^{\frac{4(M-1)}{M}} \\ B_1^{\frac{4(M-1)}{M}} \\ B_2^{\frac{4(M-1)}{M}} \\ B_3^{\frac{4(M-1)}{M}} \end{pmatrix} \right) \\ &= \frac{1}{4} (P_0, P_1, P_2, P_3) \begin{pmatrix} u^{0 \times k} \times B_0^0 + u^{1 \times k} \times B_0^{\frac{4}{M}} + \dots + u^{(M-1) \times k} \times B_0^{\frac{4(M-1)}{M}} \\ u^{0 \times k} \times B_1^0 + u^{1 \times k} \times B_1^{\frac{4}{M}} + \dots + u^{(M-1) \times k} \times B_1^{\frac{4(M-1)}{M}} \\ u^{0 \times k} \times B_2^0 + u^{1 \times k} \times B_2^{\frac{4}{M}} + \dots + u^{(M-1) \times k} \times B_2^{\frac{4(M-1)}{M}} \\ u^{0 \times k} \times B_3^0 + u^{1 \times k} \times B_3^{\frac{4}{M}} + \dots + u^{(M-1) \times k} \times B_3^{\frac{4(M-1)}{M}} \end{pmatrix}, \end{aligned} \quad (35)$$

where $k = 0, 1, \dots, M-1$, $u = \exp(-2\pi i/M)$ and $B_k^\alpha = \exp\left(\frac{2\pi i k \alpha}{4}\right)$. Therefore, Eq. (36) is obtained

$$\begin{aligned} Y_k &= \frac{1}{4} (P_0, P_1, P_2, P_3) \begin{pmatrix} 1 + \exp\left(\frac{-2\pi i k}{M}\right) + \exp\left(\frac{-2\pi i 2k}{M}\right) + \dots + \exp\left(\frac{-2\pi i (M-1)k}{M}\right) \\ 1 + \exp\left(\frac{-2\pi i k(k-1)}{M}\right) + \exp\left(\frac{-2\pi i 2(k-1)}{M}\right) + \dots + \exp\left(\frac{-2\pi i (M-1)(k-1)}{M}\right) \\ 1 + \exp\left(\frac{-2\pi i k(k-2)}{M}\right) + \exp\left(\frac{-2\pi i 2(k-2)}{M}\right) + \dots + \exp\left(\frac{-2\pi i (M-1)(k-2)}{M}\right) \\ 1 + \exp\left(\frac{-2\pi i k(k-3)}{M}\right) + \exp\left(\frac{-2\pi i 2(k-3)}{M}\right) + \dots + \exp\left(\frac{-2\pi i (M-1)(k-3)}{M}\right) \end{pmatrix} \\ &= \frac{1}{4} (P_0, P_1, P_2, P_3) \begin{pmatrix} Q_0(k) \\ Q_1(k) \\ Q_2(k) \\ Q_3(k) \end{pmatrix}. \end{aligned}$$

(36)

According to Eqs. (19), (21), (23) and (25), we can easily determine

$$Q_0(k) = \begin{cases} M & k \equiv 0 \pmod{M} \\ 0 & k \not\equiv 0 \pmod{M}, \end{cases} \quad (37)$$

$$Q_1(k) = \begin{cases} M & k \equiv 1 \pmod{M} \\ 0 & k \not\equiv 1 \pmod{M}, \end{cases} \quad (38)$$

$$Q_2(k) = \begin{cases} M & k \equiv 2 \pmod{M} \\ 0 & k \not\equiv 2 \pmod{M}, \end{cases} \quad (39)$$

and

$$Q_3(k) = \begin{cases} M & k \equiv 3 \pmod{M} \\ 0 & k \not\equiv 3 \pmod{M}. \end{cases} \quad (40)$$

Thus Eq. (36) is simplified as

$$Y_k = \begin{cases} \frac{M}{4} P_k & k = 0, 1, 2, 3 \\ 0 & k = 4, 5, \dots, M-1. \end{cases} \quad (41)$$

From Eq. (8), the MPFRFT can be expressed as

$$\begin{aligned} F_M^\alpha(\mathfrak{M}, \mathfrak{N})[f(t)] &= \frac{1}{M} (Y_0, Y_1, \dots, Y_{M-1}) \begin{pmatrix} B_0^\alpha \\ B_1^\alpha \\ \vdots \\ B_{M-1}^\alpha \end{pmatrix} f(t) \\ &= \frac{1}{4} (P_0, P_1, P_2, P_3, 0, \dots, 0) \begin{pmatrix} B_0^\alpha \\ B_1^\alpha \\ \vdots \\ B_{M-1}^\alpha \end{pmatrix} f(t) \\ &= \frac{1}{4} (P_0 B_0^\alpha + P_1 B_1^\alpha + P_2 B_2^\alpha + P_3 B_3^\alpha) f(t). \end{aligned} \quad (42)$$

At present, the MPFRFT has only four weighted terms, so the effective parameter keys are $(m_0, m_1, m_2, m_3; n_0, n_1, n_2, n_3)$. This is consistent with our previous analysis.

4. Simulation verification

In Eq. (8), the MPFRFT encryption keys are $(M, \alpha, \mathfrak{M}, \mathfrak{N})$. Here, M is a positive integer to determine the number of weighted terms ($M > 4$), α is the transformation order $\alpha \in \mathbb{R}$, $\mathfrak{M}$ and $\mathfrak{N}$ are vector parameters where $\mathfrak{M} = (m_0, m_1, \dots, m_{M-1}) \in \mathbb{Z}^M$ and $\mathfrak{N} = (n_0, n_1, \dots, n_{M-1}) \in \mathbb{Z}^M$. We set the keys to

$$\begin{cases} M = 7 \\ \alpha = \sqrt{5} \\ \mathfrak{M} = (m_0, m_1, m_2, m_3, m_4, m_5, m_6) = (45, 8, 20, 76, 657, 211, 7) \\ \mathfrak{N} = (n_0, n_1, n_2, n_3, n_4, n_5, n_6) = (3, 234, 54, 687, 763, 5, 365) \end{cases}$$

Therefore, the encryption keys can be represented as

$$(M; \alpha; \mathfrak{M}; \mathfrak{N}) = (7; \sqrt{5}; 45, 8, 20, 76, 657, 211, 7; 3, 234, 54, 687, 763, 5, 365)$$

and the decryption keys can be represented as

$$(M; \alpha; \mathfrak{M}; \mathfrak{N}) = (7; -\sqrt{5}; 45, 8, 20, 76, 657, 211, 7; 3, 234, 54, 687, 763, 5, 365)$$

The simulation results are shown in **Figure 2**. **Figure 2 (a)** is the original image, the encrypted image (ciphertext) is shown in **Figure 2 (b)**, and **Figure 2 (c)** is the decrypted image. Next, we select a set of wrong keys to decrypt the ciphertext. The selected wrong keys are

$$(M; \alpha; \mathfrak{M}; \mathfrak{N}) = (7; -\sqrt{5}; 45, 8, 20, 76, \textcolor{red}{98}, \textcolor{red}{321}, \textcolor{red}{65}; 3, 234, 54, 687, \textcolor{red}{73}, \textcolor{red}{425}, \textcolor{red}{5})$$

The wrong keys are used to decrypt the ciphertext, and the result is that the original image is well recovered as shown in **Figure 2(d)**.

Figure 2. Image encryption based on MPFRFT: (a) original image; (b) encrypted image; (c) decrypted image with correct keys; (d) decrypted image with wrong keys.

Our theoretical analysis is verified by numerical simulation. In the appendix, the Matlab code of the MPFRFT is presented, and interested researchers can verify it by themselves.

5. Conclusion

MPFRFT is widely used in information security, and its security mainly depends on parameter keys. However, our study found that many parameter keys are invalid. The MPFRFT is a generalized definition of the WFRFT. Its basis function is extended from the Fourier transform with period 4 to period M ($M > 4$). Our theoretical analysis shows that the weighted terms of the MPFRFT do not increase with the increase of the period, and there are only four weighted terms. Therefore, the keys of the system are limited, and the proponent cannot obtain a larger key space with the increase of the period. In this way, the security of the MPFRFT cannot be guaranteed.

Declaration of competing interests

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgments

On behalf of my co-authors, we would like to express our great appreciation to editor and reviewers. This study was supported by the Fundamental Research Funds for the Central Universities (N2123016); and the Scientific Research Projects of Hebei colleges and universities (QN2020511).

Appendix A

```
%% Multiple-parameter Fractional Fourier Transform (MPFRFT);
%Shih's fractional Fourier transform as basis function  $F^{(4 \times l/M)}$ .
function F = MPFRFT(alpha,M,ml,nl,N)
%This code is written by Tieyu Zhao,E-mail:zhaotieyu@neuq.edu.cn;
% alpha is the transform order;
% M is the resulting weighting term (period);
% ml and nl are parameters;
% N is the length of the signal;
for l=0:M-1
    yy=wfrft(N,4*l/M);    % WFRFT
    y{l+1}=yy;
end
Al=zeros(1,M);
for l=0:M-1
    for k=0:M-1

Al(l+1)=Al(l+1)+exp(2*pi*i*((alpha*(M*ml(k+1)+1)*(M*nl(k+1)+k))-
l*k)/M)/M;
    end
end
F=zeros(N);
for k=1:M
    F=F+Al(k)*y{k};
end

function F = wfrft(N,beta)
% Shih's fractional Fourier transform (WFRFT)
Y=eye(N);
y1=fftshift(fft(Y))/(sqrt(N));
y2=y1*y1;
y3=conj(y1);
p1=zeros(1,4);
for k=0:3
    p1(k+1)=p1(k+1)+exp(i*3*pi*(beta-k)/4)*cos(pi*(beta-
k)/2)*cos(pi*(beta-k)/4);
```

end

$F = p_1(1) * Y + p_1(2) * y_1 + p_1(3) * y_2 + p_1(4) * y_3;$

References

1. R. Tao, J. Lang, and Y. Wang, "Optical image encryption based on the multiple-parameter fractional Fourier transform," *Opt Lett* **33**, 581-583 (2008).
2. M. G. Shan, J. Chang, Z. Zhong, and B. G. Hao, "Double image encryption based on discrete multiple-parameter fractional Fourier transform and chaotic maps," *Opt Commun* **285**, 4227-4234 (2012).
3. J. Lang, "Image encryption based on the reality-preserving multiple-parameter fractional Fourier transform and chaos permutation," *Opt Laser Eng* **50**, 929-937 (2012).
4. J. Lang, "Color image encryption based on color blend and chaos permutation in the reality-preserving multiple-parameter fractional Fourier transform domain," *Opt Commun* **338**, 181-192 (2015).
5. L. S. Sui, K. K. Duan, and J. L. Liang, "Double-image encryption based on discrete multiple-parameter fractional angular transform and two-coupled logistic maps," *Opt Commun* **343**, 140-149 (2015).
6. S. Keshari, M. Salim, and S. G. Modani, "Single channel modified multiple-parameter fractional Fourier transform and scrambling technique," *Optik* **126**, 5845-5849 (2015).
7. H. L. Li, X. Y. Bai, M. G. Shan, Z. Zhong, L. Liu, and B. Liu, "Optical encryption of hyperspectral images using improved binary tree structure and phase-truncated discrete multiple-parameter fractional Fourier transform," *J Optics-Uk* **22**, 055701 (2020).
8. Q. W. Ran, H. Y. Zhang, J. Zhang, L. Y. Tan, and J. Ma, "Deficiencies of the cryptography based on multiple-parameter fractional Fourier transform," *Opt Lett* **34**, 1729-1731 (2009).
9. T. Y. Zhao and Q. W. Ran, "The Weighted Fractional Fourier Transform and Its Application in Image Encryption," *Math Probl Eng* **2019**, 4789194 (2019).
10. N. R. Zhou, T. J. Dong, and J. H. Wu, "Novel image encryption algorithm based on multiple-parameter discrete fractional random transform," *Opt Commun* **283**, 3037-3042 (2010).
11. J. Lang, "Image encryption based on the reality-preserving multiple-parameter fractional Fourier transform," *Opt Commun* **285**, 2584-2590 (2012).
12. 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," *Opt Express* **20**, 2386-2398 (2012).
13. Q. W. Ran, T. Y. Zhao, L. Yuan, J. Wang, and L. Xu, "Vector power multiple-parameter fractional Fourier transform of image encryption algorithm," *Opt Laser Eng* **62**, 80-86 (2014).
14. T. Y. Zhao, Q. W. Ran, L. Yuan, Y. Y. Chi, and J. Ma, "Security of image encryption scheme based on multi-parameter fractional Fourier transform," *Opt Commun* **376**, 47-51 (2016).
15. X. J. Kang, R. Tao, and F. Zhang, "Multiple-Parameter Discrete Fractional Transform and its Applications," *Ieee T Signal Proces* **64**, 3402-3417 (2016).
16. B. J. Chen, M. Yu, Y. H. Tian, L. D. Li, D. C. Wang, and X. M. Sun, "Multiple-parameter fractional quaternion Fourier transform and its application in colour image encryption," *Iet Image Process* **12**, 2238-2249 (2018).

17. B. H. Zhu, S. T. Liu, and Q. W. Ran, "Optical image encryption based on multifractional Fourier transforms," *Opt Lett* **25**, 1159-1161 (2000).
18. B. H. Zhu and S. T. Liu, "Optical image encryption based on the generalized fractional convolution operation," *Opt Commun* **195**, 371-381 (2001).
19. C. C. Shih, "Fractionalization of Fourier-Transform," *Opt Commun* **118**, 495-498 (1995).
20. C. Candan, M. A. Kutay, and H. M. Ozaktas, "The discrete fractional Fourier transform," *Ieee T Signal Proces* **48**, 1329-1337 (2000).
21. J. McClellan and T. Parks, "Eigenvalue and eigenvector decomposition of the discrete Fourier transform," *IEEE Transactions on Audio & Electroacoustics* **20**, 66-74 (1972).
22. B. Dickinson and K. Steiglitz, "Eigenvectors and functions of the discrete Fourier transform," *IEEE Transactions on Acoustics Speech & Signal Processing* **30**, 25-31 (1982).

Figures

Figure 1

Time-frequency denotation

Figure 2

Image encryption based on MPFRFT: (a) original image; (b) encrypted image; (c) decrypted image with correct keys; (d) decrypted image with wrong keys.