symmetry

MDPI

Article

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

Tieyu Zhao * and Yingying Chi

Information Science Teaching and Research Section, School of Mathematics and Statistics, Northeastern University at Qinhuangdao, Qinhuangdao 066004, China; chiyingying@neuq.edu.cn
* Correspondence: zhaotieyu@neuq.edu.cn

Abstract: As a symmetric encryption algorithm, 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. In this paper, we propose a new reformulation of MPFRFT and analyze it using eigen-decomposition-type fractional Fourier transform (FRFT) and weighted-type FRFT as basis functions, respectively. The results show that the effective keys are extremely limited. Furthermore, we analyze the extended encryption methods based on MPFRFT, which also have the security risk of key invalidation. Theoretical analysis and numerical simulation verify our point of view. Our discovery has important reference value for a class of generalized FRFT image encryption methods.

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

Citation: Zhao, T.; Chi, Y. Key Validity Using the Multiple-Parameter Fractional Fourier Transform for Image Encryption. *Symmetry* **2021**, *13*, 1803. https://doi.org/10.3390/sym13101803

Academic Editors: Rudolf Kawalla, Beloglazov Ilya and Jan Awrejcewicz

Received: 2 September 2021
Accepted: 26 September 2021
Published: 28 September 2021

1. Introduction

With the rapid development of information technology, image transmission has become an important means of communication. Traditional symmetric encryption algorithms (such as DES, AES, etc.) are very time-consuming and costly when applied to image encryption. The development of new image encryption algorithms has become the focus of research. Therefore, many image encryption methods have been proposed [1,2]. These include image encryption methods based on multiple-parameter fractional Fourier transform (MPFRFT) [3]. In 2008, Tao et al. proposed an image encryption method based on multiple-parameter fractional Fourier transform (MPFRFT) [3]. 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 [4–18]. The MPFRFT is an extended definition of multifractional Fourier transform [19]. Compared with previous encryption schemes [19,20], 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 [4–9]. For example, its combination with chaos is currently the most used encryption strategy [4–7], and its combination with other scrambling techniques [8,9], 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 [10,11]. Therefore, some improved schemes have been proposed [10–18]. For example, Ran et al. proposed a modified MPFRFT (m-MPFRFT), which overcomes the security risk of parameter redundancy [10], Zhao et al. proposed the vector power MPFRFT (VPMPFRFT) to overcome the security risk of parameter translation [16], and Kang et al. presented a unified framework for the MPFRFT and proposed new types of transforms in signal processing

and information security [17]. These new encryption methods improve the security of image encryption to a certain extent [10,15–17]. However, it is not difficult to find that such definitions have the same basis functions as MPFRFT. Whether the security risk of MPFRFT for image encryption affects these encryption methods is also the focus of this paper.

In this paper, we propose a new reformulation of MPFRFT. With the help of the proposed reformulation, the definition of MPFRFT is demonstrated to use eigen-decomposition-type FRFT and weighted-type FRFT as basis functions, respectively. 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 weighting term. 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 [3], which is defined as:

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

where the basic functions can be expressed as $f_l(t) = F^{4l/M}[f(t)]; l = 0, 1, 2, \cdots, M-1$. The weighting coefficient, $A_l^{\alpha}(\mathfrak{M},\mathfrak{N})$, is expressed as:

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

where $\mathfrak{M} = (m_0, m_1, \cdots, m_{M-1}) \in \mathbb{Z}^M$, $\mathfrak{N} = (n_0, n_1, \cdots, n_{M-1}) \in \mathbb{Z}^M$. According to Shih's definition [21], the weighting coefficient, A_l^{α}, can also be expressed as:

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

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

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

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

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

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

From Equations (3) and (5), we can obtain:

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

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

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

Therefore, a new reformulation of the MPFRFT is obtained, as:

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

where B_k^{α} is Equation (4).

3. Security Analysis

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

3.1. Eigen-Decomposition-Type FRFT as a Basis Function

In [3], the basis function involved in 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:

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

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 know, Equation (9) is a continuous FRFT, and a discrete FRFT is used for numerical simulation. At present, the discrete definition [22] 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 $v_k(n)$ is an arbitrary orthonormal eigenvectors set of the $N \times N$ discrete Fourier transform (DFT). Equation (11) can be written as:

$$F^{\alpha} = VD^{\alpha}V^{H}, \tag{12}$$

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

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

and

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

We only prove that N is odd (when N is even, the proof process is the same). In [23,24], 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:

$$D^{\alpha} = \mathrm{diag}\left((1)^{\alpha}, (-i)^{\alpha}, (-1)^{\alpha}, (i)^{\alpha}, (1)^{\alpha}, (-i)^{\alpha}, (-1)^{\alpha}, (i)^{\alpha}, \cdots\cdots, (1\ or -1)^{\alpha}\right). \tag{15}$$

Thus, Equation (7) can be written as:

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

where $u = \exp(-2\pi i/M)$ and $k = 0, 1, \cdots, M-1$. The eigen-decomposition-type FRFT is used as the basis function, and Equation (17) is obtained as:

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

Therefore, we obtain Equation (18) as:

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

From Equation (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:

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

Therefore, we obtain:

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

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

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

Therefore, there is:

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

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

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

Then, we can obtain:

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

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

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

Therefore, there is:

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

From Equations (20), (22), (24), and (26), then, Equation (18) can be written as:

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

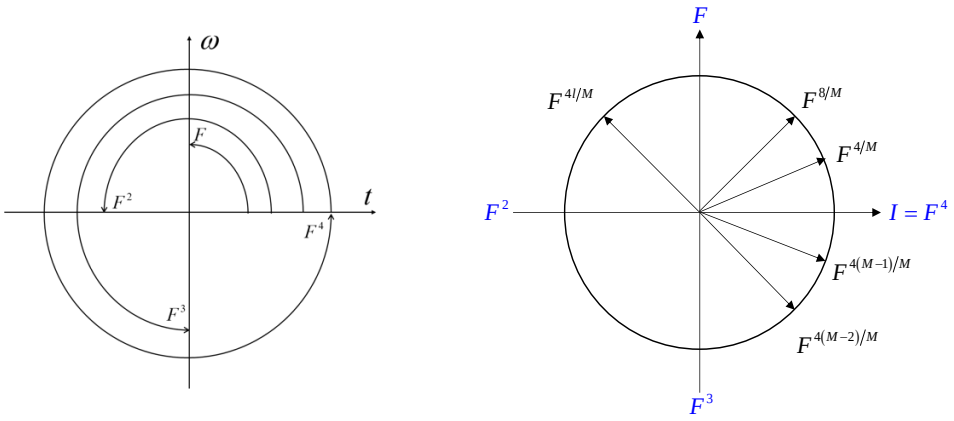
Thus, for Equation (8), the MPFRFT is expressed as:

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

From Equation (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 $(m_4, m_5, \cdots, m_{M-1}; n_4, n_5, \cdots, n_{M-1})$ are invalid. This leads to the security of the MPFRFT being impaired.

3.2. Weighted-Type FRFT as a Basis Function

The MPFRFT is a generalized multifractional Fourier transform, which has the same basis function, $F^{4l/M}$. The multifractional Fourier transform is a generalized definition of the weighted fractional Fourier transform (WFRFT) [21]. The basis functions of the WFRFT are I, F, F^2, and 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.



(**a**) (**b**)

Figure 1. (**a**) Time-frequency representation of Fourier transform, and (**b**) time-frequency representation of fractional Fourier transform.

Shih proposed the WFRFT [21], which is defined as:

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

with

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

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 the 4-weighted-type fractional Fourier transform (4-WFRFT). Equation (29) can also be expressed as:

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

According to the definition of the weighting coefficient, A_l^α [21], then, Equation (31) can be expressed as:

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

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

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

Therefore, the WFRFT can be represented as:

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

From Equations (7) and (34), we can obtain:

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

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

Equation (36) is obtained as:

$$\begin{aligned} Y_k &= \tfrac{1}{4}(P_0, P_1, P_2, P_3) \begin{pmatrix} 1+\exp\left(\frac{-2\pi i 1k}{M}\right)+\exp\left(\frac{-2\pi i 2k}{M}\right)+\cdots+\exp\left(\frac{-2\pi i(M-1)k}{M}\right) \\ 1+\exp\left(\frac{-2\pi i 1(k-1)}{M}\right)+\exp\left(\frac{-2\pi i 2(k-1)}{M}\right)+\cdots+\exp\left(\frac{-2\pi i(M-1)(k-1)}{M}\right) \\ 1+\exp\left(\frac{-2\pi i 1(k-2)}{M}\right)+\exp\left(\frac{-2\pi i 2(k-2)}{M}\right)+\cdots+\exp\left(\frac{-2\pi i(M-1)(k-2)}{M}\right) \\ 1+\exp\left(\frac{-2\pi i 1(k-3)}{M}\right)+\exp\left(\frac{-2\pi i 2(k-3)}{M}\right)+\cdots+\exp\left(\frac{-2\pi i(M-1)(k-3)}{M}\right) \end{pmatrix} \\ &= \tfrac{1}{4}(P_0, P_1, P_2, P_3) \begin{pmatrix} Q_0(k) \\ Q_1(k) \\ Q_2(k) \\ Q_3(k) \end{pmatrix}. \end{aligned} \tag{36}$$

According to Equations (19), (21), (23), and (25), we can easily determine:

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

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

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

and

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

Thus, Equation (36) is simplified as:

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

From Equation (8), the MPFRFT can be expressed as:

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

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 Equation (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

$\alpha \in \mathbb{R}$, and $\mathfrak{M}$ and $\mathfrak{N}$ are vector parameters, where $\mathfrak{M} = (m_0, m_1, \cdots, m_{M-1}) \in \mathbb{Z}^M$ and $\mathfrak{N} = (n_0, n_1, \cdots, n_{M-1}) \in \mathbb{Z}^M$. 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:

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

and the decryption keys can be represented as:

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

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

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

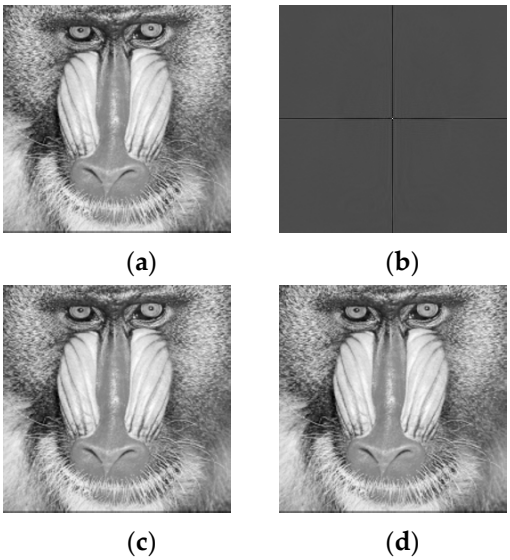


Figure 2. Image encryption based on MPFRFT: (**a**) original image, (**b**) encrypted image, (**c**) decrypted image with correct keys, and (**d**) decrypted image with wrong keys.

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

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

5. Discussion

The m-MPFRFT and VPMPFRFT are generalized definitions based on MPFRFT and are widely used in image encryption. Such image encryption methods will also have security risks of key invalidation.

In 2009, Ran et al. proposed a m-MPFRFT [10]. If B_k^α in Equation (4) becomes:

$$B_k^\alpha(r_k) = \exp\left[\frac{2\pi i \alpha (r_k M + k)}{M}\right], \tag{43}$$

then the weighting coefficient A_l^{α} becomes:

$$A_l^{\alpha}(\Re) = \frac{1}{M}\sum_{k=0}^{M-1}\exp\left\{\frac{2\pi i}{M}[\alpha(k+r_kM)-lk]\right\}, \tag{44}$$

where $\Re = (r_0, r_1, \cdots, r_{M-1}) \in \mathbb{R}^M$. Thus, the m-MPFRFT is obtained by:

$$F_M^{\alpha}(\Re)[f(x)] = \sum_{l=0}^{M-1} A_l^{\alpha}(\Re) f_l(x). \tag{45}$$

Recently, Zhao et al. proposed the definition of VPMPFRFT [15,16]. If B_k^{α} in Equation (4) becomes:

$$B_k^{\overline{\alpha}}(r_k) = \exp\left[\frac{2\pi i\alpha_k(r_kM+k)}{M}\right], \tag{46}$$

then the weighting coefficient A_l^{α} becomes:

$$A_l^{\overline{\alpha}}(\Re) = \frac{1}{M}\sum_{k=0}^{M-1}\exp\left\{\frac{2\pi i}{M}[\alpha_k(k+r_kM)-lk]\right\}, \tag{47}$$

where $\overline{\alpha} = (\alpha_0, \alpha_1, \cdots, \alpha_{M-1}) \in \mathbb{R}^M$, $\Re = (r_0, r_1, \cdots, r_{M-1}) \in \mathbb{R}^M$. Then, the definition of the VPMPFRFT can be expressed as:

$$F_M^{\overline{\alpha}}(\Re)[f(x)] = \sum_{l=0}^{M-1} A_l^{\overline{\alpha}}(\Re) f_l(x). \tag{48}$$

In the above definition, when B_k^{α} is given a different form, the corresponding weighting coefficient is A_l^{α}, and various definition forms are obtained. The common features of these definitions have the same basis function, $f_l(t) = F^{4l/M}[f(t)]$.

According to the analysis in Section 2, when Equation (43) replaces B_k^{α} of Equation (8), thus, the reformulation of m-MPFRFT can be obtained as:

$$F_M^{\alpha}(\Re)[f(t)] = \frac{1}{M}\sum_{k=0}^{M-1} Y_k B_k^{\alpha}(r_k) f(t). \tag{49}$$

Therefore, when Equation (46) replaces B_k^{α} of Equation (8), the reformulation of m-MPFRFT can be obtained as:

$$F_M^{\overline{\alpha}}(\Re)[f(t)] = \frac{1}{M}\sum_{k=0}^{M-1} Y_k B_k^{\overline{\alpha}}(r_k) f(t). \tag{50}$$

Compared with the definition of MPFRFT, m-WFRFT and VPMPFRFT are only different in the selection of B_k^{α}, while other basis functions are the same. That is, the effective weighting terms of Equations (49) and (50) are only 4. Such image encryption methods also have the security risk of key invalidation.

The m-MPFRFT is now applied to image encryption, and its keys are $(M, \alpha, \Re)$. Here, M is a positive integer to determine the number of weighted terms, α is the transformation order $\alpha \in \mathbb{R}$, and $\Re$ is the vector parameters, $\Re = (r_0, r_1, \cdots, r_{M-1}) \in \mathbb{R}^M$. In the numerical simulation, we take the keys as:

$$\begin{cases} M = 8 \\ \alpha = \sqrt{5} \\ \Re = (r_0, r_1, r_2, r_3, r_4, r_5, r_6, r_7) = \left(\sqrt{6}, \sqrt{51}, \sqrt{43}, 30, 38/3, \sqrt{19}, 11, \sqrt{62}\right) \end{cases}$$

Thus, the encryption keys are:

$$(M;\alpha;\Re) = \left(8;\sqrt{5};\sqrt{6},\sqrt{51},\sqrt{43},30,38/3,\sqrt{19},11,\sqrt{62}\right)$$

The original image and the encrypted image are shown in Figure 3a,b, respectively.

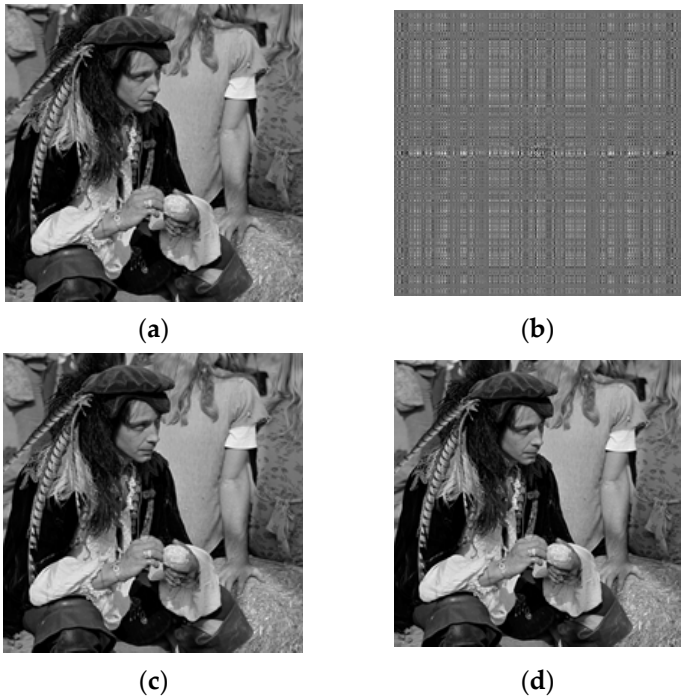


Figure 3. Image encryption based on m-MPFRFT: (**a**) original image, (**b**) encrypted image, (**c**) decrypted image with correct keys, and (**d**) decrypted image with wrong keys.

The correct decryption keys are:

$$(M;-\alpha;\Re) = \left(8;-\sqrt{5};\sqrt{6},\sqrt{51},\sqrt{43},30,38/3,\sqrt{19},11,\sqrt{62}\right)$$

The decrypted image is shown in Figure 3c.

According to our analysis, the vector parameters (r_4, r_5, r_6, r_7) are invalid. Therefore, when we use the wrong decryption keys as follows:

$$(M;-\alpha;\Re) = \left(8;-\sqrt{5};\sqrt{6},\sqrt{51},\sqrt{43},30,45,\sqrt{38},\sqrt{3},91\right)$$

we obtain the decrypted image shown in Figure 3d, and the original image can still be recovered intact.

The keys for an image encryption method based on VPMPFRFT are $(M, \overline{\alpha}, \Re)$, where M is a positive integer, $\overline{\alpha}$ and $\Re$ are vector parameters, $\overline{\alpha} = (\alpha_0, \alpha_1, \cdots, \alpha_{M-1}) \in \mathbb{R}^M$, and $\Re = (r_0, r_1, \cdots, r_{M-1}) \in \mathbb{R}^M$. In the numerical simulation, we take the keys as:

$$\begin{cases} M = 9 \\ \overline{\alpha} = (\alpha_0, \alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5, \alpha_6, \alpha_7, \alpha_8) = \left(\sqrt{6}, 17, \sqrt{19}, 30, 41/3, \sqrt{52}, 63, \sqrt{65}, 76\right) \\ \Re = (r_0, r_1, r_2, r_3, r_4, r_5, r_6, r_7, r_8) = \left(37/2, \sqrt{48}, \sqrt{59}, 70/3, 81, \sqrt{2}, 13/3, 24, \sqrt{35}\right) \end{cases}$$

Thus, the encryption keys are:

$$(M;\overline{\alpha};\Re) = \left(9;\sqrt{6},17,\sqrt{19},30,41/3,\sqrt{52},63,\sqrt{65},76;37/2,\sqrt{48},\sqrt{59},70/3,81,\sqrt{2},13/3,24,\sqrt{35}\right)$$

The original image is shown in Figure 4a, and Figure 4b shows the encrypted image.

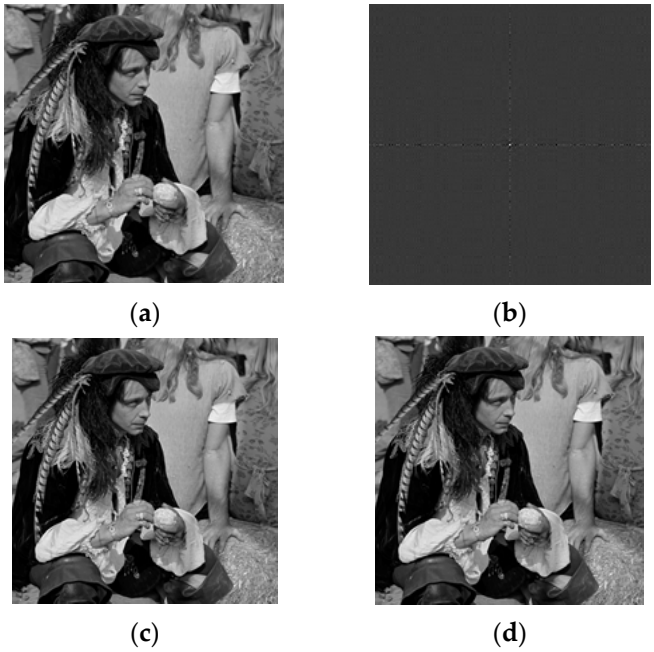


Figure 4. Image encryption based on VPMPFRFT: (**a**) original image, (**b**) encrypted image, (**c**) decrypted image with correct keys, and (**d**) decrypted image with wrong keys.

The correct decryption keys are:

$$(M; -\overline{\alpha}, \Re) = \Big(9; -\sqrt{6}, -17, -\sqrt{19}, -30, -41/3, -\sqrt{52}, -63, -\sqrt{65}, -76; \\ 37/2, \sqrt{48}, \sqrt{59}, 70/3, 81, \sqrt{2}, 13/3, 24, \sqrt{35}\Big)$$

The decrypted image is shown in Figure 4c.

According to our analysis, the vector parameter keys $(\alpha_4, \alpha_5, \alpha_6, \alpha_7, \alpha_8)$ and $(r_4, r_5, r_6, r_7, r_8)$ are invalid. Therefore, when we use the following wrong decryption keys:

$$(M; -\overline{\alpha}, \Re) = \Big(9; -\sqrt{6}, -17, -\sqrt{19}, -30, -3, -\sqrt{5}, -\sqrt{6}, -19, -\sqrt{7}; \\ 37/2, \sqrt{48}, \sqrt{59}, 70/3, \sqrt{8}, \sqrt{73}, 9, 56, \sqrt{58}\Big)$$

we obtain the decrypted image shown in Figure 4d, and the original image can still be recovered intact.

Both the image encryption method based on MPFRFT and the improved image encryption methods (m-MPFRFT, VPMPFRFT) have the security risk of key invalidation. The fundamental reason for this is caused by the period of the basis function. Since the basis function has a period of 4, there are only 4 valid weighting terms for the definitions (MPFRFT, m-MPFRFT, and VPMPFRFT). In practical application, the first parameter key is also invalid due to $B_k^{\alpha}(k = 0)$.

6. Conclusions

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. Moreover, we analyzed the generalized definitions (m-MPFRFT and VPMPFRFT) of MPFRFT and proposed the reformulation of

the definitions, which also have the security risk of key invalidation. Finally, numerical simulation verified our point of view.

Author Contributions: Methodology, T.Z.; software, T.Z.; validation, T.Z. and Y.C.; investigation, Y.C.; writing—original draft preparation, T.Z.; writing—review and editing, T.Z.; supervision, T.Z.; funding acquisition, T.Z. All authors have read and agreed to the published version of the manuscript.

Funding: 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).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Acknowledgments: The authors would like to express our great appreciation to the editor and reviewers.

Conflicts of Interest: The authors declare no conflict of interest.

Appendix A

Algorithm A1. MPFRFT_code

```
%% Multiple-parameter Fractional Fourier Transform (MPFRFT);
%Shih's fractional Fourier transform as basis function.
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);
pl=zeros(1,4);
for k=0:3
pl(k+1)=pl(k+1)+exp(i*3*pi*(beta-k)/4)*cos(pi*(beta-k)/2)*cos(pi*(beta-k)/4);
end
F=pl(1)*Y+pl(2)*y1+pl(3)*y2+pl(4)*y3;
```

References

1. Chen, W.; Javidi, B.; Chen, X. Advances in optical security systems. *Adv. Opt. Photon* **2014**, *6*, 120–155. [CrossRef]
2. Javidi, B.; Carnicer, A.; Yamaguchi, M.; Nomura, T.; Cabre, E.P.; Millan, M.; Nishchal, N.K.; Torroba, R.; Barrera, J.F.; He, W.; et al. Roadmap on optical security. *J. Opt.* **2016**, *18*, 083001. [CrossRef]
3. Tao, R.; Lang, J.; Wang, Y. Optical image encryption based on the multiple-parameter fractional Fourier transform. *Opt. Lett.* **2008**, *33*, 581–583. [CrossRef]
4. Shan, M.; Chang, J.; Zhong, Z.; Hao, B. Double image encryption based on discrete multiple-parameter fractional Fourier transform and chaotic maps. *Opt. Commun.* **2012**, *285*, 4227–4234. [CrossRef]
5. Lang, J. Image encryption based on the reality-preserving multiple-parameter fractional Fourier transform and chaos permutation. *Opt. Lasers Eng.* **2012**, *50*, 929–937. [CrossRef]
6. Lang, J. Color image encryption based on color blend and chaos permutation in the reality-preserving multiple-parameter fractional Fourier transform domain. *Opt. Commun.* **2015**, *338*, 181–192. [CrossRef]
7. Sui, L.; Duan, K.; Liang, J. Double-image encryption based on discrete multiple-parameter fractional angular transform and two-coupled logistic maps. *Opt. Commun.* **2015**, *343*, 140–149. [CrossRef]
8. Keshari, S.; Salim, M.; Modani, S.G. Single channel modified multiple-parameter fractional Fourier transform and scrambling technique. *Optik* **2015**, *126*, 5845–5849. [CrossRef]
9. Li, H.; Bai, X.; Shan, M.; Zhong, Z.; Liu, L.; Liu, B. Optical encryption of hyperspectral images using improved binary tree structure and phase-truncated discrete multiple-parameter fractional Fourier transform. *J. Opt.* **2020**, *22*, 055701. [CrossRef]
10. Ran, Q.W.; Zhang, H.Y.; Zhang, J.; Tan, L.Y.; Ma, J. Deficiencies of the cryptography based on multiple-parameter fractional Fourier transform. *Opt. Lett.* **2009**, *34*, 1729–1731. [CrossRef]
11. Zhao, T.; Ran, Q. The Weighted Fractional Fourier Transform and Its Application in Image Encryption. *Math. Probl. Eng.* **2019**, *2019*, 4789194. [CrossRef]
12. Zhou, N.; Dong, T.; Wu, J. Novel image encryption algorithm based on multiple-parameter discrete fractional random transform. *Opt. Commun.* **2010**, *283*, 3037–3042. [CrossRef]
13. Lang, J. Image encryption based on the reality-preserving multiple-parameter fractional Fourier transform. *Opt. Commun.* **2012**, *285*, 2584–2590. [CrossRef]
14. Lang, J. 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* **2012**, *20*, 2386–2398. [CrossRef]
15. Ran, Q.; Zhao, T.; Yuan, L.; Wang, J.; Xu, L. Vector power multiple-parameter fractional Fourier transform of image encryption algorithm. *Opt. Lasers Eng.* **2014**, *62*, 80–86. [CrossRef]
16. Zhao, T.; Ran, Q.; Yuan, L.; Chi, Y.; Ma, J. Security of image encryption scheme based on multi-parameter fractional Fourier transform. *Opt. Commun.* **2016**, *376*, 47–51. [CrossRef]
17. Kang, X.; Tao, R.; Zhang, F. Multiple-Parameter Discrete Fractional Transform and its Applications. *IEEE Trans. Signal Process.* **2016**, *64*, 3402–3417. [CrossRef]
18. Chen, B.; Yu, M.; Tian, Y.; Li, L.; Wang, D.; Sun, X. Multiple-parameter fractional quaternion Fourier transform and its application in colour image encryption. *IET Image Process.* **2018**, *12*, 2238–2249. [CrossRef]
19. Zhu, B.; Liu, S.; Ran, Q. Optical image encryption based on multifractional Fourier transforms. *Opt. Lett.* **2000**, *25*, 1159–1161. [CrossRef]
20. Zhu, B.; Liu, S. Optical image encryption based on the generalized fractional convolution operation. *Opt. Commun.* **2001**, *195*, 371–381. [CrossRef]
21. Shih, C.C. Fractionalization of Fourier-Transform. *Opt. Commun.* **1995**, *118*, 495–498. [CrossRef]
22. Candan, C.; Kutay, M.A.; Ozaktas, H.M. The discrete fractional Fourier transform. *IEEE Trans. Signal Process.* **2000**, *48*, 1329–1337. [CrossRef]
23. McClellan, J.; Parks, T. Eigenvalue and eigenvector decomposition of the discrete Fourier transform. *IEEE Trans. Audio Electroacoust.* **1972**, *20*, 66–74. [CrossRef]
24. Dickinson, B.; Steiglitz, K. Eigenvectors and functions of the discrete Fourier transform. *IEEE Trans. Acoust. Speech Signal Process.* **1982**, *30*, 25–31. [CrossRef]