Signal Encryption Strategy Based on Domain Change of the Fractional Fourier Transform

Wei Chen[1,2], Zunwei Fu[1], Loukas Grafakos[3], Yue Wu[1]

[1] *School of Mathematics and Statistics, Linyi University, Linyi 276000, China*
[2] *College of Information Technology, The University of Suwon, Hwaseong-si 18323, South Korea*
[3] *Department of Mathematics, University of Missouri, Columbia MO 65211, USA*

Abstract

This paper provides a double encryption algorithm that uses the lack of invertibility of the fractional Fourier transform (FRFT) on L^1. One encryption key is a function, which maps a "good" L^2-signal to a "bad" L^1-signal. The FRFT parameter which describes the rotation associated with this operator on the time-frequency plane provides the other encryption key. With the help of approximate identities, such as of the Abel and Gauss means of the FRFT established in [3], we recover the encrypted signal on the FRFT domain. This design of an encryption algorithm seems new even when using the classical Fourier transform. Finally, the feasibility of the new strategy is verified by simulation and audio examples.

Key words: fractional Fourier transform, signal encryption, approximate identities

1 Introduction

In view of the rapid development of communication and multimedia technology, the acquisition, transmission and processing of private data is of paramount importance in our digital era. Alongside with the development of digital technology, security concerns arise as a major undertaking. The implementation of data encryption and related algorithm research are key pillars to solving these problems. In the past decade, scholars have applied this research in various fields, such as telemedicine, patient data secure filing, voice communication, satellite transmission signal, and so on; on this we refer to [4, 7, 11, 13, 19, 29, 32] and references therein.

In the last two decades, the fractional Fourier transform (FRFT) has been widely favored in engineering, in view of its free parameters, its suitability in dealing with rotations in the time-frequency plane, and its convenience in algorithm adaptation; in fact, a number of algorithms have been established based on the FRFT. Moreover, the FRFT has found applications in aspects of research, such as artificial neural network, wavelet transform, time-frequency analysis, time-varying filtering, complex transmission and so on (see, e.g., [5, 16, 18, 22, 24, 28]). Moreover, it has also been used in partial differential equations (cf., [14, 17]), quantum mechanics (cf., [17, 21]), diffraction theory and optical transmission (cf., [19]), optical system and optical signal

processing (cf., [1, 12, 19]), optical image processing (cf., [12, 14]), etc. Earlier theoretical aspects of the FRFT can be found in [9, 10, 14, 15, 17, 30].

The FRFT can be interpreted as a form of the Fourier transform which incorporates a rotation of the coordinate axis on which the original signal is defined; this rotation is given counterclockwise about the origin in the time-frequency plane. Theoretically, we introduce the FRFT as an operator on $L^1(\mathbb{R})$ as follows: For $u \in L^1(\mathbb{R})$ and $\alpha \in \mathbb{R}$, the fractional Fourier transform of order α of u is defined by

$$(\mathcal{F}_\alpha u)(x) = \begin{cases} \int_{-\infty}^{+\infty} K_\alpha(x,t)u(t)\,\mathrm{d}t, & \alpha \neq n\pi, \quad n \in \mathbb{N}, \\ u(x), & \alpha = 2n\pi, \\ u(-x), & \alpha = (2n+1)\pi, \end{cases} \tag{1.1}$$

where

$$K_\alpha(x,t) = A_\alpha \exp\left[2\pi i\left(\frac{t^2}{2}\cot\alpha - xt\csc\alpha + \frac{x^2}{2}\cot\alpha\right)\right]$$

is the kernel of FRFT and

$$A_\alpha = \sqrt{1 - i\cot\alpha}. \tag{1.2}$$

It is obvious that when $\alpha = \pi/2$, the FRFT reduces to the ordinary Fourier transform, that is, $\mathcal{F}_{\pi/2} = \mathcal{F}$. Recall that the Fourier transform of u defined as

$$(\mathcal{F}u)(x) = \int_{-\infty}^{+\infty} u(t)e^{-2\pi ixt}\mathrm{d}t. \tag{1.3}$$

If the Fourier transform of a signal is another signal that lives on an axis perpendicular to the original signal time axis, the αth FRFT of a signal lives on the counterclockwise rotation by the angle α of the original signal time axis.

To the best of our knowledge, researchers have only applied the L^2 theory of FRFT and did not consider an L^1 theory. As the FRFT of L^1-signal, $\mathcal{F}_\alpha u$, may not be integrable in general, we cannot invert the FRFT on L^1. In [3], we developed the harmonic analysis theoretical background that addresses FRFT inversion issues of an L^1-signal via summability techniques. Based on our earlier research and inspired by the above literature, in this paper, we use this approximate inversion to study the signal encryption from a new perspective.

2   Mathematical background

In this section, we recall properties of FRFT and analyze their numerical adaptation. Define the chirp operator $\mathcal{M}_\alpha$ acting on functions ϕ in $L^1(\mathbb{R})$ as follows:

$$\mathcal{M}_\alpha\phi(x) = e^{\pi ix^2 \cot\alpha}\phi(x).$$

For $\alpha \neq n\pi$, let A_α be as in (1.2). Then the FRFT of $u \in L^1(\mathbb{R})$ can be written as

$$\begin{aligned}(\mathcal{F}_\alpha u)(x) &= A_\alpha e^{i\pi x^2 \cot\alpha}(\mathcal{F}e^{i\pi(\cdot)^2 \cot\alpha}u)(x\csc\alpha) \\ &= A_\alpha\mathcal{M}_\alpha(\mathcal{F}\mathcal{M}_\alpha u)(x\csc\alpha).\end{aligned} \tag{2.1}$$

In view of (2.1), we see that the FRFT of a signal $u(t)$ can be decomposed into four simpler operators, according to the diagram of Fig. 2.1:
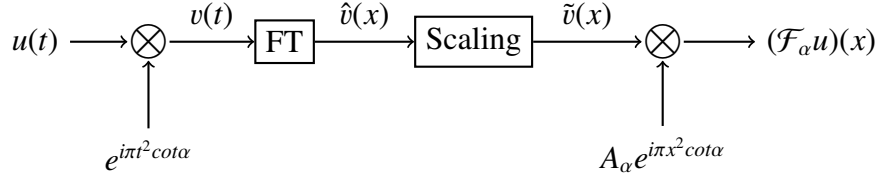
2

Figure 2.1: The decomposition of the FRFT.

(i) chirp modulation, $v(t) = e^{\pi i t^2 \cot \alpha} u(t)$;

(ii) Fourier transform, $\hat{v}(x) = (\mathcal{F}v)(x)$;

(iii) scaling, $\tilde{v}(x) = \hat{v}(x \csc \alpha)$;

(iv) chirp modulation, $(\mathcal{F}_\alpha u)(x) = A_\alpha e^{\pi i x^2 \cot \alpha} \tilde{v}(x)$.

Generally speaking, the FRFT was studied on the Schwartz space $S(\mathbb{R})$ or on $L^2(\mathbb{R})$. Thanks to topological properties of these spaces, the operator $\mathcal{F}_\alpha$ on $S(\mathbb{R})$ or $L^2(\mathbb{R})$ is unitary, invertible (with inverse transform $\mathcal{F}_{-\alpha}$) and forms an additive group (i.e., $\mathcal{F}_{\alpha_1}\mathcal{F}_{\alpha_2} = \mathcal{F}_{\alpha_1+\alpha_2}$). However, many common functions do not belong to $S(\mathbb{R})$ or $L^2(\mathbb{R})$. For example, the following useful signal on the line

$$u(t) = \begin{cases} ne^{-i\pi x^2 \cot \alpha}, & n \le t < n + \frac{1}{n^3}, \\ 0, & \text{otherwise.} \end{cases} \tag{2.2}$$

lies in $L^1(\mathbb{R})$ but not in $L^2(\mathbb{R})$. Using (1.1), we calculate the FRFT of this function:

$$(\mathcal{F}_\alpha u)(x) = \frac{A_\alpha e^{i\pi x^2 \cot \alpha}}{2\pi i x \csc \alpha} \sum_{n=1}^{\infty} n e^{-2n\pi i x \csc \alpha} \left(1 - e^{-\frac{2\pi i x \csc \alpha}{n^3}}\right),$$

where A_α is as in (1.2).

In the $L^1(\mathbb{R})$ setting, problems of convergence arise when studying FRFT inversion. Given the FRFT of an L^1-signal of in fractional Fourier domain, how to recover it back into time domain to be the original signal? We naturally hope that

$$(\mathcal{F}_{-\alpha}\mathcal{F}_\alpha u)(t) = \int_{-\infty}^{+\infty} (\mathcal{F}_\alpha u)(x) K_{-\alpha}(x, t) \mathrm{d}x = u(t) \tag{2.3}$$

Unfortunately, when u is integrable, one may not necessarily have that $\mathcal{F}_\alpha u$ is integrable, so the integral in (2.3) might not make sense. In fact, $\mathcal{F}_\alpha u$ is nonintegrable in general (cf., [6, pp. 12]). For example, let

$$u(t) = e^{-\pi i t^2} |t|^{-1/2} \operatorname{rect}(t). \tag{2.4}$$

Then $u \in L^1(\mathbb{R})$ but

$$U(x) := (\mathcal{F}_{\pi/4} u)(x) = 2^{3/4} A_\alpha e^{i\pi x^2} \frac{C\left(\sqrt{\frac{2^{3/2}}{\pi}|x|}\right)}{\sqrt{|x|}} \tag{2.5}$$

3

and $U \notin L^1(\mathbb{R})$. Then $\mathcal{F}_{-\alpha}\mathcal{F}_{\alpha}u$ does not make sense. Here rect(t) is the rectangle function on the line defined by

$$\text{rect}(t) = \begin{cases} 1, & |t| \le 1, \\ 0, & |t| > 1, \end{cases}$$

and C(x) is the Fresnel cosine integral function defined by $\text{C}(x) = \int_0^x \cos \frac{\pi s^2}{2} \mathrm{d}s$.

In order to overcome the difficulty of non-integrability and recover the original signal, we adopt the idea of inversion via summability means, established in our earlier work [3].

Definition 2.1. Given $\Phi \in C_0(\mathbb{R})$ and $\Phi(0) = 1$, a function u, and $\varepsilon > 0$ we define

$$M_{\varepsilon,\Phi_{\alpha}}(u) := \int_{-\infty}^{+\infty} (\mathcal{F}_{\alpha}u)(x)K_{-\alpha}(x,\cdot)\Phi_{\alpha}(\varepsilon x)\mathrm{d}x,$$

where

$$\Phi_{\alpha}(x) := \Phi(x \csc \alpha).$$

The expressions $M_{\varepsilon,\Phi_{\alpha}}(u)$ (with varying ε) are called the Φ_{α} *means of the fractional Fourier integral of u.*

The following results concern FRFT approximate identities.

Theorem 2.1. *If $\Phi, \mathcal{F}\Phi \in L^1(\mathbb{R})$ and $\|\mathcal{F}\Phi\|_{L^1} = 1$, then the Φ_{α} means of the fractional Fourier integral of u are convergent to u in the sense of L^1 norm, that is,*

$$\lim_{\varepsilon \to 0} \left\|M_{\varepsilon,\Phi_{\alpha}}(u) - u\right\|_{L^1} = 0.$$

Theorem 2.2. *Suppose that $\Phi, \mathcal{F}\Phi$ lie in $L^1(\mathbb{R})$ and that the function $\psi(x) = \sup_{|t| \ge |x|} |(\mathcal{F}\Phi)(t)|$ is integrable over the line and $\|\mathcal{F}\Phi\|_{L^1} = 1$. Then the Φ_{α} means of the fractional Fourier integral of f are a.e. convergent to f, that is,*

$$M_{\varepsilon,\Phi_{\alpha}}(u)(t) \to u(t)$$

as $\varepsilon \to 0$ for almost all $t \in \mathbb{R}$.

Even if $\mathcal{F}_{\alpha}u$ is non-integrable, once multiplied by a smooth cutoff, its inverse FRFT can be defined. Then, in view of theorems 2.1 and 2.2, we can reconstruct the original signal u as a limit of the Φ_{α} means of $\mathcal{F}_{\alpha}u$ as $\varepsilon \to 0$.

In engineering applications, it is necessary to calculate the discrete fractional Fourier transform (DFRFT). It is not surprising that the numerical implementation of the DFRFT is more complicated than that of the ordinary discrete Fourier transform (DFT). At present, there are various types of fast DFRFT algorithms with different processing methods and variable accuracy (cf., [2, 20, 23]). These form the basis for the successful application of FRFT in signal processing. A basic point in the definition of the discrete FRFT is its sufficient proximity to the continuous FRFT. To recover the original signal from the fractional Fourier domain back to the time domain, one usually tries to numerically calculate the FRFT of order $-\alpha$ of (2.5). If we ignore the domain of the original signal in the implementation of the algorithm, we will not be able to successfully restore the signal. The essential reason is that (2.5) is not integrable.

3 Signal encryption and decryption

3.1 Encryption algorithm

From the perspective of signal encryption, the difficulty of the FRFT inversion problem of L^1 functions can be used to improve the security of the encryption. Specifically, for a real-valued signal u, we first map it to a signal v which lies in $L^1(\mathbb{R}) \backslash L^2(\mathbb{R})$, and then through the fractional Fourier transform, we obtain the encrypted signal $u^e = \mathcal{F}_\alpha v$; here and in the sequel, the superscript e indicates the encryption process and the superscript d indicates the decryption process. This kind of encryption based on FRFT usually needs to use the inverse FRFT $\mathcal{F}_{-\alpha}$ when decrypting. However, as mentioned above, the inverse transform $\mathcal{F}_{-\alpha} u^e$ does not make sense if $u^e \notin L^1(\mathbb{R})$. This presents deciphering complications, even if the secret key α is known.

The FRFT is a common and efficient tool in signal encryption. The difficulty of deciphering can be enhanced by adding keys such as the multiple iterations in [11], combinations with the jigsaw transform [7], joint transform correlators [29], the region shift encoding [4], chaotic maps [32], multiple-phase codes [13], etc. This paper only focuses on algorithms involving special properties of FRFT on $L^1(\mathbb{R})$.

Theorem 3.1. *For any bounded function u and $\omega \in L^1(\mathbb{R}) \setminus L^2(\mathbb{R})$ with $\omega(t) \neq 0$ for $t \in \mathbb{R}$, let $P_\omega u = u_\omega := (u + M)\omega$, $M = 1 + \sup_{t \in \mathbb{R}} |u(t)|$. Then $u_\omega \in L^1(\mathbb{R}) \setminus L^2(\mathbb{R})$.*

Proof. Because $1 \le u(t) + M \le 2M$, then

$$\int_{-\infty}^{+\infty} |u_\omega(t)| \, \mathrm{d}x = \int_{-\infty}^{+\infty} |u(t) + M| \, |\omega(t)| \mathrm{d}t$$
$$\le 2M \int_{-\infty}^{+\infty} |\omega(t)| \, \mathrm{d}t < +\infty,$$

and

$$\int_{-\infty}^{+\infty} |u_\omega(t)|^2 \, \mathrm{d}x = \int_{-\infty}^{+\infty} |u(t) + M|^2 \, |\omega(t)|^2 \mathrm{d}t$$
$$\ge \int_{-\infty}^{+\infty} |\omega(t)|^2 \, \mathrm{d}t = +\infty.$$

Then, we have $u_\omega \in L^1(\mathbb{R})$ and $u_\omega \notin L^2(\mathbb{R})$. The desired result is proved. □

Consider the following examples:

$$\omega_1(t) = \sum_{i=1}^{n} |t - \tau_i|^{-1/2} \chi_{[-k,k]}(t), \tag{3.1}$$
$$\tau_i \in [-k, k], \ , k \in \mathbb{R}^+, \ i = 1, 2, \ldots, n,$$

$$\omega_2(t) = \sum_{n=1}^{\infty} \left(\sqrt{n} \chi_{(\frac{1}{n+1}, \frac{1}{n}]}(|t|) + \frac{\chi_{(n,n+1]}(|t|)}{(n+1)^2} \right), \tag{3.2}$$

where $\chi_{[a,b]}$ denotes the characteristic function of the interval $[a, b]$.
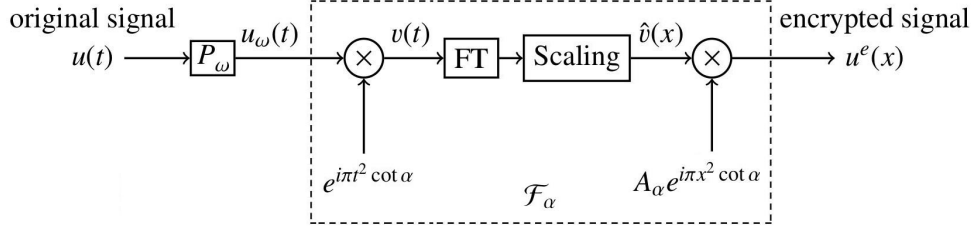
5

Figure 3.1: The process of encryption algorithm.

The function in (3.1) is a linear combination of functions of type (2.4), and obviously lies in $L^1(\mathbb{R}) \setminus L^2(\mathbb{R})$. Also,

$$\omega_2(t) = \begin{cases} \sqrt{n}, & \frac{1}{n+1} < |t| \le \frac{1}{n}, \\ \frac{1}{(n+1)^2} & n < |t| \le n+1, \end{cases} \quad n = 1, 2, \dots .$$

We have

$$\int_{\mathbb{R}} |\omega_2(t)| \, dt = 2 \sum_{n=1}^{\infty} \int_{\frac{1}{n+1}}^{\frac{1}{n}} \sqrt{n} \, dt + 2 \sum_{n=1}^{\infty} \int_{n}^{n+1} \frac{1}{(n+1)^2} \, dt$$

$$= 2 \sum_{n=1}^{\infty} \frac{1}{\sqrt{n}(n+1)} + 2 \sum_{n=1}^{\infty} \frac{1}{(n+1)^2} < \infty$$

and

$$\int_{\mathbb{R}} |\omega_2(t)|^2 \, dt = 2 \sum_{n=1}^{\infty} \int_{\frac{1}{n+1}}^{\frac{1}{n}} n \, dt + 2 \sum_{n=1}^{\infty} \int_{n}^{n+1} \frac{1}{(n+1)^4} \, dt$$

$$\ge 2 \sum_{n=1}^{\infty} \frac{1}{n+1} = \infty.$$

Remark 3.1. Denote by $Q_\omega u_\omega := \frac{u_\omega}{\omega} - M$, then it is easy to see that $Q_\omega u_\omega = u$. For example, let $u(t) = \mathrm{rect}(t)$, $\omega = \omega_1$. Then $P_\omega u \in L^1(\mathbb{R}) \setminus L^2(\mathbb{R})$ and $Q_\omega u_\omega = u(t) = \mathrm{rect}(t)$.

Let u be a bounded signal function to be encrypted. In this paper, we always assume that u is a real-valued function. First, we randomly select an n-dimensional sequence $\{\tau_i\} \in [-k, k]$ and then pick a function ω as in (3.1) to map u to u_ω. By Theorem 3.1, $u_\omega \in L^1(\mathbb{R}) \setminus L^2(\mathbb{R})$. Then, through the FRFT of order α, we get the encrypted signal $u^e = \mathcal{F}_\alpha u_\omega$. In view of the chirp decomposition of FRFT (Equ. (2.1)), the encryption process can be divided into the following steps, according to the diagram of Fig. 3.1:

(i) mapping u into $L^1(\mathbb{R}) \setminus L^2(\mathbb{R})$: $u_\omega = P_\omega u$;

(ii) chirp modulation: $v(t) = e^{\pi i t^2 \cot \alpha} u_\omega(t)$;

(iii) Fourier transformation (with scale variation):

$$\hat{v}(x) = (\mathcal{F} v)(x \csc \alpha);$$

6

(iv) chirp modulation: $u^e(x) = A_\alpha e^{\pi i x^2 \cot \alpha} \hat{v}(x) = \mathcal{F}_\alpha u_\omega$.

In this way, we obtain the encrypted signal in the fractional Fourier domain, which can be expressed as

$$u^e(x) = (\mathcal{F}_\alpha P_\omega u)(x)$$
$$= \int_{-\infty}^{+\infty} K_\alpha(x, t)(u(t) + M)\omega(t)\,dt, \tag{3.3}$$

where $M = 1 + \sup_{t \in \mathbb{R}} |u(t)|$.

Here, the algorithm has two secret keys: the operator P_ω (including sequence $\{\tau_i\}$) and the order α of FRFT. The keys here provide high security. On the one hand, the assurance that $u^e(x)$ is not integrable, provides instability in the reconstruction of the original signal through the inverse FRFT, as mentioned above. On the other hand, it is known that the operator $\mathcal{F}_\alpha$ is not continuous in the order α, that is, $\mathcal{F}_\beta$ may not map to $\mathcal{F}_\alpha$ as $\beta \to \alpha$. Therefore, it cannot be decrypted properly when the order α is unknown.

3.2   Decryption algorithm

In spaces where an inverse transform is inoperative, in order to introduce the decryption algorithm, we study inversion by adopting approximate identities. We focus on two functions that give rise to special Φ_α means (Definition 2.1). Denote by

$$\begin{cases} a_\alpha(x) = e^{-2\pi\varepsilon|\csc \alpha|\|x\|}, \\ g_\alpha(x) = e^{-4\pi^2 \varepsilon x^2 \csc^2 \alpha}. \end{cases} \tag{3.4}$$

The Φ_α means

$$M_{\varepsilon, a_\alpha}(u) := \int_{-\infty}^{+\infty} (\mathcal{F}_\alpha u)(x) K_{-\alpha}(x, \cdot) a_\alpha(x) dx$$

and

$$M_{\varepsilon, g_\alpha}(u) := \int_{-\infty}^{+\infty} (\mathcal{F}_\alpha u)(x) K_{-\alpha}(x, \cdot) g_\alpha(x) dx$$

are called the *Abel mean* and *Gauss mean* of the fractional Fourier integral of u, respectively. The following results are well-known.

Lemma 3.2 ([8, 27]). *Let $\varepsilon > 0$. Then*

(a) $\mathcal{F}\left[e^{-2\pi\varepsilon|\cdot|}\right](x) = \frac{1}{\pi} \frac{\varepsilon}{\varepsilon^2 + x^2} =: P_\varepsilon(x)$ (Poisson kernel);

(b) $\mathcal{F}\left[e^{-4\pi^2\varepsilon|\cdot|^2}\right](x) = \frac{1}{(4\pi\varepsilon)^{1/2}} e^{-x^2/4\varepsilon} =: G_\varepsilon(x)$ (Gauss-Weierstrass kernel).

(c) $G_\varepsilon, P_\varepsilon \in L^1(\mathbb{R})$;

(d) $\int_{-\infty}^{+\infty} G_\varepsilon(x)\,dx = \int_{-\infty}^{+\infty} P_\varepsilon(x)\,dx = 1$.
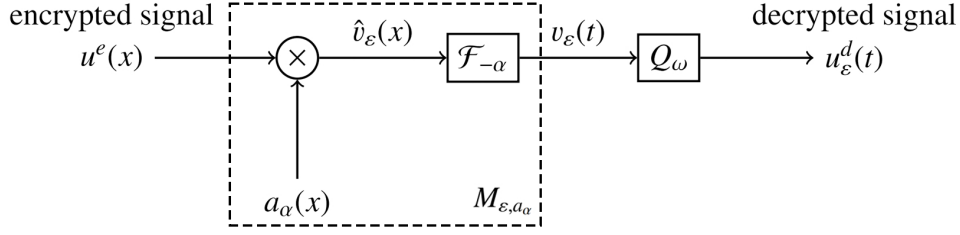
7

Figure 3.2: The process of decryption algorithm.

Combining with Theorem 2.1 and Theorem 2.2, we can obtain the following results immediately.

Theorem 3.3. *The Abel and Gauss means of the fractional Fourier integral of u^e (the encrypted signal) converge to u_ω in the sense of L^1 norm and a.e., that is,*

(i) $\lim\limits_{\varepsilon \to 0} \|\mathcal{F}_{-\alpha}(a_\alpha u^e) - u_\omega\|_{L^1} = 0,$

$\quad \lim\limits_{\varepsilon \to 0} \|\mathcal{F}_{-\alpha}(g_\alpha u^e) - u_\omega\|_{L^1} = 0;$

(ii) $\lim\limits_{\varepsilon \to 0} \mathcal{F}_{-\alpha}(a_\alpha u^e)(t) = u_\omega(t)$ *for a. e. $t \in \mathbb{R}$,*

$\quad \lim\limits_{\varepsilon \to 0} \mathcal{F}_{-\alpha}(g_\alpha u^e)(t) = u_\omega(t)$ *for a. e. $t \in \mathbb{R}$.*

Remark 3.2. From the expressions of the kernel functions in (3.4), it is obvious that the numerical implementation of function $a_\alpha(x)$ is less demanding than that of function $g_\alpha(x)$. So in the following encryption algorithm, we choose the function $a_\alpha(x)$ and use the fractional Abel means to approximate the original signal.

Given an encrypted signal u^e, we can obtain the associated decrypted signal u^d by taking the Abel means of the fractional Fourier integral of u^e with ε small enough. The decryption process may be divided into the following steps according to the diagram of Fig. 3.2:

(i) multiplication by the Abel function $a_\alpha(x)$: $\hat{v}_\varepsilon(x) = u^e(x)a_\alpha(x)$;

(ii) inverse FRFT: $v_\varepsilon(t) = (\mathcal{F}_{-\alpha}\hat{v}_\varepsilon)(t)$;

(iii) action by Q_ω: $u_\varepsilon^d(t) = Q_\omega v_\varepsilon(t) = v_\varepsilon(t)/\omega(t) - M$.

This process can be simply described as

$$
\begin{aligned}
u_\varepsilon^d(t) &= Q_\omega \left[M_{\varepsilon,a_\alpha} u \right](t) \\
&= Q_\omega [\mathcal{F}_{-\alpha}(a_\alpha u^e)](t).
\end{aligned}
\tag{3.5}
$$

Through the aforementioned method, we can restore the encrypted signal $u^e(x)$ from the fractional Fourier domain back to the time domain. Since u is a real-valued signal, the amplitude of the signal u_ε^d can approximate the original signal u as $\varepsilon \to 0$, in view of Theorem 3.3 (as in Fig. 4.2). In other words, for ε sufficiently small, the error between the decrypted signal u_ε^d and the original signal u can be arbitrarily small. Furthermore, accuracy is improved when the parameter ε gets smaller. Replacing $u^e(t)$ by the "Abel average" $u^e(t)a_\alpha(t)$ yields improved smoothness and results in fewer discretization errors.
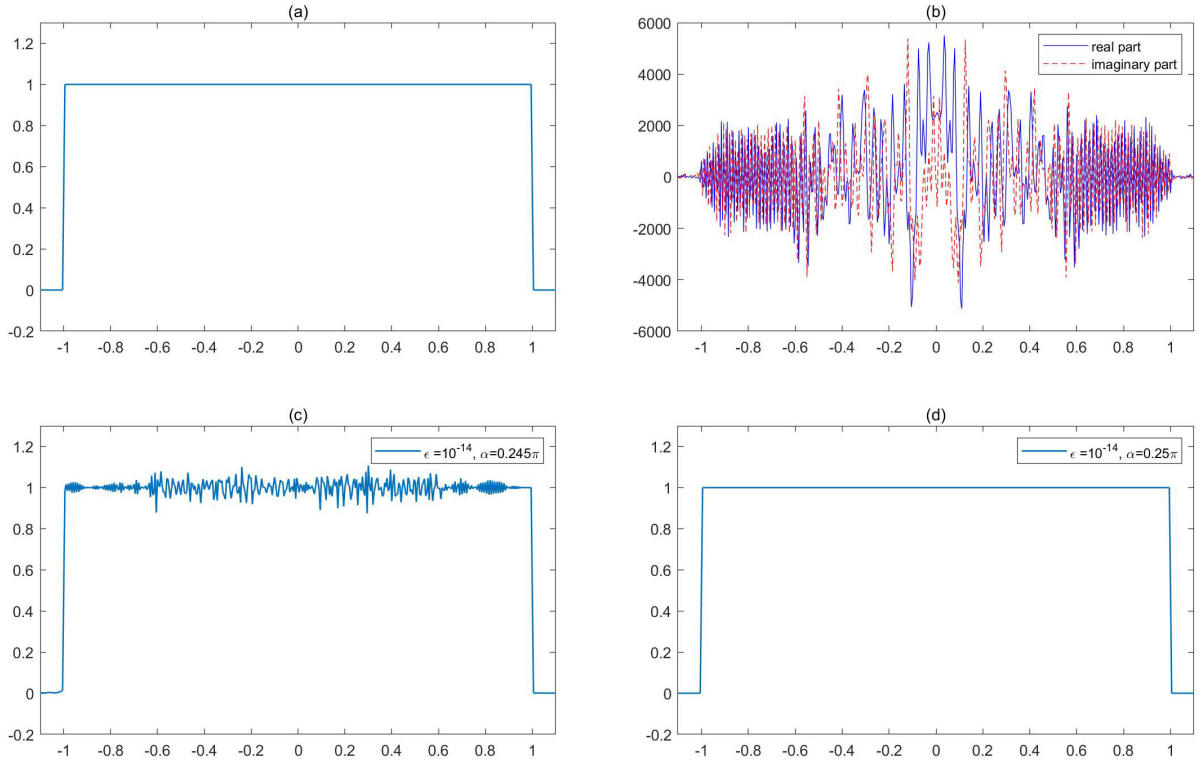
8

Figure 4.1: (a) The original signal sect (t); (b) the real and imaginary part graphs of the encrypted signal $u^e(t)$; the decrypted signal u^d with (c) incorrect key $\alpha = 0.245\pi$ and (d) correct key $\alpha = 0.25\pi$ for $\varepsilon = 10^{-14}$.

4 Simulation examples and applications in audio encrytion

We take a unit rectangular signal $u(t) = \text{rect}(t)$ as an example. Here we randomly select a sequence $\{\tau_i\} \in [-1.1, 1.1]$ and let $\omega(t) = \sum_{i=1}^{n} |t - \tau_i|^{-1/2} \chi_{[-1.1,1.1]}$ as in (3.1). Denote by

$$u_\omega(t) := P_\omega u(t) = \sum_{i=1}^{n} |t - \tau_i|^{-1/2} \text{rect}(t).$$

Then $u_\omega \in L^1(\mathbb{R})$ but $u_\omega \notin L^2(\mathbb{R})$. Take the fractional order $\alpha = \pi/4$ as a secret key. Through the $\pi/4$-th FRFT of u_ω, we get the encrypted signal $u^e = \mathcal{F}_{\pi/4} u_\omega$ (see Fig. 4.1 (b)) in the fractional Fourier domain. Similar to (2.4), we can see that $u^e \notin L^1(\mathbb{R})$ and the inverse FRFT

$$\int_{-\infty}^{+\infty} u^e(x) K_{-\pi/4}(x, t) \mathrm{d}x \tag{4.1}$$

do not make sense.

In order to recover the original signal $u(t)$, we should use the approximating method, that is, take the Abel means of the integral (4.1)

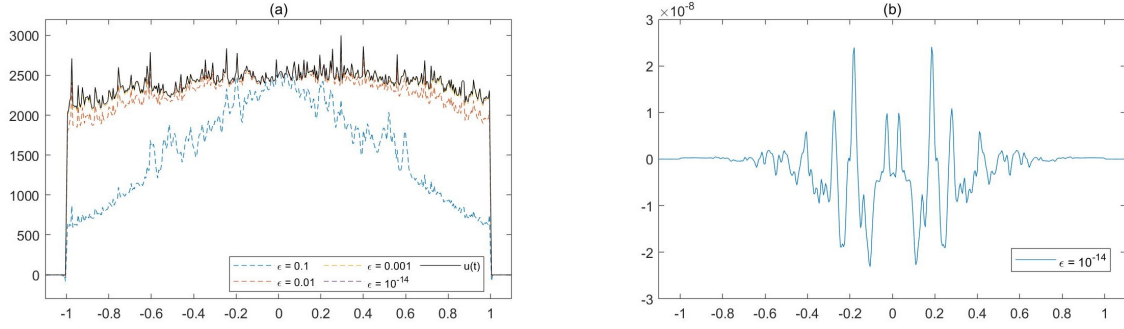$$u_{\varepsilon,\omega}(t) = A_{-\alpha} \int_{-\infty}^{+\infty} u^e(x) K_{-\pi/4}(x, t) a_\alpha(x) \mathrm{d}x. \tag{4.2}$$

9

Figure 4.2: (a) The decrypted signal $u_{\varepsilon,\omega}(t)$ obtained by Abel means with various ε; (b) the error for $\varepsilon = 10^{-14}$.

By Theorem 3.3, we know that $u_{\varepsilon,\omega}(t) \to u_\omega(t)$ for a.e. $t \in \mathbb{R}$ as $\varepsilon \to 0$, as shown in Fig. 4.2 (a). Fig. 4.1 (d) shows the decrypted signal $u^d(t)$ obtaining by take Abel means of the integral (4.1) with $\varepsilon = 10^{-14}$. As shown in Fig. 4.2 (b), the numerical accuracy achieves the order of magnitude of 10^{-8}. In summary, the encryption method proposed in this paper guarantees the security of the encryption process regardless the way of the decryption or the security of secret keys.

Next, we applied the encryption strategy introduced above to encrypt the audio signal. Let's take Beethoven's famous piano music "For Elise" (an 8 seconds clip) as an example. We randomly select a sequence $\{\tau_i\} \in [0, 8]$ and $\alpha = \pi/4$ as the secret keys. Let

$$\omega(t) = \sum_{i=1}^{n} |t - \tau_i|^{-1/2} \chi_{[0,8]}(t)$$

as in (3.1). In the light of the algorithms shown in Fig. 3.1 and Fig. 3.2, we get the encrypted and decrypted audio by using the FRFT algorithm based on FFT (Fast Fourier Transform). The waveform of the encrypted and decrypted audio signal "For Elise" can be found in Fig. 4.3.

5   Connections with Fractional Fourier multipliers

In signal encryption, FRFT is often used in combination with other transforms or operators, as mentioned at the beginning of Section 3.1. Fourier multipliers are operators defined by altering the Fourier transform by multiplication; these play an important role in mathematical analysis and signal processing. The authors' previous work [3] introduced Fourier multipliers in the FRFT context. In this section, we combine these with the encryption algorithm described in Section 3 to a new multiple encryption.

Let $1 \le p \le \infty$ and $m_\alpha \in L^\infty(\mathbb{R})$. Define the operator T_{m_α} as

$$\mathcal{F}_\alpha (T_{m_\alpha} f)(x) = m_\alpha(x)(\mathcal{F}_\alpha f)(x), \ \forall f \in L^2(\mathbb{R}) \cap L^p(\mathbb{R}). \tag{5.1}$$

10

(a) The original audio signal u

(b) The single encrypted audio signal $P_\omega u$

(c) The double encrypted audio signal $\mathcal{F}_{\pi/4} P_\omega u$

(d) The decrypted audio signal with correct key $\alpha = 0.25\pi$

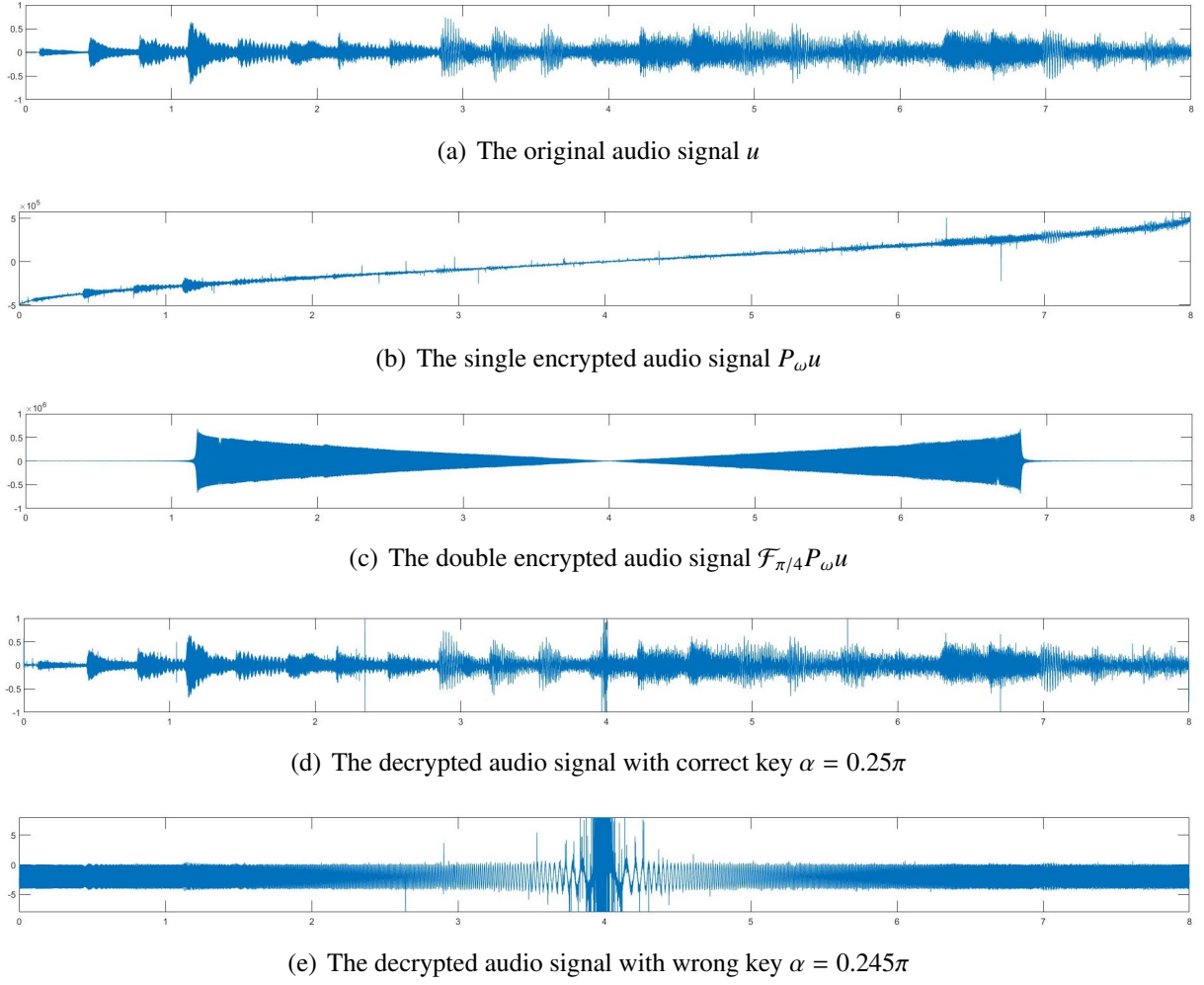(e) The decrypted audio signal with wrong key $\alpha = 0.245\pi$

Figure 4.3: Waveform of the encrypted and decrypted audio signal "For Elise".

The function m_α is called *the L^p Fourier multiplier of order α*, if there exist a constant $C_{p,\alpha} > 0$ such that

$$\left\| T_{m_\alpha} f \right\|_p \leq C_{p,\alpha} \left\| f \right\|_p, \quad \forall f \in L^2(\mathbb{R}) \cap L^p(\mathbb{R}). \tag{5.2}$$

As $L^2(\mathbb{R}) \cap L^p(\mathbb{R})$ is dense in $L^p(\mathbb{R})$, there is a unique bounded extension of T_{m_α} in $L^p(\mathbb{R})$ satisfying (5.2). This extension is also denoted by T_{m_α} and

$$T_{m_\alpha} f = \mathcal{F}_{-\alpha} \left[m_\alpha \left(\mathcal{F}_\alpha f \right) \right].$$

Given an L^2-signal u to be encrypted. Let T_{m_β} be the operator associated with a fractional L^p multipler m_β. Then $T_{m_\beta} u \in L^2(\mathbb{R})$. Next, repeat the encryption process as in Fig. 3.1 for $T_{m_\beta} u$ and we get the encrypted signal u^e. According to the diagram of Fig. 5.1, u^e can be expressed as

$$u^e = \mathcal{F}_\alpha \left[P_\omega \left(T_{m_\beta} u \right) \right].$$

In view of Fig. 3.2, the decryption process is shown in Fig. 5.2 and

$$u_\varepsilon^d = T_{m_\beta}^{-1} \left(Q_\omega M_{\varepsilon, a_\alpha} u^e \right)$$
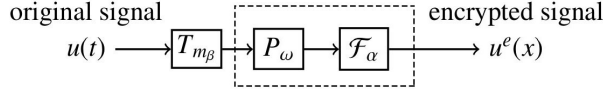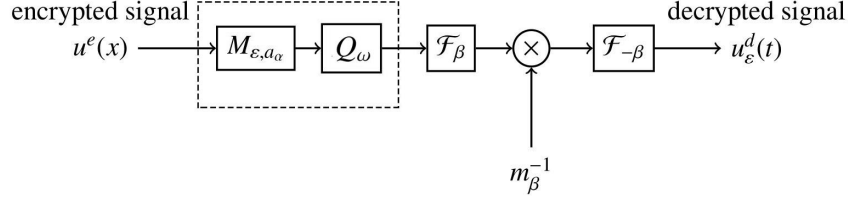
11

Figure 5.1: The process of encryption algorithm

Figure 5.2: The process of decryption algorithm

$$= \mathcal{F}_{-\beta} m_\beta^{-1} \mathcal{F}_\beta \left[Q_\omega \mathcal{F}_{-\alpha} \left(a_\alpha(x) u^e \right) \right].$$

In view of (5.1), many important fractional integral operators can be expressed in terms of fractional L^p multiplier, for example the fractional Hilbert transform. Recall that the classical Hilbert transform is defined as

$$(\mathcal{H}u)(t) = \text{p.v.} \ \frac{1}{\pi} \int_{-\infty}^{+\infty} \frac{u(\tau)}{t - \tau} d\tau. \tag{5.3}$$

The Hilbert transform of order β is defined as (cf., [30])

$$(\mathcal{H}_\beta u)(t) = \text{p.v.} \ \frac{e^{-i\pi t^2 \cot \beta}}{\pi} \int_{-\infty}^{+\infty} \frac{u(\tau) e^{i\pi \tau^2 \cot \beta}}{t - \tau} d\tau. \tag{5.4}$$

For $1 < p < \infty$, the operator $\mathcal{H}_\beta$ is bounded from $L^p(\mathbb{R})$ to $L^p(\mathbb{R})$. By [30, Theorem 4], we see that

$$m_\beta = -i \text{sgn} \left((\pi - \beta) \omega' \right)$$

is a fractional L^p multiplier and the associated operator T_{m_β} is the fractional Hilbert transform, that is,

$$\left(\mathcal{F}_\beta \mathcal{H}_\beta u \right) (\omega') = -i \text{sgn} \left((\pi - \beta) \omega' \right) \left(\mathcal{F}_\beta u \right) (\omega'). \tag{5.5}$$

Without loss of generality, assume that $\beta \in (0, \pi)$. It can be seen from (5.5) that the Hilbert transform of order β is a phase-shift converter that multiplies the positive portion in β-th fractional Fourier domain of signal u by $-i$, that is, maintaining the same amplitude, shifts the phase by $-\pi/2$, while the negative portion of $\mathcal{F}_\beta u$ is shifted by $\pi/2$. As shown in Fig. 5.3.

Take $T_{m_\beta} = \mathcal{H}_\beta$ and ω as in (3.1) as an example. The encryption process shown in Fig. 5.1 can be divided into the following steps:

(i) phase shifting, $u_1 = \mathcal{H}_\beta u$: shifting the phase of positive portion of the original signal u in β-th Fourier domain by $-\pi/2$, while shifting the phase of negative portion of $\mathcal{F}_\beta u$ by $\pi/2$;

(ii) adjusting amplitude, $u_2 = P_\omega u_1$: enlarging the amplitude nearby τ_i, $i = 1, 2, \ldots, n$;
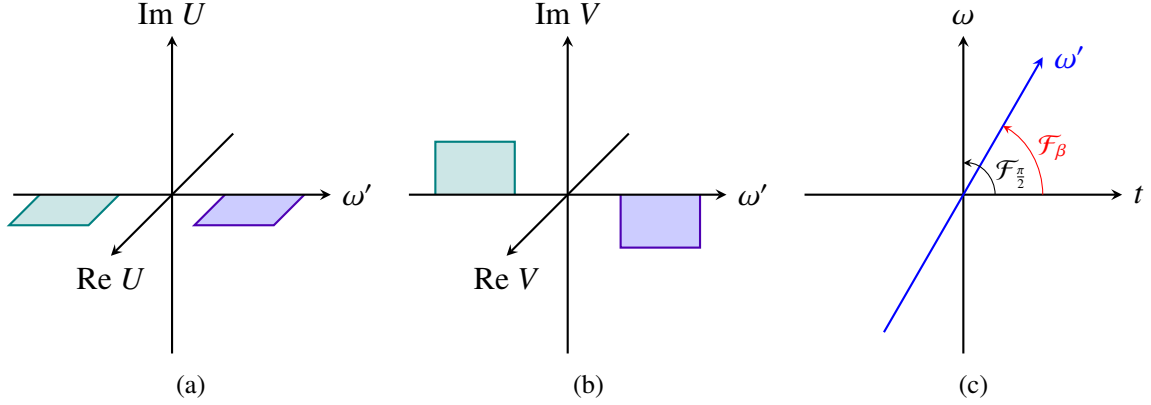
12

Figure 5.3: Phase-shifting effect of the βth-order Hilbert transform ((a) the original signal: $U = (\mathcal{F}_\beta u)(\omega')$; (b) after Hilbert transform of order β: $V = (\mathcal{F}_\beta \mathcal{H}_\beta(u)(\omega')$; (c) rotation of the time-frequency plane).

(iii) rotation of time-frequency plane, $u^e = \mathcal{F}_\alpha u_2$: counterclockwise rotation with an angle of α of signal u_2 from the time axis to x-axis around the origin in the time-frequency plane.

In this way, we triply encrypt the signal. If any one of the keys is erroneous, the original signal cannot be reconstructed. In addition, there are various other options for m_α and T_{m_α}, such as fractional Poisson integral operator, fractional Gauss-Weierstrass integral operator and so on.

6 Conclusion

FRFT is a powerful tool widely used in signal processing. In this work, we elaborated the impact provided by altering the domain of the signals. We pointed out that the FRFT of an L^1-signal is usually noninvertible. Then we provided a double encryption algorithm based on the different properties of FRFT in $L^1(\mathbb{R})$ and $L^2(\mathbb{R})$ spaces. We mapped the to-be-encrypted signal to a "bad" L^1-signal and obtained an encrypted signal by applying the FRFT. Here, the two keys are the function ω and the order α. With the help of Abel and Gauss means of FRFT, we used the idea of identity approximation to recover the encrypted signal from the fractional Fourier domain back to the time domain.

On the one hand, according to the encryption algorithm in this paper, the original signal u is multiplied by the secret function ω, and then the FRFT is performed. It is known from the convolution theorem (see [31]) that

$$\mathcal{F}_\alpha(u\omega)(x) = A_{-\alpha} e^{i\pi x^2 \cot\alpha} \left(U_\alpha * \Omega_\alpha\right)(x),$$

where $U_\alpha(t) = e^{-i\pi t^2 \cot\alpha} \mathcal{F}_\alpha(u)(t)$, $\Omega_\alpha(t) = e^{-i\pi t^2 \cot\alpha} \mathcal{F}_\alpha(\omega e^{-i\pi(\cdot)^2 \cot\alpha})(t)$. Namely, the product of a signal in the time domain becomes a convolution in fractional Fourier domain. Obviously, the convolution operation greatly increases the difficulty for the decipher to separate u from ω. Further, by the Heisenberg's uncertainty principle (see [25] and [26, pp. 158]), it is impossible for a signal to have compact support in both time domain and fractional Fourier domain. A

13

function and its FRFT cannot both be essentially localized. Somewhat more precisely, if the "preponderance" of the mass of a function is concentrated in an interval of finite length, then the preponderance of the mass of its FRFT cannot lie in an interval of finite length. This means that the decipher cannot obtain all the characteristics of the original signal u and the secret function ω from the encrypted signal u^e, which increases the difficulty of deciphering. On the other hand, using the FRFT L^1 theory established in [3], the encryption algorithm in this paper not only further improves security, but also ensures the feasibility and accuracy of decryption. This can be shown in the simulation examples and applications in audio encrytion. Finally we studied the general idea of signal encryption combined with fractional Fourier multipliers, and looked at the fractional Hilbert transform as an example.

For the sake of simplicity, this paper only studied the related problems of one-dimensional signals. In fact, using a similar idea, one may establish the L^1 identity approximation theory of high-dimensional FRFT and apply it to image encryption. The idea in Theorem 3.1, combined with [6, Theorem 1.12], seems to provide a new design of an encryption algorithm even in the case of the classical Fourier transform.

Acknowledgments

References

[1] L. M. Bernardo, O. D. D. Soares, Fractional Fourier transforms and imaging, J. Opt. Soc. Am. A 11 (10) (1994) 2622–2626.

[2] C. Candan, M. A. Kutay, H. M. Ozaktas, The discrete fractional Fourier transform, IEEE Trans. Signal Process. 48 (5) (2000) 1329–1337.

[3] W. Chen, Z. Fu, L. Grafakos, Y. Wu, Fractional Fourier transforms on L^p and applications, Appl. Comput. Harmon. Anal. 55 (2021) 71–96.

[4] L. Chen, D. Zhao, F. Ge, Gray images embedded in a color image and encrypted with FRFT and Region Shift Encoding methods, Opt. Commun. 283 (10) (2010) 2043 – 2049.

[5] I. Djurovic, S. Stankovic, I. Pitas, Digital watermarking in the fractional Fourier transformation domain, J. Netw. Comput. Appl. 24 (2) (2001) 167 – 173.

[6] J. Duoandikoetxea, Fourier analysis, Vol. 29 of Graduate Studies in Mathematics, American Mathematical Society, Providence, RI, 2001.

[7] B. Hennelly, J. T. Sheridan, Optical image encryption by random shifting in fractional Fourier domains, Opt. Lett. 28 (4) (2003) 269–271.

[8] L. Grafakos, Classical Fourier analysis, Graduate Texts in Mathematics, vol. 249, Springer, New York, 3rd ed., 2014.

[9] F. H. Kerr, Namias' fractional Fourier transforms on L^2 and applications to differential equations, J. Math. Anal. Appl. 136 (2) (1988) 404 – 418.

[10] F. H. Kerr, A distributional approach to Namias' fractional Fourier transforms, Proc. Roy. Soc. Edinburgh Sect. A 108 (1988) 133–143.

[11] Z. Liu, S. Liu, Double image encryption based on iterative fractional Fourier transform, Opt. Commun. 275 (2) (2007) 324 – 329.

[12] S. Liu, H. Ren, J. Zhang, X. Zhang, Image-scaling problem in the optical fractional Fourier transform, Appl. Opt. 36 (23) (1997) 5671–5674.

[13] S. Liu, L. Yu, B. Zhu, Optical image encryption by cascaded fractional Fourier transforms with random phase filtering, Opt. Commun. 187 (1) (2001) 57 – 63.

[14] A. W. Lohmann, Image rotation, wigner rotation, and the fractional Fourier transform, J. Opt. Soc. Am. A 10 (10) (1993) 2181–2186.

[15] A. C. McBride, Kerr F. H., On namias's fractional Fourier transforms, IMA J. Appl. Math. 39 (1987) 159–175.

[16] T. Musha, H. Uchida, M. Nagashima, Self-monitoring sonar transducer array with internal accelerometers, IEEE J. Oceanic Eng. 27 (1) (2002) 28–34.

[17] V. Namias, The fractional order Fourier transform and its application to quantum mechanics, IMA J. Appl. Math. 25 (1980) 241–265.

[18] V. A. Narayanan, K. Prabhu, The fractional Fourier transform: theory, implementation and error analysis, Microprocess. Microsy. 27 (10) (2003) 511 – 521.

[19] H. M. Ozaktas, Z. Zalevsky, M. Kutay-Alper, The fractional Fourier transform : with applications in optics and signal processing, Wiley, New York, 2001.

[20] S.-C. Pei, M.-H. Yeh, C.-C. Tseng, Discrete fractional Fourier transform based on orthogonal projections, IEEE Trans. Signal Process. 47 (5) (1999) 1335–1348.

[21] M. G. Raymer, M. Beck, D. McAlister, Complex wave-field reconstruction using phase-space tomography, Phys. Rev. Lett. 72 (1994) 1137–1140.

[22] I. Samil Yetik, A. Nehorai, Beamforming using the fractional Fourier transform, IEEE Trans. Signal Process. 51 (6) (2003) 1663–1668.

[23] B. Santhanam, J. H. McClellan, The discrete rotational Fourier transform, IEEE Trans. Signal Process. 44 (4) (1996) 994–998.

[24] E. Sejdić, I. Djurović, L. Stanković, Fractional Fourier transform as a signal processing tool: An overview of recent developments, Signal Process. 91 (6) (2011) 1351 – 1369.

[25] S. Shinde, V. M. Gadre, An uncertainly principle for real signals in the fractional Fourier transform domain, IEEE Trans. Signal Process. 49 (11) (2001) 2545–2548.

[26] E. M. Stein, R. Shakarchi, Fourier analysis: an introduction, Princeton Univ. Press, Princeton, N.J., 2003.

[27] E. M. Stein, G. Weiss, Introduction to Fourier analysis on Euclidean spaces, Princeton Univ. Press, Princeton, N.J., 1971.

[28] R. Tao, Y. Li, Y. Wang, Short-time fractional Fourier transform and its applications, IEEE Trans. Signal Process. 58 (5) (2010) 2568–2580.

[29] J. M. Vilardy, Y. Torres, M. S. Millán, E. Pérez-Cabré, Generalized formulation of an encryption system based on a joint transform correlator and fractional Fourier transform, J. Opt. 16 (12) (2014) 125405.

[30] A. I. Zayed, Hilbert transform associated with the fractional Fourier transform, IEEE Sig-

nal Process. Lett. 5 (8) (1998) 206–208.

[31] A. I. Zayed, A convolution and product theorem for the fractional Fourier transform, IEEE Signal Process. Lett. 5 (4) (1998) 101–103.

[32] H. Zhao, Z. Zhong, W. Fang, H. Xie, Y. Zhang, M. Shan, Double-image encryption using chaotic maps and nonlinear non-DC joint fractional Fourier transform correlator, Opt. Eng. 55 (9) (2016) 093109.