On the Performance of Diversified Hybrid Carrier System Based on the Extended WFRFT

Ge Song, Xiaojie Fang, and Xuejun Sha(✉)

School of Electronics and Information Engineering,
Harbin Institute of Technology, Harbin 150000, China
shaxuejun@hit.edu.cn

Abstract. In this paper, an extended hybrid carrier system based on extended weighted fractional Fourier transform is proposed to improve the confidentiality of wireless communication. We illustrate the principles and put forward a fast algorithm to ensure the feasibility of the scheme. By extending the existing forms of WFRFT, the proposed scheme achieves a great improvement of the parameter dimensions and constructs diversified anti-interception signals, which significantly reduces the interception probability of eavesdroppers without consuming more physical layer resources or power. The validity of the EWFRFT scheme is verified by theoretical analysis and numerical simulations, and the performance of the system is evaluated in terms of the secrecy capacity, bit error rate, and computational complexity. Simulation results and analysis show that the proposed scheme remedies the defects of the existing hybrid carrier system and safeguards the physical layer security of the system effectively at the cost of a slight increase in computational complexity.

Keywords: WFRFT · Physical layer security · Computational complexity · Hybrid carrier

1 Introduction

With the rapid development of information technology, the demand for security of communication is increasing, and related issues have been widely concerned and studied [1]. The current research is dominated by the information layer encryption system with cryptography as the core, which is mainly based on the encryption and decryption algorithms deployed in the upper layer of the

Supported by the Natural Science Foundation of China under Grant 61901140, supported by China Postdoctoral Science Foundation Funded Project under Grant 2019M650067, supported by Science and Technology on Communication Networks Laboratory under Grant 6142104190203.

Q. Guo et al. (Eds.): WiSATS 2021, LNICST 410, pp. 568–582, 2022.
https://doi.org/10.1007/978-3-030-93398-2_51

protocol stack to meet the requirements of communication confidentiality and authentication. However, due to the insufficient consideration on the physical layer of wireless communication, the existing security schemes still have room for improvement [2,3]. The physical layer security technologies protect the communication signal and the device itself based on some essential characteristics of the physical layer in the wireless transmission of the signal, rather than pursuing the computational security that cryptography relies on [4,5]. Researchers have proposed artificial noise, transmit precoding, cooperative jamming, and the combination of multiple physical layer technologies to enhance the security capacity of the system and ensure the confidentiality of communication, which have achieved rich research result [6–8]. The development of physical layer security systems has made up for the lack of the underlying secrecy performance of traditional cryptography, which has the advantages of good compatibility and saving resources as well as challenges such as power consumption, hardware conditions, and engineering implementation.

In recent years, it is considered a worthy research direction that protecting physical layer waveforms through transform domain signal processing. In particular, the weighted fractional Fourier transform (WFRFT) has been paid more and more attention to the anti-detection and anti-interception of the signal due to its unique four-component superposition structure and beneficial changes to the signal characteristics. [9] introduces WFRFT into the communication system and reveals its physical significance. It points out that the hybrid carrier system based on WFRFT realizes the fusion of single carrier system and multi-carrier system. On this basis, a large number of studies demonstrate that because of the time-frequency backup structure of WFRFT, the hybrid carrier system shows robust anti-channel interference capability in different scenarios [10,11]. On the other hand, the feasibility and advantages of WFRFT in the field of communication security are also valued. By changing the constellation characteristics of the signal through the hybrid carrier modulation, the signal with Gaussian-like distribution can be constructed to realize the concealment of communication signals. Meanwhile, transform parameters can be designed to make the eavesdroppers misjudge the form of the transformation. In addition, the sensitivity of transform parameters can also be utilized to deteriorate the equivalent signal-to-noise ratio of the eavesdropper to reduce the probability of interception. Based on the four-component structure and good security features of WFRFT, a series of secure transmission schemes are proposed and analyzed to cope with the rapid development of targeted interception means by eavesdroppers [12,13]. However, some potential safety hazards have gradually emerged. As the security capability of WFRFT is constrained by the transform parameters and the transformation degree of freedom is limited, the signal is at risk of being cracked. With the extensive research of WFRFT theory, the eavesdroppers gradually master the same prior knowledge of the fraction domain as the partner, which makes the transformation in the form of a single parameter unable to effectively guarantee the security of the system, especially facing eavesdroppers with strong computing capacity.

To cope with the defects of the existing hybrid carrier system, on the one hand, researchers try to combine WFRFT with spread spectrum, antenna array, chaos interference, and other physical layer security technologies to improve the overall secrecy performance of the system [14–16]. On the other hand, there are also some studies on the extension of the transformation form. MP-WFRFT shows the possibility of parameter extension through the construction of coefficient parameter vectors [17]. Furthermore, GWFRFT is proposed in [18], which has more abundant multi-component energy distribution schemes. Compared with WFRFT, GWFRFT can improve the dimension partly due to the relaxation of the boundary conditions, but its research mainly focuses on combating channel fading through parameter design. The potential safety hazards of the existing HC system have not been effectively remedied. Therefore, it is of great research value that extending the WFRFT form to construct diversified anti-intercepted signal forms.

In this paper, we propose a new form of extended weighted fractional Fourier transform and illustrate its advantages in the anti-interception of the signal. The proposed transformation greatly improves the diversity and confidentiality of the signal through extension of the basic operator and the construction of the weighting coefficient vector without consuming more physical resources or power. This paper presents the mathematical principles of the EWFRFT scheme, and a fast implementation process is put forward to simplify the computational complexity of partner communication in ordet to ensure the feasibility of the scheme. Theoretical analysis and simulation verification demonstrates that the proposed scheme can improve the security of the system effectively.

The remainder of this paper is organized as follows: The basic theory of the WFRFT is presented in Sect. 2. The mechanism and implementation process of the proposed EWFRFT scheme are described in detail in Sects. 3, and the improvement of system performance is analyzed. In Sect. 4, the numerical simulations of the proposed scheme are provided. Finally, Sect. 5 concludes this paper.

2 Preliminary

According to [19], the classical weighted fractional Fourier transform can be defined as

$$F^a[x] = \sum_{l=0}^{3} \omega_l(\alpha) F^l x \tag{1}$$

where F is the normalized DFT matrix, whose elements in row m-th and column n-th satisfying as $[F]_{m,n} = \frac{1}{\sqrt{N}} \exp\left[\frac{-2\pi mn}{N} i\right]$. $\omega_l(\alpha), l = 0, 1, 2, 3$ is the weighted coefficient generated by the transform order α, and its calculation method is shown as follows

$$\omega_l(\alpha) = \frac{1}{4} \sum_{k=0}^{3} \exp\left[\frac{2\pi(\alpha - l)k}{4} i\right] \tag{2}$$

The WFRFT operator satisfies periodicity, unitarity, and additivity, as shown in (3)–(5).

$$F^{a+4}[x] = F^{a}[x] \tag{3}$$

$$F^{\alpha}\left[F^{-\alpha}[x]\right] = x \tag{4}$$

$$F^{a+\beta}[x] = F^{a}\left[F^{\beta}[x]\right] \tag{5}$$

MP-WFRFT is an extended form of WFRFT, whose weighting coefficients can be expressed as follows

$$\omega_p^{\alpha,m_k,n_k} = \frac{1}{4}\sum_{k=0}^{3}\exp\left\{\frac{2\pi j}{4}\left[\left(4m_k+1\right)\alpha\left(k+4n_k\right)-pk\right]\right\} \tag{6}$$

where $\{m_k, n_k\} \in Z^+, k = 0, 1, 2, 3$. Further, [18] proposes the GWFRFT with relaxed boundary conditions, and its weighting coefficients can be expressed as

$$\begin{cases} \omega_0^{\theta} = \frac{1}{4}\left(e^{\theta_0 i} + e^{\theta_1 i} + e^{\theta_2 i} + e^{\theta_3 i}\right) \\ \omega_1^{\theta} = \frac{1}{4}\left(e^{\theta_0 i} - e^{\theta_1 i} - e^{\theta_2 i} + e^{\theta_3 i}\right) \\ \omega_2^{\theta} = \frac{1}{4}\left(e^{\theta_0 i} - e^{\theta_1 i} + e^{\theta_2 i} - e^{\theta_3 i}\right) \\ \omega_3^{\theta} = \frac{1}{4}\left(e^{\theta_0 i} + e^{\theta_1 i} - e^{\theta_2 i} - e^{\theta_3 i}\right) \end{cases} \tag{7}$$

where $\theta_k, k = 0, 1, 2, 3$ are the transform parameters of period 2π. Due to $F^0 = \mathrm{I}, F^2 = \Pi$, where I is the unit matrix identity and Π is the shift matrix satisfying $[\Pi]_{m,n} = \delta\left(\langle m+n\rangle_N\right)$ where $\langle\cdot\rangle_N$ denotes modulo-N calculation, these WFRFT forms can be implemented by the FFT module and inversion module, and their computational complexity is slightly increased compared with FFT.

3 System Description

3.1 Extended Weighted Fractional Fourier Transform

Weighted fractional Fourier transform has the feature of dispersing the signal energy into four components in proportion. For eavesdroppers, since the specific dispersing method is unknown, the original signal can be recovered only by parameter scanning. On this basis, an extended weighted fractional Fourier transform (EWFRFT) is proposed. By extending the basic operator and constructing the weighting coefficient vector, the signal energy can be further distributed to more components, which greatly increases the diversity of the transformation and the difficulty of intercepting. The proposed transformation can make up for the defects of the existing hybrid carrier system and effectively improve the physical layer security of the communication system. The EWFRFT scheme can be expressed as follows

$$Y = \sum_{l=0}^{N-1} H_l T^l x \tag{8}$$

x is the original modulation signal, and T is the basic operator matrix with period N. To better realize the purpose of energy dispersion, elements in N are taken to satisfy $[T]_{m,n} = \delta(\langle n-m \rangle_N - 1)$, where $[\cdot]_{m,n}$ represents the m-th row and n-th column elements in the matrix. The diagonal matrix H_l is the weighting coefficient matrix of the transformation. The inverse transformation of with coefficient matrix ${H_l}^{-1}$ can be expressed as $\tilde{x} = \sum_{l=0}^{N-1} {H_l}^{-1} T^l Y = \sum_{(l+p) \bmod N=0}^{N-1} {H_l}^{-1} T^l H_p T^p x + \sum_{(l+p) \bmod N=1}^{N-1} \sum_{l=0}^{N-1} {H_l}^{-1} T^l H_p T^p x$. In order to satisfy the reliability of the partner communication, $\tilde{x} = x$ should be required. Since the basic operator matrix T satisfies $\left[T^l H_p T^p\right]_{m,n} = 0, m \neq n, (l+p) \bmod N = 0, \left[T^l H_p T^p\right]_{m,n} = 0, m = n, (l+p) \bmod N = q$, the transformation should satisfy the following relation.

$$\begin{cases} \sum\limits_{\substack{l=0 \\ (l+p) \bmod N=0}}^{N-1} {H_l}^{-1} T^l H_p T^p = I \\ \sum\limits_{\substack{l=0 \\ (l+p) \bmod N=q}}^{N-1} {H_l}^{-1} T^l H_p T^p = 0_{N \times N}, q = 1, \ldots, N-1 \end{cases} \tag{9}$$

A set of weighting coefficient is presented in (10), which can be obtained through the iterative method as shown in (11).

$$h_n^m = \prod_{k=0}^{\log_2 N - 1} h_{k,n}^m \tag{10}$$

where k is the iteration series, h_n^m is the element in H_l, which can be expressed as $[H_l]_{m,m} = h_n^m, (n-m) \bmod N = l$ or $[H_l]_{n,n} = h_n^m, (m-n) \bmod N = l$, and $h_{k,n}^m$ is the iteration coefficient of order k, which can be obtained as follows

$$h_{k,n}^m = \begin{cases} \frac{1}{2}\left(e^{\theta_{k,0}^{\left[\frac{z_k^m}{2^{k+1}}\right]_i}} + e^{\theta_{k,1}^{\left[\frac{z_k^m}{2^{k+1}}\right]_i}}\right), \left[\frac{z_k^m}{2^k}\right] = \left[\frac{n}{2^k}\right] \\ \frac{1}{2}\left(e^{\theta_{k,0}^{\left[\frac{z_k^m}{2^{k+1}}\right]_i}} - e^{\theta_{k,1}^{\left[\frac{z_k^m}{2^{k+1}}\right]_i}}\right), others \end{cases} \tag{11}$$

where $\theta_{k,0}^t, \theta_{k,1}^t, t = 0, 1, \ldots, \frac{N}{2^{k+1}} - 1$ are the transform parameters and $[\cdot]$ represents rounding down. When $k = \log_2 N - 1$, $z_k^m = m$, and when $k = 0, 1, \ldots, \log_2 N - 2$, z_k^m can be obtained by iteration of the following method.

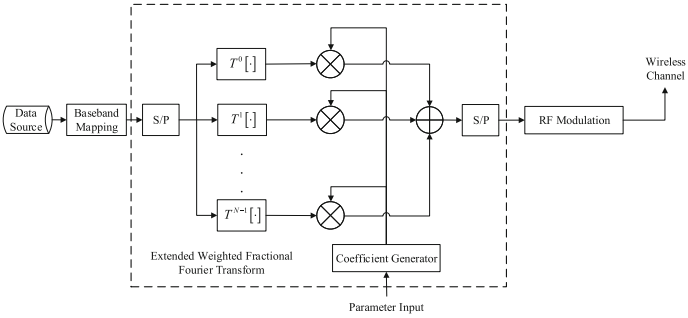
$$z_k^m = \begin{cases} z_{k+1}^m, h_{k+1,n}^m = \frac{1}{2}\left(e^{\theta_{k+1,0}^t i} + e^{\theta_{k+1,1}^t i}\right), t = 0, 1, \ldots, \frac{N}{2^{k+1}} - 1 \\ 2^{k+3}\left[\frac{z_{k+1}^m}{2^{k+2}}\right] + 2^{k+2} - z_{k+1}^m - 1, others \end{cases} \tag{12}$$

In this way, we get the expression of EWFRFT, which is an extension of the existing weighted transformation. Through the design of the weighting

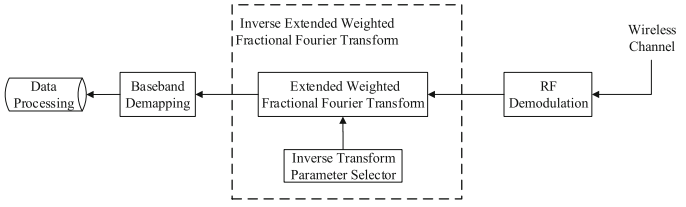
coefficients, the proposed scheme greatly increases the parameter dimension of WFRFT without losing the excellent characteristics of the existing HC signals, which is suitable for the communication system and has the advantage of security. As for eavesdroppers, the probability of accurately judging the form of transformation will be greatly reduced due to the diversity of transformation. To achieve a high probability of signal interception by carrying out the correct inverse transformation, it is necessary to periodically scan all transform parameters on the basis of an accurate judgment of the transformation form, which has to paid unacceptable cost of computational complexity. Therefore, the security of the physical layer waveform is strongly guaranteed.

3.2 System Model

In this section, we propose the EWFRFT-based secure transmission scheme to enhance the confidentiality of communication. The system model is shown in Fig. 1. At the transmitter, EWFRFT is carried out for each code block of the signal. At the receiver, due to the shared transform parameters, the partners can perform a corresponding inverse transformation to recover the signal accurately. While for eavesdroppers, without loss of generality, it is assumed that the mechanism of weighted-type transformation is public, but the specific scheme is unknown. Besides, since we mainly concern the security of the system, the anti-fading process such as equalization is omitted in the block diagram.



(a) The transmitter



(b) The receiver

Fig. 1. The framework of the proposed scheme.

As shown in Fig. 1 - (a), the proposed scheme generates the weighting coefficients according to the transform parameters and utilizes the parallel structure to carry out the weighted summation of the components processed by the periodic operator to obtain the EWFRFT signal. In this case, the computational complexity of EWFRFT can be expressed as $o(N \times N)$, which obviously has room for optimization. To decrease the cost of cooperative communication, we give a fast implementation scheme just like simplifying the calculation of DFT by FFT, which can ensure the feasibility of the proposed scheme. For briefness, it can be expressed in matrix form as follows

$$Y = \mathscr{F}^{\theta}[x] = T[F_k]\, x, k = 0, 1, \ldots, \log_2 N - 1 \tag{13}$$

where $\mathscr{F}^{\theta}$ represents the EWFRFT operator with parameter θ, $F_E = T[F_k]$ is the EWFRFT matrix, which carries out the multiplicative operation on F_k, that is $F_E = F_0 F_1 \ldots F_{N-1}$ or $F_E = F_{N-1} F_{N-2} \ldots F_0$. F_k is the block diagonal matrix of size $N \times N$, where the j-th subblock can be expressed as

$$[F_k]_j = \omega_0^{k,j} I_{2^{k+1}} + \omega_1^{k,j} \Pi_{2^{k+1}}, j = 0, 1, \ldots, \frac{N}{2^{k+1}} - 1 \tag{14}$$

I is the unit matrix identity and Π is the shift matrix, whose elements satisfying $[\Pi]_{m,n} = \delta(\langle n + m + 1 \rangle_N)$, where 2^{k+1} is the size of subblocks. $\omega_0^{k,j}, \omega_1^{k,j}$ is the weighting coefficients expressed as

$$\begin{cases} \omega_0^{k,j} = \frac{1}{2}\left(e^{\theta_{k,0}^j i} + e^{\theta_{k,1}^j i}\right) \\ \omega_1^{k,j} = \frac{1}{2}\left(e^{\theta_{k,0}^j i} - e^{\theta_{k,1}^j i}\right) \end{cases} \tag{15}$$

where $\theta_{k,0}^j, \theta_{k,1}^j$ is the $2N - 2$ transform parameters. At this point, the computational complexity of the system can be expressed as $o(2N \log_2 N)$. By contrast, the fast algorithm greatly reduces the cost of EWFRFT, which makes the proposed scheme feasible.

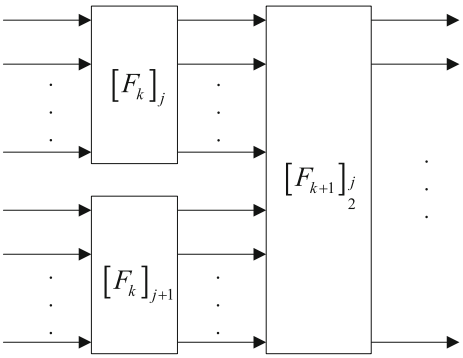


Fig. 2. Basic iterative structure of the EWFRFT fast algorithm.

Figure 2 shows a basic iterative structure schematic diagram of the simplified implementation process, which can be combined step by step to realize the EWFRFT. It is worth noting that due to the unitarity of the iteration function, the EWFRFT simplified algorithm can realize the undistorted recovery of the signal as long as the reverse transformation is carried out step by step in the opposite order to the forward one, thus there are diversified iteration methods. In addition, the iterative function is not unique, but can also be extended to the generalized weighted fractional Fourier transform to further increase the parameter dimension, while its computational complexity will also increase to a certain extent. It can be found that due to the diversity of basic operators, the proposed scheme has strong design flexibility, which is beneficial to resist the eavesdropping of unauthorized receivers. In practical application, it should be reasonably selected according to the system complexity limit and the security requirements to ensure the overall performance of the system.

Next, we describe the structure of the receiver, as shown in Fig. 1 - (b). The inverse transform module can also be implemented in a simplified multi-level iterative process. For the partners, since all parameters are shared, the original signal can be recovered by performing the corresponding inverse transformation shown as follows

$$Y = \mathscr{F}_{-1}^{\theta}[x] = T^{-1}\left[F_k^{-1}\right] x \tag{16}$$

where $T^{-1}[\cdot] = \left(T\left[(\cdot)^T\right]\right)^T$ is the multiplication in the order opposite to the operator $T[\cdot]$, and the k-th inverse transformation matrix F_k^{-1} is the block diagonal matrix, where the j-th subblock can be expressed as

$$\left[F_k^{-1}\right]_j = \frac{1}{2}\left[\left(e^{\left[\theta_{k,0}^j\right]^r i} + e^{\left[\theta_{k,1}^j\right]^r i}\right) I + \left(e^{\left[\theta_{k,0}^j\right]^r i} - e^{\left[\theta_{k,1}^j\right]^r i}\right) \Pi\right] \tag{17}$$

where the inverse transform parameters satisfying $\left[\theta_{k,0}^j\right]^r = -\theta_{k,0}^j$, $\left[\theta_{k,1}^j\right]^r = -\theta_{k,1}^j$. Through the inverse transformation, the original signal can be restored without reduction of the equivalent signal-to-noise ratio, which ensures the reliability of the communication of the partner. Besides, EWFRFT is compatible with the existing communication system and various physical layer security schemes. The proposed scheme has good universality in the field of anti-interception.

3.3 Analysis of Anti-interception Performance

In this section, we will analyze the anti-interception performance of the system in detail. For eavesdroppers, the existence and carrier scheme of the signal need to be accurately detected first. Similar to the HC signal, the EWFRFT has the advantage of changing the signal characteristics. From the point of signal detection, the signal with Gaussian-like distribution can effectively resist the detection. Due to the diversity of EWFRFT, rich transformation can be obtained to make the signal show Gaussian-like statistical property through parameter

designs to realize the hiding or camouflage of the signal. Thus, the signal can not be accurately detected rely on prior knowledge by eavesdroppers, which can effectively make up for the defect caused by the simple change of signal characteristics with the parameter in the existing HC system.

Next, we focus on the receiving performance of eavesdroppers. To reassemble the original signal from the energy dispersed signal, it should accurately judge the signal processing means adopted by the transmitter and select the correct inverse transformation operator to realize the signal reconstruction. When the operator can not be exactly chosen, the eavesdropper will hardly obtain any useful information in high probability. In fact, due to the extension of the transformation form, EWFRFT has the extensibility and design flexibility of the basic operator, which will create obstacles for detecting the signal and ensure the physical layer security of the system. On this basis, the eavesdroppers not only need to master the concrete implementation process of the EWFRFT fast algorithm to realize the inverse transformation of the appropriate complexity but also need to determine all transform parameters. Otherwise, it will lead to a decline in receiving performance. We assume that the eavesdroppers adopt the same fast algorithm as the partners to process the signal, which can be expressed as

$$y = \mathscr{F}_{-1}^{\theta_e}\left[\mathscr{F}^{\theta}[x]\right] = T^{-1}\left[F_k^e\right] T\left[F_k\right] x \tag{18}$$

The inverse transform parameters of the eavesdroppers can be expressed as $\left[\theta_{k,0}^j\right]_e^r = -\theta_{k,0}^j + \sigma_k, \left[\theta_{k,1}^j\right]_e^r = -\theta_{k,1}^j$, since the weighting coefficient of transformation satisfies $\sum_{\substack{0\le u,v\le 1\\ u+v=l}} \omega_u^{k,j}(\theta_p)\omega_v^{k,j}(\tau_p) = \omega_l^{k,j}(\theta_p+\tau_p)$, we can obtain $F_k^e F_k = diag\left(F_{k,0}^e F_{k,0}, F_{k,1}^e F_{k,1}, \ldots, F_{k,\frac{N}{2^{k+1}}-1}^e F_{k,\frac{N}{2^{k+1}}-1}\right) = F_k^{\sigma_k}$. In this case, the received signal can be expressed as

$$Y = T\left[F_k^{\sigma_k}\right] x = F^{\Delta} x \tag{19}$$

where $\Delta = \left[\sigma_0, \sigma_1, \ldots, \sigma_{\log_2 N-1}\right]$ is the error parameter vector, and $F_k^{\sigma_k}$ is the block diagonal matrix satisfying $\left[F_k^{\sigma_k}\right]_q = \frac{1}{2}\left[\left(e^{\sigma_k i}+1\right) I + \left(e^{\sigma_k i}-1\right) \Pi\right]$, $q = 0, 1, \ldots, \frac{N}{2^{k+1}}-1$. It can be seen that due to the existence of parameter errors, the unitarity of EWFRFT is destroyed, which introduces additional signal distortion and decline the receiving performance. At this point, the received signal under the fading channel can be expressed as

$$Y_e = |g_e|^2 F^{\Delta} X + T^{-1}\left[F_k^e\right] g_e^* V^e \tag{20}$$

where g_e is the random channel gains and V^e is the AWGN noise vector with variance σ_e^2. It can be seen that the distortion of the received signal is jointly determined by channel parameters and the error of inverse transform parameters. With the increase of the error, the equivalent signal-to-noise ratio of the eavesdropper decreases rapidly, which harms the receiving reliability. Then, expected secrecy capacity of the proposed system can be expressed as

$$
\begin{aligned}
C_s &= \underset{g_p,g_e}{E}\left[\log_2(1+\eta)-\log_2(1+\eta_e)\right]^+ \\
&= \underset{g_p,g_e}{E}\left[\log_2\left(\frac{\sigma_e^2|g_p|^2P_s+\sigma_s^2\sigma_e^2}{\sigma_s^2|g_e|^2P_s+\sigma_e^2\sigma_s^2}\right)\right. \\
&\left.+\log_2\left(1+\frac{P_s}{\sigma_e^2}|g_e|^2\left(1-\frac{1}{N^3}\sum_{c=0}^{N-1}\left|\prod_{k=0}^{\log_2 N-1}\left(\exp\left(\theta_{k,0}^{\left[\frac{c}{2^{k+1}}\right]}i\right)+1\right)\right|^2\right)\right)\right]^+
\end{aligned}
\tag{21}
$$

where $E[\cdot]$ represents the expectation. $\eta=\frac{|g_p|^2P_s}{\sigma_s^2}$ is the signal-to-noise ratio of the legitimate receiver. While the equivalent SNR of eavesdroppers can be expressed as $\eta_e=\frac{|H_0|^2P_s}{\sum_{e=1}^{N-1}|H_e|^2P_s+\sigma_e^2}$. Since $\frac{1}{4}\left|\sum_{s=0}^{1}\exp\left[\left(\theta_{k,s}^{\left[\frac{c}{2^{k+1}}\right]}\right)i\right]\right|^2\leq 1$, there is $C_s\geq C_0=\underset{g_p,g_e}{E}\left[\log_2\left(1+\frac{|g_p|^2P_s}{\sigma_s^2}\right)-\log_2\left(1+\frac{|g_e|^2P_s}{\sigma_e^2}\right)\right]$. It can be seen that the introduction of EWFRFT provides an additional gain aside from the channel for the enhancement of the secrecy performance, and improve the expected secrecy capacity. On the other hand, the transform parameters with higher dimensions greatly improve the diversity of signals and guarantee the flexibility of the weighted transformation design, which is beneficial to the physical layer waveform anti-interception. The system is easy to obtain better security. For the eavesdroppers, to achieve a better reception effect, the secrecy capacity caused by EWFRFT should be reduced as far as possible to make it meet $C_s\approx C_0$. In this case, the error parameter vector should satisfy

$$
\left[\theta_{k,q}^{j}\right]_e-\left[\theta_{k,q}^{j}\right]_r=\sigma_k\leq\psi_k, j=0,1,\ldots,\tfrac{N}{2^{k+1}}-1, q=0,1 \tag{22}
$$

where $\Psi=\left[\psi_0\ \psi_1\ \ldots\ \psi_{\log_2 N-1}\right]$ is the tolerance of parameter sensitivity, which should be reasonably selected according to communication requirements. To obtain the inverse transformation satisfying the sensitivity tolerance, the eavesdropper can only scan each transform parameter within the period 2π by traversal. In this way, the computational complexity of the eavesdropper can be expressed as

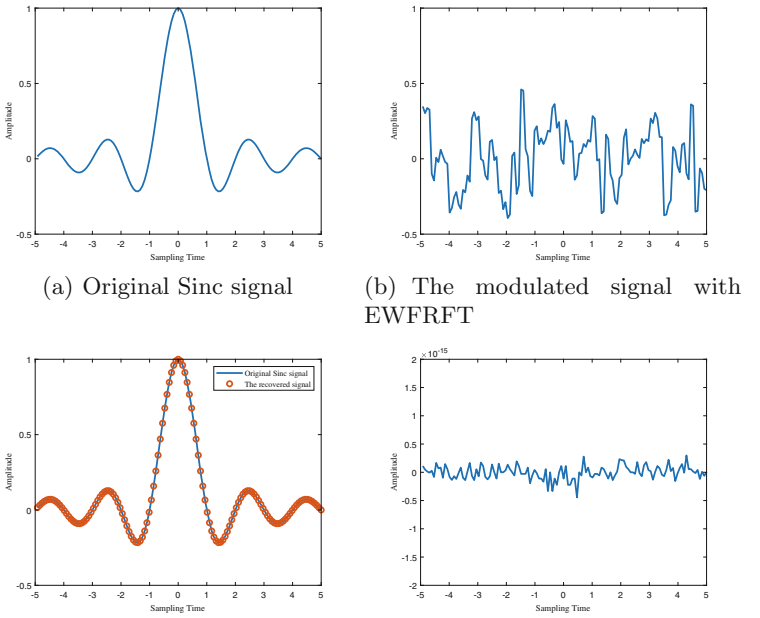
$$
o\left(\prod_{k=0}^{\log_2 N-1}\left(\frac{2\pi}{\psi_k}\right)^{\frac{N}{2^k}}2N\log_2 N\right) \tag{23}
$$

Compared with the computational complexity of the eavesdropper in the WFRFT scheme expressed as $o\left[\frac{4}{\Delta_\alpha}(N\log_2 N+4N)\right]$ and the GWFRFT scheme expressed as $o\left[\left(\frac{2\pi}{\Delta_G}\right)^4(N\log_2 N+4N)\right]$, it can be seen that the EWFRFT scheme greatly increases the cost of eavesdropping due to the extension of the transformation form, which reduces the probability of interception signals through parameter cracking, thus effectively makes up the drawbacks of the existing WFRFT schemes and ensures the anti-interception performance of the

system. In this case, the partner computational complexity of the proposed scheme $o\left(2N\log_2 N\right)$ is slightly higher than that of the existing WFRFT scheme $o\left(N\log_2 N + 4N\right)$ and GWFRFT scheme $o\left(N\log_2 N + 4N\right)$, but still in the same magnitude, which is acceptable without adversely affecting the communication of partners. The EWFRFT scheme gains a great improvement of secrecy performance with a small increase in computational complexity.

4 Simulation Results and Discussion

In this section, the performance of the proposed EWFRFT-based extended hybrid carrier security system will be illustrated through numerical simulations. First, we verify the feasibility of the scheme, as shown in Fig. 3.



(a) Original Sinc signal

(b) The modulated signal with EWFRFT

(c) The recovered signal of the fast algorithm

(d) The error between recovered signal and original signal

Fig. 3. The feasibility of the EWFRFT scheme.

Sinc function is used as the original signal in the simulation as shown in Fig. 3 - (a). First, we perform EWFRFT modulation on the original Sinc signal as (8) with weighting coefficients generated according to (10), and the result is shown in Fig. 3 - (b). At this point, if the transformation can guarantee the unitarity, the original signal can be recovered by the corresponding inverse transformation. The fast algorithm as shown in (13) is adopted to demodulate the

modulated signal, and the result is shown in Fig. 3 - (c). The error between the demodulation result and the original signal is given in Fig. 3 - (d). As can be seen from the simulation results, the undistorted recovery of the EWFRFT modulated signal is realized, which proves the unitarity of EWFRFT and the equivalence of the fast algorithm with the original transform, thus guaranteeing the feasibility of the proposed scheme in anti-interception.

On the premise of verifying its mathematical mechanism, we concern about the anti-detection feature of EWFRFT signals. The degree of Gaussian-like distribution of the signal can be measured by kurtosis $K_X = \frac{E[X-E(X)]^4}{E^2[X-E(X)]^2} - 3$. The simulation results show that there are rich parameter combinations of EWFRFT that can achieve $K_X \approx 0$ regardless of the modulation mode. That is, different from the WFRFT signal with the transform parameter α, due to the extension of parameter dimensions, the proposed scheme has design flexibility and can achieve diversified Gaussian-like distribution, which has advantages in signal hiding and anti-recognition as well as good universality.

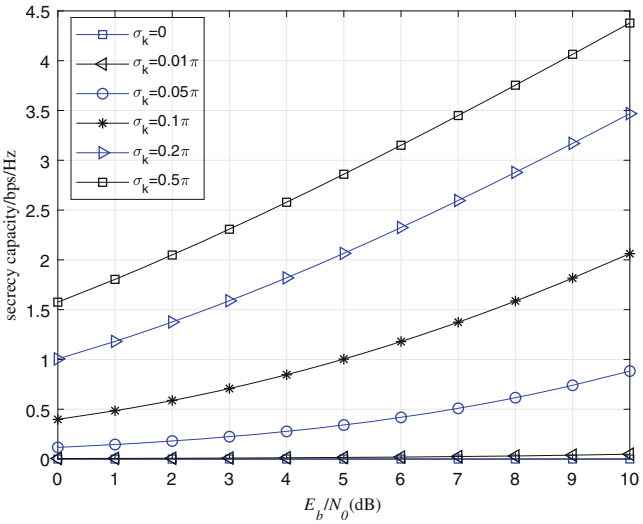


Fig. 4. Secrecy capacity of the proposed scheme.

Then, we analyze the expected secrecy capacity of the system, which is intuitively presented in Fig. 4. It can be seen that, when parameters cannot be correctly selected, the expected secrecy capacity shows a steep growth trend with the increase of SNR as well as that of parameters error, indicating that the system has achieved great secrecy performance. It should be noted that to clearly describe the influence of EWFRFT on the eavesdropper, we assume that the channel conditions of the cooperative receiver and the eavesdropper are the same in the simulation. That is, the expected secrecy capacity of the proposed scheme as shown in the Fig. 4 depends on the energy dispersion and aggregation

process provided by EWFRFT, rather than the superiority or confidentiality of channel gain. On this basis, because of its good compatibility, it is no obstacle to combine the EWFRFT scheme with various traditional physical layer security technologies that can selectively degrade the eavesdropper's channel, which will obtain higher secrecy capacity obviously.

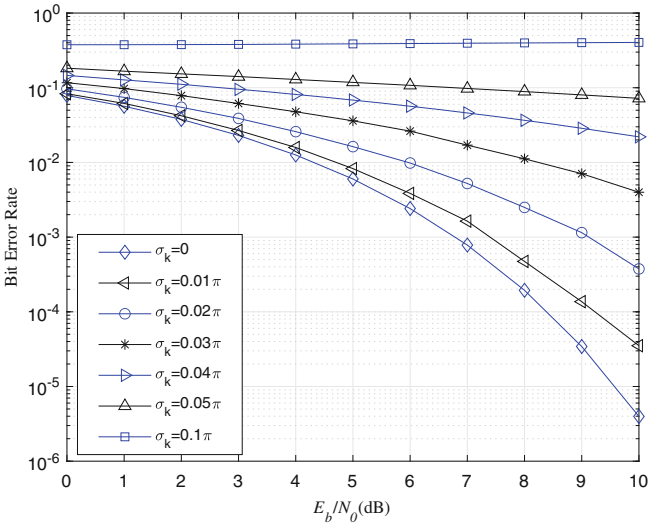


Fig. 5. BER performance of the proposed scheme.

Next, we illustrate the effectiveness of the proposed scheme through the bit error rate. Figure 5 shows the BER curve of the eavesdropper under different parameter errors. QPSK modulation is adopted. We pay attention to the receiving performance in the AWGN channel to show that the signal distortion caused by parameter mismatch reduces the equivalent SNR of the eavesdropper and worsens BER performance, which is the main reason for the improvement of the security. The simulation results show that the increase of σ_k will decrease the BER performance of the eavesdropper. More specifically, under the condition of Eb/N0 = 10 dB, the increase of bit error rate can be clearly observed when $\sigma_k = 0.01$, while BER increases by more than 4 magnitudes when $\sigma_k = 0.05$, which means that the eavesdropper can hardly obtain any useful information compared with the partner. The core advantage of the EWFRFT scheme is that the extension of the transformation greatly increases the dimension of the parameters as well as the cost of interception. According to the tolerance determined by the analysis results of sensitivity, the eavesdroppers have to scan all the transform parameters to obtain the signal. In the communication scenarios with real-time requirements, especially considering more uncertainty brought about by dynamic changes of parameters jointly, it will inevitably lead to the decline

of receiving performance when the eavesdropper cannot pay such a high computational complexity, which effectively guarantees the confidentiality of communication.

In addition, it should be pointed out that in the previous analysis, we assumed that the eavesdroppers master the same knowledge as the partner, as well as accurately select the basic operator of transformation and the iterative scheme of the fast algorithm, but there might be errors in the judgment of parameters. In fact, as an extension of WFRFT, basic operators and parameter generation schemes of EWFRFT have great diversity. The eavesdropper cannot get correct inverse transformation results with the wrong operator even if all parameters are scanned in full cycle, which is the additional security brought by the diversity of EWFRFT. The secrecy performance is effectively improved compared to existing HC systems.

5 Conclusion

This paper focuses on the anti-interception of physical layer waveform in the wireless communication system. To remedy the potential safety hazards of the existing hybrid carrier system, we propose a new EWFRFT scheme and illustrate its superiority. In the proposed scheme, the anti-interception advantages brought by the diversity of EWFRFT signal are fully utilized, and greatly increase the difficulty and cost of intercepting signals for eavesdroppers without affecting the communication of the partner, which effectively guarantees the robust non-zero secrecy capacity. Theoretical analysis and numerical simulations show that, compared with the traditional hybrid carrier system, the proposed scheme can significantly improve the confidentiality of communication with a slight computational complexity increase. Future work will focus on combination with traditional physical layer security schemes to deal with the increasingly sophisticated interception methods of eavesdroppers.

References

1. Cao, J., et al.: A survey on security aspects for 3GPP 5G networks. IEEE Commun. Surv. Tutor. **22**(1), 170–195 (2020)
2. Liang, X., Zhang, K., Shen, X., Lin, X.: Security and privacy in mobile social networks: challenges and solutions. IEEE Wirel. Commun. **21**(1), 33–41 (2014)
3. Choo, K.R., Gritzalis, S., Park, J.H.: Cryptographic solutions for industrial internet-of-things: research challenges and opportunities. IEEE Trans. Ind. Inf. **14**(8), 3567–3569 (2018)
4. Zou, Y., Zhu, J., Wang, X., Hanzo, L.: A survey on wireless security: technical challenges, recent advances, and future trends. Proc. IEEE **104**(9), 1727–1765 (2016)
5. Wang, D., Bai, B., Zhao, W., Han, Z.: A survey of optimization approaches for wireless physical layer security. IEEE Commun. Surv. Tutor. **21**(2), 1878–1911 (2019). Second quarter
6. Jameel, F., Wyne, S., Kaddoum, G., Duong, T.Q.: A comprehensive survey on cooperative relaying and jamming strategies for physical layer security. IEEE Commun. Surv. Tutor. **21**(3), 2734–2771 (2019). thirdquarter

7. Li, L., Hu, Y., Zhang, H., Liang, W., Gao, A.: Deep learning based physical layer security of D2D underlay cellular network. China Commun. **17**(2), 93–106 (2020)
8. Zhang, Y., Shen, Y., Jiang, X., Kasahara, S.: Secure millimeter-wave ad hoc communications using physical layer security. IEEE Trans. Inf. Forensics Secur. 1 (2021)
9. Mei, L., Sha, X., Zhang, N.: The approach to carrier scheme convergence based on 4-weighted fractional Fourier transform. IEEE Commun. Lett. **14**(6), 503–505 (2010)
10. Hui, Y., Li, B., Tong, Z.: 4-weighted fractional Fourier transform over doubly selective channels and optimal order selecting algorithm. Electron. Lett. **51**(2), 177–179 (2015)
11. Wang, Z., Mei, L., Sha, X., Leung, V.C.M.: BER analysis of WFRFT precoded OFDM and GFDM waveforms with an integer time offset. IEEE Trans. Veh. Technol. **67**(10), 9097–9111 (2018)
12. Mei, L., Sha, X., Zhang, N.: Covert communication based on waveform overlay with weighted fractional Fourier transform signals. In: 2010 IEEE International Conference on Wireless Communications, Networking and Information Security, pp. 472–475. Beijing, China (2010)
13. Yuan, L., Xinyu, D., Jialiang, W., Ruiyang, X., Zhe, Z., Hujun, L.: WFRFT modulation recognition based on HOC and optimal order searching algorithm. J. Syst. Eng. Electron. **29**(3), 462–470 (2018)
14. Cheng, Q., Fusco, V., Zhu, J., Wang, S., Wang, F.: WFRFT-aided power-efficient multi-beam directional modulation schemes based on frequency diverse array. IEEE Trans. Wirel. Commun. **18**(11), 5211–5226 (2019)
15. Da, X., et al.: Embedding WFRFT signals Into TDCS for secure communications. IEEE Access **6**, 54938–54951 (2018)
16. Fang, X., Zhang, N., Zhang, S., Chen, D., Sha, X., Shen, X.: On physical layer security: weighted fractional Fourier transform based user cooperation. IEEE Trans. Wirel. Commun. **16**(8), 5498–5510 (2017)
17. Fang, X., Sha, X., Li, Y.: MP-WFRFT and constellation scrambling based physical layer security system. China Commun. **13**(2), 138–145 (2016)
18. Ma, C., Sha, X., Mei, L., Fang, X.: An equal component power-based generalized hybrid carrier system. IEEE Commun. Lett. **23**(2), 378–381 (2019)
19. Shih, C.C.: Fractionalization of Fourier transform. Opt. Commun. **118**, 495–498 (1995)