IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received May 21, 2019, accepted June 3, 2019, date of publication June 5, 2019, date of current version June 20, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2921109

MP-WFRFT and Chaotic Scrambling Aided Directional Modulation Technique for Physical Layer Security Enhancement

FENG LIU[1], LING WANG[1,2], (Member, IEEE), JIAN XIE[1,2], (Member, IEEE), YUEXIAN WANG[1,3], (Member, IEEE), AND ZHAOLIN ZHANG[1]

[1]School of Electronics and Information, Northwestern Polytechnical University, Xi'an 710072, China
[2]Research and Development Institute, Northwestern Polytechnical University, Shenzhen 518057, China
[3]School of Electrical and Electronic Engineering, The University of Adelaide, Adelaide, SA 5005, Australia

Corresponding authors: Ling Wang (lingwang@nwpu.edu.cn) and Jian Xie (xiejian@nwpu.edu.cn)

This work was supported in part by the National Natural Science Foundation of China under Grant 61771404, Grant 61601372, and Grant 61801390, and in part by the Science, Technology and Innovation Commission of Shenzhen Municipality under Grant JCYJ20170306154016149 and Grant JCYJ20170815154325384.

ABSTRACT Directional modulation (DM) technique based on artificial noise (AN) enables the physical layer security (PLS) for wireless communications in free space. However, on one hand, the introduction of AN results in less power efficient for a DM system; on the other hand, the AN-aided DM technique is strongly dependent on the channel state information (CSI) of transceivers, which greatly limits its practical application. What is more, when the eavesdropper (EVE) is slowly approaching the legitimate user (LU) or the EVE and the LU are in the same direction, the transmission security cannot be guaranteed. To circumvent these problems, DM technique with multiple parameters weighted-type fractional Fourier transform (MP-WFRFT) and chaotic scrambling (CS) aided is proposed in this paper to realize the power-efficient and security-enhanced wireless transmissions. Then, the symbol error rate (SER), secrecy rate, robustness, and anti-interception performance of the proposed method are analyzed and simulated. The simulation results are presented to verify that the proposed method is more power-efficient than the traditional AN-aided DM schemes, and the PLS is guaranteed due to the proposed approach, albeit knowing the intended direction for an EVE.

INDEX TERMS Directional modulation (DM), artificial noise (AN), physical layer security (PLS), multiple parameters weighted-type fractional Fourier transform (MP-WFRFT), chaotic scrambling (CS), symbol error rate (SER).

I. INTRODUCTION

Besides connectivity and reliability, security is another significant crux for modern communication systems. For a wired communication system, communicating devices are physically connected through cables. An eavesdropper (Eve) is unable to access the system for illicit activities without direct association. Compared with wired communication systems, the information security has been a critical issue for wireless communication systems due to the broadcast nature of radio propagation. The air interface is open and accessible to all users authorized and unauthorized. The open environment makes confidential information transmissions more vulnerable to malicious attacks, including both the passive eavesdropping for data interception and the active jamming for disrupting legitimate transmissions [1]–[3].

Conventionally, key-based high-layer encryption techniques have been adopted broadly to secure data transmission, regardless whether the communication systems are wired or wireless [4]–[6]. However, these state-of-the-art encryption algorithms, deemed secure enough nowadays, may be insufficient or even not suitable with the development of mobile Internet and intense computational resource availability. Fortunately, keyless physical layer security (PLS) techniques enable the secure transmission by only exploiting the characteristics of wireless channels to avoid spectral

The associate editor coordinating the review of this manuscript and approving it for publication was Huapeng Zhao.

resources and signaling overhead wasted [7]–[9]. Specially, based on the randomness of wireless channels, channel codes were employed to ensure communication security and reliability simultaneously at the physical layer, such as, Wyner codes [8], polar codes [10], low-density parity-check (LDPC) codes [11], and fountain codes [12].

In the last decade, an emerging promising technique named directional modulation (DM), mainly aiming at physical layer security, has attracted extension studies for its unique characteristic. The characteristic is that DM creates desired amplitude and phase in desired direction(s) for each symbol while distorting the symbols in all other directions [3].

Generally speaking, DM is a transmitter side technology, which can be classified into two categories according to the implementation method. One is the optimization method at the radio frequency (RF) frontend (e.g., [13]–[30]). The other is the artificial noise (AN) aided method at the base band in the literatures [31]–[42].

In fact, the initial DM works were achieved by reconfiguring the antenna radiating elements during the transmission. Here, the direction-dependent signal was obtained by altering the effective length and scattering property of a reflector [13]–[15] or by re-routing the excitation currents on radiating structures [16]. Similarly, the excitation weighting updates were performed utilizing attenuators and phase shifters [17]–[20]. Bit error rate (BER) driven DM synthesis methods were demonstrated in [17], [18], [21], [22]. Another types of DM synthesis methods by constraining different properties of array far-field radiation pattern were described in [23], [24]. Besides, wireless transmissions at the RF frontend using antenna subset modulation (ASM) [25], a switched antenna array [26], a linear sparse array (LSA) [27], [28], and a frequency diversity array (FDA) [29], [30] were proposed and further developed. However, the implementation of DM at the RF stage is lack of flexibility, which results in high complexity for the DM signals synthesis. Therefore, the AN-aided DM implementation at the baseband instead of at the RF frontend is emerging at the right moment. The first attempt to link DM systems and AN concepts was presented in [31], which did not elucidate some important aspects related to a DM system design. The authors in [32], [33] further developed AN and orthogonal vector concepts for the single/multi-beam DM synthesis. Then, a robust synthesis method based on AN was put forward in [34] for single-beam scenario, in [35] for multi-beam scenario. Recently, a secure and precise wireless transmission scheme by joint use of AN projection, phase alignment, random subcarrier selection (RSCS) based on orthogonal frequency division multiplexing (OFDM) and DM was proposed for PLS in [36]. Furthermore, the AN-aided methods were also applied into FDA to achieve DM synthesis in [37]–[39].

Obviously, the introduction of AN lowers the power efficiency inevitably. For some power sensitive scenarios, the AN-aided methods may be not suitable. Meanwhile, in an AN-aided DM system, the CSI required for enabling PLS may be imperfect or even unavailable. This has an abominable impact on the design of the beamforming vector and the projection matrix. Above all, all DM works mentioned above have their Achilles' heel when eavesdroppers locate within the information beam-width of the DM system [13]. Thus, this paper is proposed to circumvent these problems by integrating the cryptographic techniques on physical layer for a DM system. Combining cryptographic techniques with DM technique offers another way to improve the security performance significantly. Here, the joint use of multiple cryptographic techniques includes multiple parameters weighted-type fractional Fourier transform (MP-WFRFT) and Chaotic Scrambling (CS).

The fractionalization of Fourier transform was first suggested in 1980 as a novel way to solve the Schröfidinger equation [40]. Then, the concept of WFRFT was brought up by Shih [41]. The definition of MP-WFRFT was given in [42], [43] and it was applied to signal processing. After the WFRFT transform, the distribution of the symbolic energy in the time-frequency domain will be changed, resulting in the rotation and fission of the constellations, thereby it can be applied to the PLS by concealing the signals. In the last decade, the WFRFT technique has been applied to PLS extensively [44]–[51]. An original scheme for covert communication based on waveform overlay with WFRFT signals was proposed in [44]. In [45], 4-WFRFT was applied in hybrid carrier spread spectrum system. In the DFT-based communication systems, the WFRFT operation was used as a precoding scheme to suppress the narrow-band interference (NBI) in [46]. The WFRFT technique and parallel combinatory spreading technology were integrated for secret communications in [47]. A novel transmission scheme based on constellation rotation and WFRFT is proposed to enhance the physical layer security in polarization modulation based dual-polarized satellite communications in [48]. In [49], A novel constellation-splitting criterion in MP-WFRFT modulations was presented for guaranteeing the communication security. The MP-WFRFT technique was also applied into a spatial modulation system for PLS in [50].

Chaotic Scrambling can be viewed as another cryptographic technique at the physical layer. Chaos-based communication has emerged as a promising way to provide data confidentiality due to its high initial condition sensitivity [51]. The transmitted signals are concealed with chaotic sequence, which has a highly unpredictable and random-look nature. The chaotic sequence is sensitive to the parameters' changes and a small variation of any parameter changes the results considerably [52], [53]. Therefore, it can counteract the malicious eavesdroppers efficiently in a DM system.

The amalgamation of WFRFT and DM techniques was proposed to enhance the PLS for the very first time in literature [54]. On the basis of their work, we put forward a practical secure wireless transmission scheme to transmit confidential information to the legitimate user (LU) by the

joint use of multiple techniques including MP-WFRFT, CS, and DM. Totally speaking, the main contributions can be summarized as follows:

(1) The MP-WFRFT technique is introduced into the DM system for the first time. In doing so, the performance of the PLS is significantly enhanced compared with a traditional DM system.

(2) The CS technique is also applied into the DM system for the very first time. The anti-interception performance is remarkably improved compared with a conventional DM system.

(3) The symbol error rate (SER), secrecy rate, robustness and anti-interception performance of the proposed scheme are analyzed, simulated and verified.

The remaining part of this paper is structured as follows. A detailed review of the principle of MP-WFRFT and CS techniques is presented in Section II. The scheme of the directional modulation with the help of WFRFT and CS techniques is proposed in Section III. Then, Section IV provides the analysis of the SER, secrecy rate, robustness, and anti-interception performance of the proposed scheme. Next, Section V gives simulation results and discussions. Finally, Section VI concludes the paper.

Throughout the paper, the following notations will be used: Signs $(\cdot)^{-1}$, $(\cdot)^{+}$, $(\cdot)^{\mathrm{T}}$ and $(\cdot)^{\mathrm{H}}$ designate the inverse, the Moore-Penrose pseudo-inverse, the transpose and the complex conjugate transpose operations of a matrix, respectively; Operator $|\cdot|$ represents modulus; Operator "$\circ$" denotes the Hadamard product; The operations $F_M^{(\alpha,\mathbf{V})}(\cdot)$, $F_M^{(-\alpha,\mathbf{V})}(\cdot)$, $T(\cdot)$, and $T^{-1}(\cdot)$ designate the MP-WFRFT, MP-IWFRFT, DFT, and IDFT; The sign $Q(\cdot)$ denotes the tail distribution function of the standard normal distribution; The notation $\mathbb{E}(\cdot)$ refers to the expectation operation; The notation $[\cdot]^{\diamond}$ means $\max\{0, \cdot\}$; The functions $\mathrm{Im}[\cdot]$ and $\mathrm{Re}[\cdot]$ denote the real and imaginary part of an arithmetical expression, respectively; Notations $\mathbb{Z}$, $\mathbb{R}$, and $\mathbb{C}$ denote the sets of the integer, real, complex numbers; $\mathbf{I}_K$ denotes the identity matrix with size $K \times K$; while $\mathcal{CN}(0, \sigma^2)$ refers to the complex Gaussian distribution with zero mean and variance σ^2.

II. REVIEW OF MP-WFRFT AND CS

A. MP-WFRFT

The MP-WFRFT transforms a sequence of N complex numbers, $X_0(n) := x_0, x_1, \ldots, x_{N-1}$, into another sequence of N complex numbers, $S_0(n) := s_0, s_1, \ldots, s_{N-1}$, which is defined by

$$S_0(n) = F_M^{(\alpha,\mathbf{V})}[X_0(n)] = \sum_{l=0}^{M-1} \omega_l(\alpha, \mathbf{V}) X_l(n), \tag{1}$$

where $\alpha \in \mathbb{R}$ is the transform order, $\mathbf{V} \in \mathbb{Z}^{1\times 2M}$ is the introduced scaling vector. Let $MV = [m_0, m_1, \ldots, m_{M-1}]$, $NV = [n_0, n_1, \ldots, n_{M-1}]$, and we have $\mathbf{V} = [MV, NV]$. $\omega_l(\alpha, \mathbf{V})$, $l \in [0, M-1]$ is the l-th weight coefficient. Here, $X_l(n)$ denotes the l-th times discrete Fourier transform (DFT) of $X_0(n)$.

The definitions of normalized DFT and normalized inverse DFT are given by

$$\begin{aligned} X(k) &= T[x(n)] \\ &= \frac{1}{\sqrt{N}} \sum_{n=0}^{N-1} x(n) e^{-\mathrm{j}2\pi kn/N}, \quad k \in [0, N-1], \end{aligned} \tag{2}$$

and

$$\begin{aligned} x(n) &= T^{-1}[X(k)] \\ &= \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} X(k) e^{\mathrm{j}2\pi kn/N}, \quad n \in [0, N-1], \end{aligned} \tag{3}$$

in several, where N is the interval length of DFT, n and k denote the discrete time and frequency, separately.

Nevertheless, we find that the integer-order DFT is a periodic operation. Repeated the applications of the DFT would bring the sequence back to itself. As we know, there are only four different integer-order DFT functions as follows.

$$\begin{aligned} T^0[x(n)] &= X_0(n), \\ T^1[x(n)] &= X_1(n), \\ T^2[x(n)] &= T^1[X_1(n)] = X_2(n), \\ T^3[x(n)] &= T^1[X_2(n)] = X_3(n). \end{aligned} \tag{4}$$

Therefore, it is reasonable to consider that any MP-WFRFT is a weighted combination of these four functions.

The l-th weight coefficient $\omega_l(\alpha, \mathbf{V})$ is obtained by

$$\omega_l(\alpha, \mathbf{V}) = \frac{1}{M} \sum_{k=0}^{M-1} \exp\{\pm \frac{2\pi \mathrm{j}}{M} [(Mm_k + 1)(k + Mn_k)\alpha - lk]\}. \tag{5}$$

The transform order α has a periodicity of M, i.e.,

$$\omega_l(\alpha, \mathbf{V}) = \omega_l(\alpha + M, \mathbf{V}). \tag{6}$$

Then, substituting Eq. (6) into Eq. (1), we have

$$F_M^{(\alpha,\mathbf{V})}[X_0(n)] = F_M^{(\alpha+M,\mathbf{V})}[X_0(n)]. \tag{7}$$

This is the periodical property of the MP-WFRFT operation.

The MP-WFRFT can be reduced to an ordinary DFT when α is an integer, i.e.,

$$\begin{aligned} F_M^{(0,\mathbf{V})}[X_0(n)] &= X_0(n), \\ F_M^{(1,\mathbf{V})}[X_0(n)] &= T^1[X_0(n)] = X_1(n). \end{aligned} \tag{8}$$

Meanwhile, MP-WFRFT satisfies the additive property, which is given by

$$\begin{aligned} F_M^{(\alpha+\beta,\mathbf{V})}[X_0(n)] &= F_M^{(\alpha,\mathbf{V})}[F_M^{(\beta,\mathbf{V})}[X_0(n)]] \\ &= F_M^{(\beta,\mathbf{V})}[F_M^{(\alpha,\mathbf{V})}[X_0(n)]], \end{aligned} \tag{9}$$

where $\alpha, \beta \in \mathbb{R}$ are two arbitrary real numbers.

Moreover, MP-WFRFT satisfies the linear property, which is given by

$$F_M^{(\alpha,\mathbf{V})}[aX_0(n)+bY_0(n)]=aF_M^{(\alpha,\mathbf{V})}[X_0(n)]+bF_M^{(\alpha,\mathbf{V})}[Y_0(n)], \tag{10}$$

where $X_0(n)$, $Y_0(n) \in \mathbb{C}^{1\times L}$ are two complex sequences, and $a, b \in \mathbb{C}$ are two complex numbers.

The inverse of MP-WFRFT $F_M^{(\alpha,\mathbf{V})}[X_0(n)]$ is defined as $F_M^{(-\alpha,\mathbf{V})}[X_0(n)]$. Therefore, we can easily recover the original sequence $X_0(n)$ from the transformed sequence $S_0(n)$ by doing α order MP-IWFRFT, i.e., $-\alpha$ order MP-WFRFT, as follows

$$F_M^{(-\alpha,\mathbf{V})}[S_0(n)] = \sum_{l=0}^{M-1} \omega_l(-\alpha,\mathbf{V})S_l(n) = X_0(n), \tag{11}$$

where $S_l(n)$ denotes the l-th times DFT of $S_0(n)$, and $S_l(n)$, $l = 0, 1, \ldots, M-1$ is the $\alpha - th$ order MP-WFRFT of $X_l(n)$, $l = 0, 1, \ldots, M-1$, respectively. Unless note otherwise, let $M = 4$ hereinafter.

The proof is seen in Appendix.

Take QPSK (Quadrature Phase Shift Keying) signals for example, the constellations after MP-WFRFT with different transformation parameters $(\alpha, \mathbf{V})$ will occur rotation, diffusion, splitting and confusion as shown in Fig. 1, which is beneficial for physical layer security.

B. CS

The complex dynamic behaviors of chaotic scrambling meet the need for confidentiality. Therefore, CS has been widely used in the field of signal encryption. In this paper, CS is introduced into the DM system to enhance the physical layer security for the first time. As we known, one dimensional Logistic map with the advantages of simple structure and excellent performance makes it one of the most widely used chaotic maps. Thus, we adopt one dimensional Logistic map as chaos model to generate the CS sequence, which is given by [53]

$$x_{n+1} = \mu x_n(1 - x_n), \tag{12}$$

where x_0 is an arbitrary number between zero and one, and x_n represents the nth value iterated by Eq. (12). The parameter μ denotes bifurcation parameter, the values of interest for which are those in the interval (0, 4].

Once the system parameter μ is determinate, for any initial value, the Logistic map can iteratively generate a unique sequence. When μ falls into the interval $(3.569945, 4]$, the sequence will fall into chaos. Slight variations for the initial value x_0 yield dramatically different results over time, which is a prime characteristic of chaos. This characteristic makes it very suitable as an ideal scrambling sequence to enhance physical layer security.

Still take QPSK signals into account, the signals' constellations after the CS operations with different transformation parameters (μ, x_0) will occur random rotation as displayed in Fig. 2, which is beneficial for physical layer security.

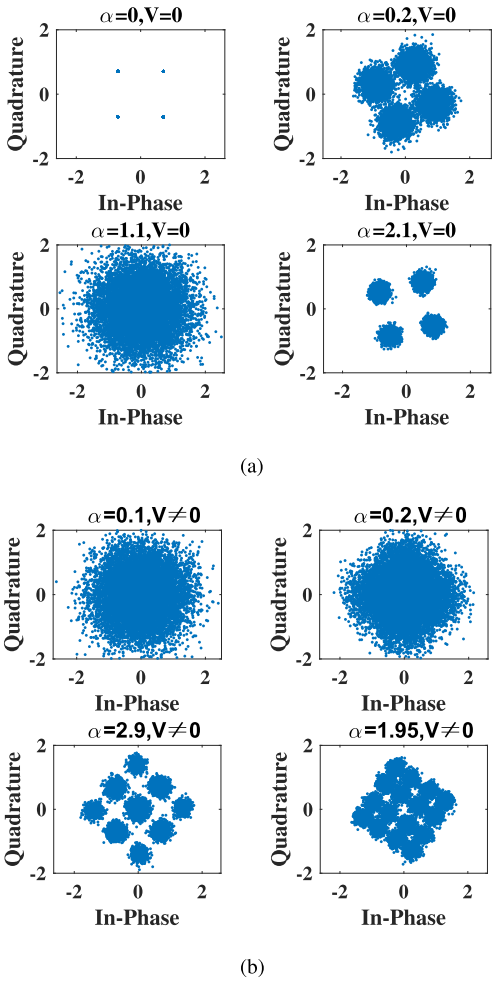

FIGURE 1. The constellations of the QPSK signals after the WFRFT operations with different transformation parameters. (a) $\mathbf{V} = \mathbf{0}$; (b) $\mathbf{V} \neq \mathbf{0}$.

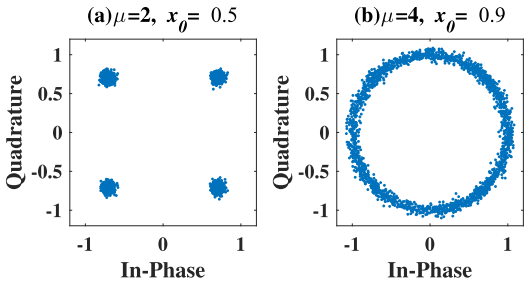

FIGURE 2. The constellations after CS with different parameters. (a) QPSK, (b) CS.

III. SYSTEM MODEL AND PROPOSED DM TECHNIQUE BASED ON MP-WFRFT AND CS

A. SYSTEM MODEL

A multiple-input single-output (MISO) DM system with N transmitting antennas and one single receiving antenna is adopted for a LU or an Eve sketched in Fig. 3. Here, the base station has *a-priori* information about the direction of the LU, but not of the potential Eve. However, the ideas proposed in this paper can also be extended to a multiple-input multiple-output (MIMO) system for multiple LUs or eavesdroppers.

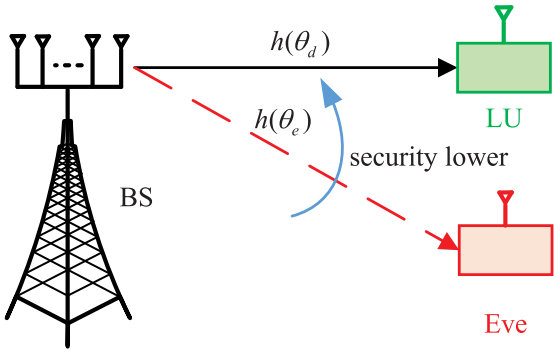

FIGURE 3. A DM System with a LU and an Eve.

A uniform linear array (ULA) equipped with omnidirectional antennas is utilized for the base station (BS), i.e., the DM transmitter. Generally, the maximum interelement spacing is set to half a wavelength of the frequency of interest to avoid spatial aliasing. Our method works for uniform planar arrays and uniform cylindrical arrays, i.e., 2D/3D multidimensional periodic arrays. Owing to the fact that the ULA positioned on the x-y plane cannot resolve pitch angle, the angular location of the receivers is only specified by the azimuth angle.

Without loss of generality, assuming transmitting signals via a narrow-band channel and the receivers located in the far-field region. Let θ_d and θ_e denote the azimuth angle of the LU and the Eve, respectively.

The normalized steering vector for an arbitrary receiver located along the direction θ can be written as

$$\mathbf{h}(\theta) = \frac{1}{\sqrt{N}}[\underbrace{e^{\mathrm{j}2\pi\varphi_\theta(1)}}_{h_1(\theta)}, \ldots, \underbrace{e^{\mathrm{j}2\pi\varphi_\theta(n)}}_{h_n(\theta)}, \ldots, \underbrace{e^{\mathrm{j}2\pi\varphi_\theta(N)}}_{h_N(\theta)}]^{\mathrm{H}}, \quad (13)$$

where $\varphi_\theta(n)$ is given by

$$\varphi_\theta(n) = \frac{(1-n)d\cos\theta}{\lambda} = \frac{(1-n)\cos\theta}{2}, \quad (14)$$

where d denotes the interelement spacing, and $\lambda = c/f_0$ is the free-space wavelength, where c is the speed of light and f_0 is the carrier frequency of interest. For a ULA, $d = \lambda/2$.

B. DM TECHNIQUE BASED ON MP-WFRFT AND CS

The architecture of the base station for the proposed DM scheme based on MP-WFRFT and CS is depicted in Fig. 4. The novel scheme introduces two key-based modules into a conventional DM system simultaneously. One is the MP-WFRFT module with parameters $(\alpha, \mathbf{V})$. The other is the CS module with parameters (μ, x_0). The encryption of the signals is achieved via MP-WFRFT and CS operations, which leads to the rotation, splitting, dispersion and confusion of the constellation of the signals.

For the sake of clarity, in the proposed scheme, the source data consists of modulated symbols, like M-ary PSK, or MQAM (Multiple Quadrature Amplitude Modulation) symbols. Here, the transmitting symbol vector can

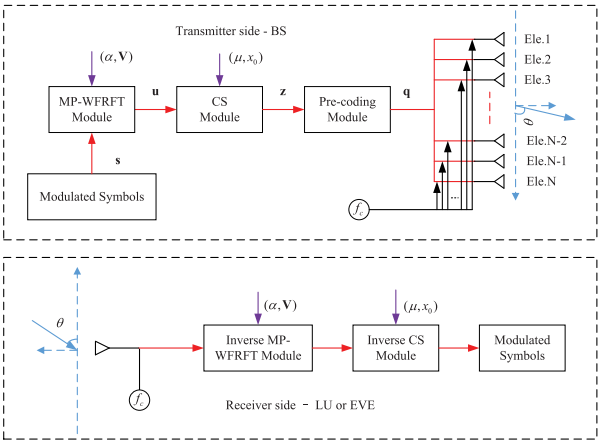

FIGURE 4. The structure of BS and receivers for the MP-WFRFT and CS aided DM scheme.

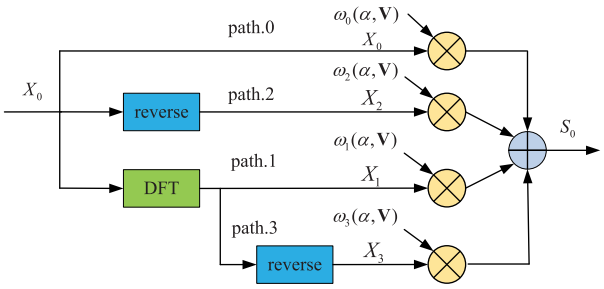

FIGURE 5. The implementation of the MP-WFRFT operation.

be written as

$$\mathbf{s} = [s_1, \ldots, s_m, \ldots, s_L], \quad (15)$$

where s_m denotes the mth symbol, and it satisfies $\mathbb{E}\{s_m^* s_m\} = 1$. Meanwhile, $\mathbf{s}$ can also be viewed as a symbol frame of length L. Firstly, do MP-WFRFT operation with parameters $(\alpha, \mathbf{V})$ on the symbol vector $\mathbf{s}$, which yields

$$\mathbf{u} = F^{(\alpha,\mathbf{V})}[\mathbf{s}] = \sum_{i=0}^{3} \omega_i(\alpha, \mathbf{V})\mathbf{s}_i, \quad (16)$$

where

$$\omega_i(\alpha, \mathbf{V}) = \frac{1}{4}\sum_{k=0}^{3} \exp\{\pm\frac{\mathrm{j}\pi}{2}[(4m_k+1)(k+4n_k)\alpha - ik]\}, \quad (17)$$

and $\mathbf{s}_i$ represents the ith times DFT of the symbol vector $\mathbf{s}$.

The implementation of the MP-WFRFT operation is demonstrated in Fig. 5. According to the basic properties of DFT, the sequence X_0 and X_1 can be reversed to get X_2 and X_3. Therefore, the MP-WFRFT operation needs only one DFT, two sequence inversion, a few multiplication and addition operations in practice. Meanwhile, using Eq. (11), we can easily recover the symbol vector $\mathbf{s}$ by $\mathbf{s} = F^{(-\alpha,\mathbf{V})}[\mathbf{u}]$.

Secondly, before doing CS operation, we need to generate a chaotic sequence $\mathbf{x} = [x_0, x_1, \ldots, x_{L-1}]$ via $L-1$ times iteration by Eq. (12) with the parameters (μ, x_0). Next, the chaotic

scrambling sequence $\mathbf{c}$ can be defined as

$$\mathbf{c} = \exp(\mathrm{j}2\pi\mathbf{x}). \tag{18}$$

Similarly, the chaotic descrambling sequence $\mathbf{c}'$ is given by

$$\mathbf{c}' = \exp(-\mathrm{j}2\pi\mathbf{x}). \tag{19}$$

Then, the CS is operated on the vector $\mathbf{u}$, which yields

$$\mathbf{z} = \mathbf{c} \circ \mathbf{u}. \tag{20}$$

Here, the implementation of the CS operation is displayed in Fig. 6.

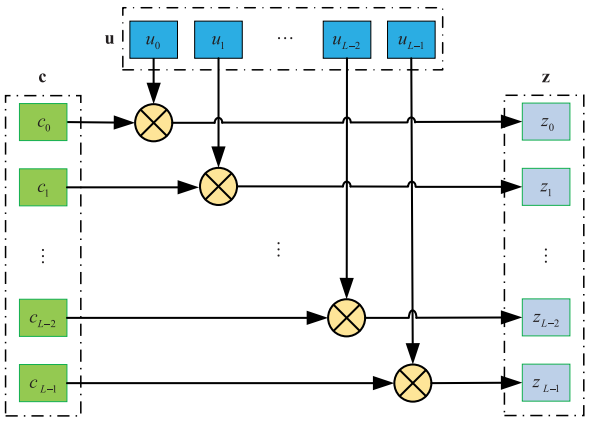

FIGURE 6. The implementation of the CS operation.

Thirdly, in order to match the N antenna elements, the modulated symbol vector should be processed with a pre-coding matrix $\mathbf{P}$. The normalized steering vector of the LU is $\mathbf{h}(\theta_d)$. In order to achieve the DM, the pre-coding matrix $\mathbf{P}$ at the base station side can be given by

$$\mathbf{P} = [\mathbf{h}^{\mathrm{H}}(\theta_d)]^{+} = \mathbf{h}(\theta_d)[\mathbf{h}^{\mathrm{H}}(\theta_d)\mathbf{h}(\theta_d)]^{-1}. \tag{21}$$

Obviously, $\mathbf{h}^{\mathrm{H}}(\theta_d)[\mathbf{h}^{\mathrm{H}}(\theta_d)]^{+} = \mathrm{I}_1$, and

$$\mathbf{h}^{\mathrm{H}}(\theta_d)[\mathbf{h}^{\mathrm{H}}(\theta_d)]^{+}\mathbf{h}^{\mathrm{H}}(\theta_d) = \mathbf{h}^{\mathrm{H}}(\theta_d). \tag{22}$$

After pre-coding, the radiated signal matrix $\mathbf{q} \in \mathbb{C}^{N\times L}$ for N antenna elements for L symbols can be written as

$$\mathbf{q} = \sqrt{P_t}\mathbf{P}\mathbf{z} = \sqrt{P_t}\mathbf{P} \cdot (\exp(\mathrm{j}2\pi\mathbf{x}) \circ F^{(\alpha,\mathbf{V})}[\mathbf{s}]), \tag{23}$$

where P_t is the total transmit power.

Without loss of generality, assuming a narrow-band line-of-sight (LOS) channel with perfect synchronization and symbol-rate sampling, the received signal vector $\mathbf{y} = [y_1, \ldots, y_L]$ along with any direction θ can be written as

$$\mathbf{y}(\theta) = \mathbf{h}^{\mathrm{H}}(\theta)\mathbf{q} + \mathbf{n}, \tag{24}$$

where $\mathbf{n} = [n_1, n_2, \ldots, n_L]$ is the normalized additive white Gaussian noise (AWGN) vector with probability density function (PDF) being $\mathbf{n} \sim \mathcal{CN}(0_{L\times 1}, \sigma_n^2\mathbf{I}_L)$.

Meanwhile, assuming that the private keys of the MP-WFRFT and CS operations are exchanging perfectly for the LU through a secure channel, the eavesdroppers cannot acquire the private parameters. Therefore, for a LU, the received signal vectors are operated by the inverse CS and inverse MP-WFRFT with the known parameters (μ, x_0) and $(-\alpha, \mathbf{V})$, successively, which yields

$$\mathbf{y}^{LU} = F^{(-\alpha,\mathbf{V})}(\mathbf{y}(\theta_d) \circ \mathbf{c}'). \tag{25}$$

Using Eq. (18) to Eq. (24), we expand Eq. (25) as

$$\begin{aligned}\mathbf{y}^{LU} = {} & F^{(-\alpha,\mathbf{V})}[(\mathbf{h}^{\mathrm{H}}(\theta_d)(\sqrt{P_t}[\mathbf{h}^{\mathrm{H}}(\theta_d)]^{+} \\ & \cdot (\exp(\mathrm{j}2\pi\mathbf{x}) \circ F^{(\alpha,\mathbf{V})}[\mathbf{s}])) + \mathbf{n}^{LU}) \circ \exp(-\mathrm{j}2\pi\mathbf{x})],\end{aligned} \tag{26}$$

which along with Eq. (8) to Eq. (10) helps us simplify Eq. (26) as

$$\begin{aligned}\mathbf{y}^{LU} &= \underbrace{\sqrt{P_t}\mathbf{s}}_{\text{information}} + \underbrace{F^{(-\alpha,\mathbf{V})}[\mathbf{n}^{LU} \circ \exp(-\mathrm{j}2\pi\mathbf{x})]}_{\text{noise}} \\ &= \underbrace{\sqrt{P_t}\mathbf{s}}_{\text{information}} + \underbrace{\mathbf{n}'^{LU}}_{\text{noise}}\end{aligned} \tag{27}$$

where $\mathbf{n}^{LU} = [n_1^{LU}, n_2^{LU}, \ldots, n_L^{LU}] \sim \mathcal{CN}(\mathbf{0}_{L\times 1}, \sigma_{n^{LU}}^2\mathbf{I}_L)$ is the AWGN vector for LU; $\mathbf{n}'^{LU} = [n_1'^{LU}, n_2'^{LU}, \ldots, n_L'^{LU}]$ is the noise vector after inverse CS and inverse MP-WFRFT. Because the distribution characteristics of AWGN are not changed by the CS and MP-WFRFT operations [43], we still have $\mathbf{n}'^{LU} \sim \mathcal{CN}(\mathbf{0}_{L\times 1}, \sigma_{n^{LU}}^2\mathbf{I}_L)$.

Therefore, The LU can recover the confidential information $\mathbf{s}$ via Eq. (27) readily.

However, for an Eve located in the direction θ_e, the received signal vector can be given by

$$\mathbf{y}^{EVE} = \mathbf{h}^{\mathrm{H}}(\theta_e)\mathbf{q} + \mathbf{n}^{EVE}. \tag{28}$$

Substituting Eq. (23) into Eq. (28), we have

$$\begin{aligned}\mathbf{y}^{EVE} = {} & \mathbf{h}^{\mathrm{H}}(\theta_e)\sqrt{P_t}[\mathbf{h}^{\mathrm{H}}(\theta_d)]^{+}(\exp(\mathrm{j}2\pi\mathbf{x}) \circ F^{(\alpha,\mathbf{V})}[\mathbf{s}]) + \mathbf{n}^{EVE} \\ = {} & \underbrace{\mathbf{h}^{\mathrm{H}}(\theta_e)\sqrt{P_t}[\mathbf{h}^{\mathrm{H}}(\theta_d)]^{+}(\omega_0(\alpha, \mathbf{V}) \cdot \exp(\mathrm{j}2\pi\mathbf{x}) \circ \mathbf{s})}_{\text{Scrambled information}} \\ & + \underbrace{\mathbf{h}^{\mathrm{H}}(\theta_e)\sqrt{P_t}[\mathbf{h}^{\mathrm{H}}(\theta_d)]^{+}(\exp(\mathrm{j}2\pi\mathbf{x}) \circ \sum_{i=1}^{3}\omega_i(\alpha, \mathbf{V})\mathbf{s}_i)}_{\text{Equivalent AN}} \\ & + \underbrace{\mathbf{n}^{EVE}}_{\text{noise}}.\end{aligned} \tag{29}$$

Here, n^{EVE} is still viewed as the normalized AWGN vector with PDF being $\mathbf{n}^{EVE} \sim \mathcal{CN}(\mathbf{0}_{L\times 1}, \sigma_{n^{EVE}}^2\mathbf{I}_L)$.

It is easy to see that the received signal vector of the Eve consists of three parts. The first part is the scrambled confidential information distorted by the CS and MP-WFRFT operations. The second part is the equivalent AN caused by MP-WFRFT operation mostly. And the third part is the normal AWGN. Even though there is no practical AN inserted in the emitting signal vectors, the operation of MP-WFRFT can introduce equivalent AN into eavesdroppers' receiver, which indicates that the proposed DM scheme is more power-efficient than the traditional AN aided DM system.

On the other hand, the eavesdroppers have no *a-priori* direction information of the LU and the parameters for MP-WFRFT and CS operations, which makes it impossible to recover the confidential information for Eves. What's more, even if the eavesdroppers are located near the LU or even at the same position as the LU, the physical layer security can also be guaranteed for the excellent anti-interception performance of the MP-WFRFT and CS techniques. Therefore, combining cryptographic technologies with a DM system offers a new way to improve the security performance significantly.

In summary, the detailed algorithm process of the DM scheme based on MP-WFRFT and CS is shown in Table 1.

TABLE 1. The algorithm process for the proposed scheme.

Steps	Content
Step 1	For each symbol frame, do MP-WFRFT operation with given parameters $(\alpha, \mathbf{V})$.
Step 2	Generate the CS sequence with fixed parameters (μ, x_0), then do CS operation with the output of step 1.
Step 3	Design the precoding matrix $\mathbf{P}$, and process the output of step 2 with $\mathbf{P}$ to project the symbols to the desired direction.
Step 4	Use a single antenna to receive the symbols, then do inverse MP-WFRFT operation with shared parameters $(\alpha, \mathbf{V})$.
Step 5	Do inverse CS operation with the same CS parameters (μ, x_0) to recover confidential information.

IV. PERFORMANCE ANALYSIS

Symbol error rate, secrecy rate, robustness and anti-interception performance are four key criterions to evaluate the performance of a DM system [3]. Then, the SER, secrecy rate, robustness and anti-interception performance of the proposed scheme are analyzed in this section, hereinafter.

A. SYMBOL ERROR RATE

For the sake of analysis, assume $\sigma^2_{\mathbf{n}^{LU}} = \sigma^2_{\mathbf{n}^{EVE}} = \sigma^2_{\mathbf{n}}$, neglect the path loss, and normalize the baseband symbols. Therefore, the signal-to-noise ratio (SNR) r of the received symbols can be given by

$$r = \frac{P_t}{\sigma^2_{n^{LU}}} = \frac{P_t}{\sigma^2_{n^{EVE}}} = \frac{P_t}{\sigma^2_n}. \tag{30}$$

By comparison, the received SNR of a conventional DM system can be expressed as

$$r^{AN} = \frac{\beta^2 P_t}{\sigma^2_n} = \beta^2 r, \tag{31}$$

where $\beta \in (0, 1]$ is the power allocation coefficient for the confidential information.

In the following paper, only QPSK modulation is taken into account. The theoretical SER of QPSK signals in AWGN channel can be calculated as [55]

$$P_s = 1 - (1 - Q(\sqrt{r}))^2 = 2Q(\sqrt{r}) - Q^2(\sqrt{r}), \tag{32}$$

where $Q(x) = \frac{1}{\sqrt{2\pi}} \int_x^\infty \exp(-\frac{x^2}{2})dx$.

Assuming that the weighting terms, $\mathbf{s}$, $\mathbf{s}_1$, $\mathbf{s}_2$,and $\mathbf{s}_3$ in Eq. (29) have the same average power, i.e., $P_t/4$. For eavesdroppers, the received symbols will be affected because the MP-WFRFT operation would cause the rotation and splitting of the signal in the complex plane. So, let the impact factor be $\cos\theta_{rot}$. Since the energy of the signals before and after the MP-WFRFT operation is conserved, we have

$$\cos\theta_{rot} \cdot \sum_{i=0}^{3} |\omega_i(\alpha, \mathbf{V})|^2 = 1. \tag{33}$$

The useful information is only the weighted term of the original signal $\mathbf{s}$. The average power of the signals received by the eavesdropping receiver is written as

$$P_{\text{WFRFT}} = \frac{P_t}{4} \cdot |\omega_0(\alpha, \mathbf{V})|^2 \cdot \cos^2\theta_{rot}. \tag{34}$$

To simplify Eq. (33), let $\mathbf{V} = \mathbf{0}$, we can rewrite Eq. (33) as

$$P_{\text{WFRFT}} = \frac{P_t}{4} \cdot \cos^2\frac{\alpha\pi}{4}\cos^2\frac{\alpha\pi}{2}\cos^2\frac{3\alpha\pi}{4}. \tag{35}$$

Meanwhile, the signals are scrambled by the sequence $\mathbf{c}$. We spread the sequence $\mathbf{c}$ using Euler's formula as

$$\mathbf{c} = \cos(2\pi\mathbf{x}) + \mathrm{j}\sin(2\pi\mathbf{x}). \tag{36}$$

Then, the average signal energy received by the eavesdropping receiver after the CS operation is equivalent to

$$P_{CS} = \frac{P_t}{4} \cdot \cos^2\frac{\alpha\pi}{4}\cos^2\frac{\alpha\pi}{2}\cos^2\frac{3\alpha\pi}{4}\cos(2\pi\mathbf{x}). \tag{37}$$

At this point, the received SNR r^{EVE} for an Eve is transformed to

$$r^{EVE} = \frac{P_{CS}}{\sigma^2_n}. \tag{38}$$

Therefore, substituting Eq. (30) into Eq. (32), the SER for a LU is derived as

$$P_s{}^{LU} = 2Q(\sqrt{r}) - Q^2(\sqrt{r}). \tag{39}$$

Substituting Eq. (31) into Eq. (32), the SER for a LU aided with AN can be written as

$$P_s{}^{AN} = 2Q(\sqrt{r^{AN}}) - Q^2(\sqrt{r^{AN}}) = 2Q(\beta\sqrt{r}) - Q^2(\beta\sqrt{r}). \tag{40}$$

Substituting Eq. (38) into Eq. (32), the SER for an Eve is expressed as

$$P_s{}^{EVE} = 2Q(\sqrt{r^{EVE}}) - Q^2(\sqrt{r^{EVE}}). \tag{41}$$

It is noted that the SER for a LU aided with AN is affected by the power allocation factor β and for an Eve, it is affected by the parameters $(\alpha, \mathbf{V})$ for MP-WFRFT and the chaotic scrambling sequence $\mathbf{x}$ both.

B. SECRECY RATE

In the light of Eq. (27), the signal-to-interference-plus-noise ratio (SINR) of the LU is given by

$$SINR^{LU} = \frac{P_t}{\sigma_n^2} = r. \tag{42}$$

By dint of Eq. (42), the achievable rate of the link between the BS and the LU can be expressed as

$$\begin{aligned} R^{LU} &= \log_2(1 + SINR^{LU}) \\ &= \log_2(1 + r). \end{aligned} \tag{43}$$

According to Eq. (29) and Eq. (37), the SINR of the Eve is given by

$$SINR^{EVE} = \frac{P_{CS}}{P_t - P_{CS} + \sigma_n^2}. \tag{44}$$

Using Eq. (44), the achievable rate of the link between the BS and the Eve can be obtained by

$$\begin{aligned} R^{EVE} &= \log_2(1 + SINR^{EVE}) \\ &= \log_2(1 + \frac{P_{CS}}{P_t - P_{CS} + \sigma_n^2}). \end{aligned} \tag{45}$$

Thus, the secrecy rate of the proposed DM scheme is defined as

$$R_S = [R^{LU} - R^{EVE}]^{\diamond}. \tag{46}$$

C. ROBUSTNESS

In this part, the robustness of the proposed DM system aided with MP-WFRFT and CS techniques is studied about the imperfect bearing of the LU. Generally, in order to achieve the DM, the base station is assumed to know the direction of the LU. However, in the actual application scenario, whether using GPS positioning or the traditional DOA estimation algorithms, there is a certain angle error in the orientation information. The estimated direction $\widehat{\theta_d}$ of the LU is written as

$$\widehat{\theta_d} = \theta_d + \Delta\theta_d, \tag{47}$$

where θ_d is the estimated angle error.

Then, the corresponding steering vector and pre-coding matrix with estimated errors should be updated to

$$\widehat{\mathbf{P}} = [\mathbf{h}^{\mathrm{H}}(\widehat{\theta_d})]^{+}. \tag{48}$$

where θ_d is the estimated angle error.

Therefore, the normalization characteristic would be affected by the estimated error. Simulations are provided in Section V to analyze the security of the proposed system, which can retain as long as the estimated error within acceptable limits.

D. ANTI-INTERCEPTION PERFORMANCE

In the proposed DM system based on MP-WFRFT and CS, the BS and the LU share the private parameters via a secure channel. The LU can acquire the perfect parameters for inverse MP-WFRFT and inverse CS operations. In a worse scenario, the Eve knows the MP-WFRFT and CS operations and cracks them with imperfect parameters.

Next, we will analyze the impact of the MP-WFRFT and CS operations on constellation. The constellation of the QPSK modulated signals will occur rotation and splitting via MP-WFRFT modulation. The rotation angle can be expressed as

$$\theta_{MP-WFRFT} = \arctan \frac{\mathrm{Im}[\omega_i(\alpha, \mathbf{V})]}{\mathrm{Re}[\omega_i(\alpha, \mathbf{V})]} = \pm\frac{3\pi\alpha i}{4}. \tag{49}$$

It is noted that the rotation angle is only dependent on the transform order α. When the value of α is small, the constellation rotation is not obvious, and the anti-interception performance is not strong enough. Therefore, the CS is introduced after the MP-WFRFT modulation. The phase of the signals will be further rotated after the CS operation. The extra rotation angle can be written as

$$\begin{aligned} \theta_{\mathrm{CS}} &= \arctan \frac{\mathrm{Im}[\mathbf{c}]}{\mathrm{Re}[\mathbf{c}]} \\ &= \arctan \frac{\mathrm{Im}[\exp(\mathrm{j}2\pi\mathbf{x})]}{\mathrm{Re}[\exp(\mathrm{j}2\pi\mathbf{x})]}. \end{aligned} \tag{50}$$

Therefore, the total rotation angle can be derived as

$$\theta_{total} = \theta_{MP-WFRFT} + \theta_{\mathrm{CS}}. \tag{51}$$

Meanwhile, the constellation of the synthesized signal will be diffusion with the variation of parameters. When eavesdroppers do not know the MP-WFRFT and CS operations on the transmitting signals, it is impossible to crack the confidential information. Even if the eavesdrops know the MP-WFRFT and CS operations, it is an extremely hard task for them to scan out the correct parameters. In order to evaluate the anti-interception performance of the proposed DM system, we conduct related simulations through Monte Carlo methods provided in Section V.

TABLE 2. Comparisons for proposed DM, conventional DM and AN-aided DM schemes.

Items	Conventional	AN-aided	Proposed
Computation complexity	$O(LN^2)$	$O(2LN^2)$	$O(LN^2) + O(L)$
Power-efficient	Yes	No	Yes
Neighbor security*	No	No	Yes

* The case where the Eve is within the information beam-width region.

E. COMPARISONS FOR PROPOSED DM, CONVENTIONAL DM AND AN-AIDED DM SCHEMES

Table 2 compares the proposed DM scheme with conventional DM scheme and AN-aided DM scheme, from which the main advantages of the proposed DM scheme can be summarized as follows:

(1) Compared with conventional DM scheme, the computational complexity increases just a bit for the proposed DM scheme. However, compared with AN-aided DM scheme, our method has a lower computation complexity.

(2) Since no AN is inserted in the transmitting signals, the proposed DM scheme is more power-efficient than the AN-aided DM scheme.

(3) Most importantly, beneficiated from the inherent security of the MP-WFRFT and CS techniques, the transmission security of the proposed DM scheme can also be guaranteed even if the Eve's direction is close to or the same as the LU's.

In a word, our proposed DM scheme is more power-efficient and much securer with very little complexity increased.

V. SIMULATION RESULTS AND DISCUSSIONS

In this section, the SER, secrecy rate, robustness and anti-interception performance of the MP-WFRFT and CS Aided DM system are simulated. The main detailed simulation parameters are listed in Table 3.

TABLE 3. Simulation parameters.

Parameters	Value
Number of ULA elements, N	21
Carrier frequency, f_0	10 GHz
Length of the symbol frame, L	128
Total power of the transmit symbol, P_t	1
Desired direction, θ_d	$0°$, $30°$
SNR in the desired direction	12 dB
Power allocation factor, β	0.9, 0.8, 0.7
MP-WFRFT parameters, $(\alpha, \mathbf{V})$	(0.5, [0 6 0 0 0 0 0 6])
CS parameters, (μ, x_0)	(4, 0.9)
Modulation mode	QPSK

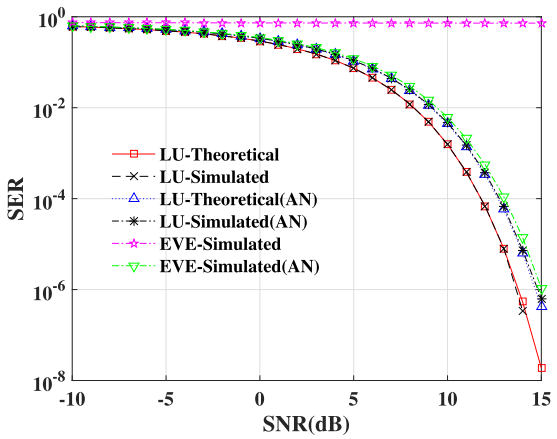

FIGURE 7. SER performances versus SNR in the desired direction.

A. SYMBOL ERROR RATE

Fig. 7 depicts the SER performances of the LU and the Eve located in the desired direction versus SNR for the proposed DM scheme and the traditional AN aided DM system. It is easy to see that 1) the simulation results of the SER are almost identical to the theoretical calculation results; 2) the SNR requested for the proposed scheme is about 1 dB less than that of the AN aided DM scheme when SERs are less than 10^{-2}; 3) when the Eve located within the information beam-width region, the SER is as good as the AN aided DM system, while the proposed DM scheme can prevent eavesdroppers from eavesdropping.

Fig. 8 demonstrates the SER performances versus azimuth for the proposed DM system and the AN aided DM scheme with the same SNR, respectively. As we can see, the

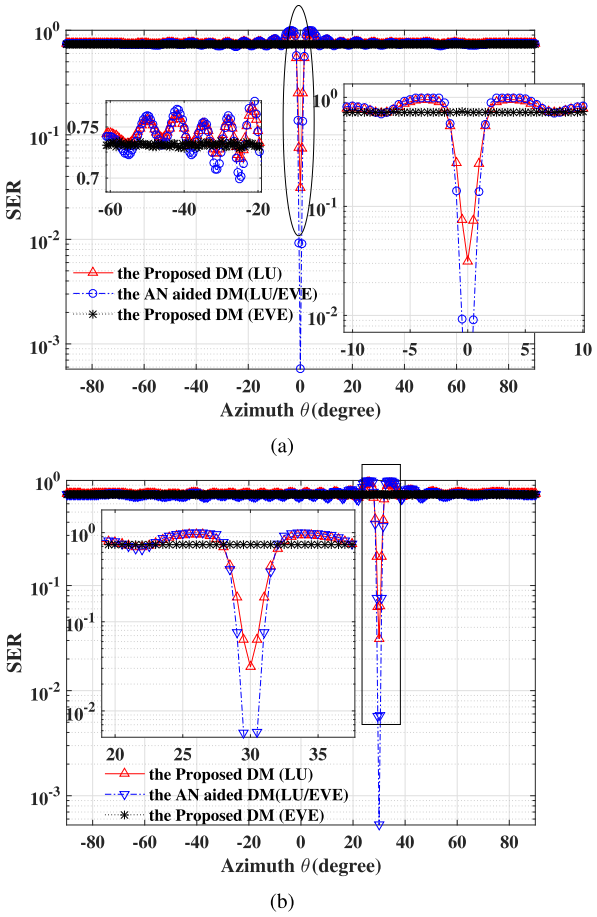

FIGURE 8. SER performances versus azimuth. (a) Broadside; (b) off-broadside.

information beam-width of the proposed DM scheme is much narrower than that of the AN-aided DM system due to the power-efficient. For eavesdroppers, they can crack the confidential information using high sensitive receiver in the AN-aided DM system near the desired direction. However, the security can also be guaranteed in the proposed DM system, no matter where the eavesdropper is or how sensitive the receiver is.

B. SECRECY RATE

Fig. 9 (a) displays the achievable rate of the LU versus SNR for the proposed DM system and the AN-aided system with different power allocation factors. As expected, the achievable rates of the LU for the proposed system are much higher than that of the AN-aided system when the SNR is the same. Meanwhile, the achievable rates are decreasing as the power distribution factor decreases. Fig. 9 (b) depicts the achievable rate of the EVE versus SNR for the proposed DM system. As we can see, the achievable rates of the EVE are approximately 0 bps/Hz with different parameters for MP-WFRFT and CS operations. Fig. 9 (c) demonstrates the secrecy rate for the proposed DM system and the AN-aided system. The simulation results are similar to Fig. 9 (a). Obviously, the secrecy rate of the proposed scheme is higher than

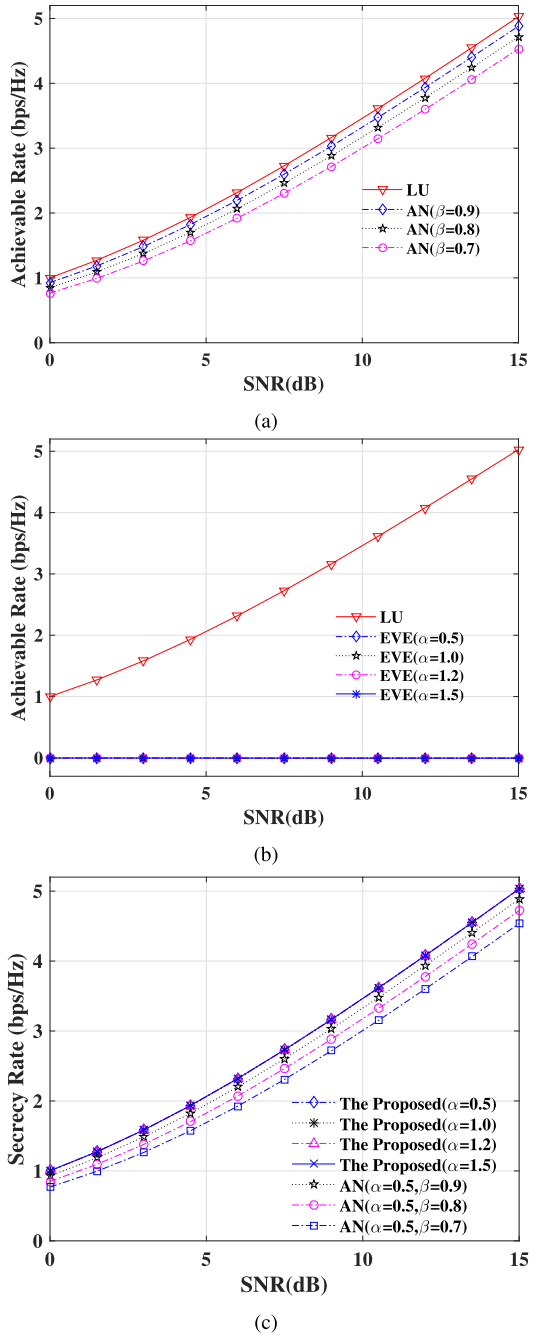

FIGURE 9. Secrecy rate performance versus SNR. (a) Achievable rate for LU; (b) Achievable rate for EVE; (c) Secrecy rate.

that of the AN-aided system. Meanwhile, the secrecy rates are always positive wherever the Eves are located. Compared with the AN-aided scheme, the proposed system is much more secure and reliable.

The SER performance versus SNR with different imperfect estimation errors of the LU's desired direction are displayed in Fig. 10. It is easy to see that for a given SER (e.g., SER $= 10^{-4}$), there is about 1.0 dB loss of the SNR when estimated angle error is $\Delta\theta_d = 2°$. Therefore, as long as the estimated angle errors are less than 2∘, at most 1 dB extra SNR is requested to achieve the same SER as the ideal case.

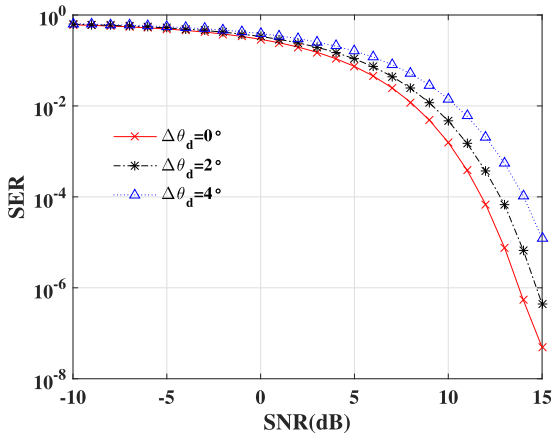

FIGURE 10. Robustness of the proposed DM scheme with different estimation errors of the desired direction.

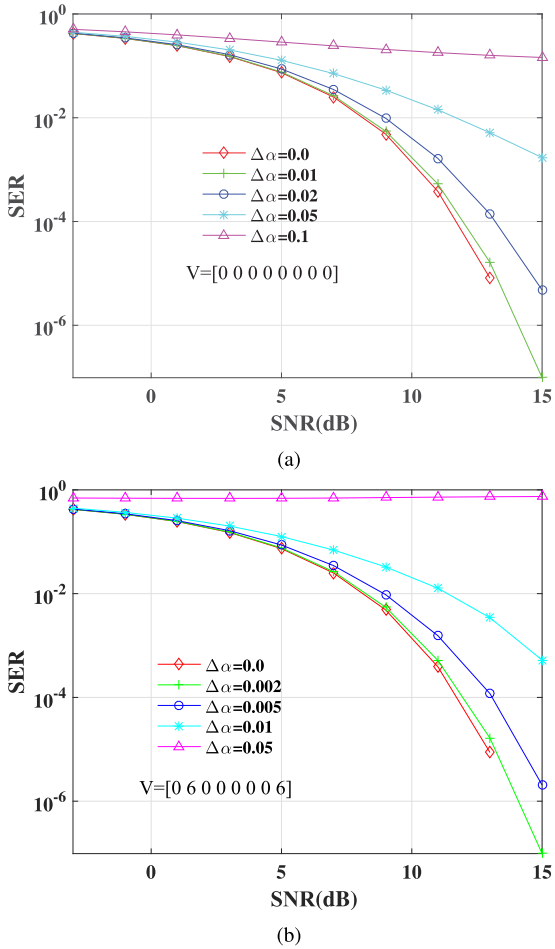

FIGURE 11. The anti-interception performance for the MP-WFRFT operations. (a) V = [0,0, 0, 0, 0, 0, 0, 0]; (b) V = [0, 6,0, 0, 0, 0, 0, 6].

C. ANTI-INTERCEPTION PERFORMANCE

The anti-interception performance of the MP-WFRFT and CS operations is depicted in Fig. 11 and Fig. 12, respectively. As we can see, the SER performance of the proposed DM scheme will worsen much along with a bit mismatched parameters. The eavesdroppers want to recover the relatively

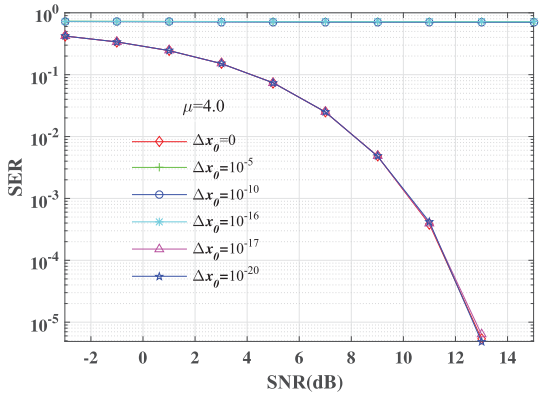

FIGURE 12. The anti-interception performance for the CS operations with different initial values.

accurate confidential information, they should search for the exact parameter α within the error $\Delta\alpha \leq 0.01$, $\mathbf{V} = \mathbf{0}$, $\Delta\alpha \leq 0.002$, $\mathbf{V} \neq \mathbf{0}$, for the MP-WFRFT operation; for the exact parameter x_0 within the error $\Delta x_0 \leq 10^{-17}$, for the CS operation. Especially, owing to the high initial condition sensitivity of the CS operation, the SERs of the proposed DM are always close to 75% when the scanning errors are no less than 10^{-16}. Meanwhile, by contrast, the changing rules of constellations in the proposed DM system are more complicated, and the constellations have good deceptiveness as shown in Fig. 1 and Fig. 2. Therefore, the proposed DM system can achieve physical layer security effectively.

VI. CONCLUSION

With the assistance of the MP-WFRFT and Chaotic Scrambling techniques, a power-effect and effective DM system aided with the MP-WFRFT and the CS operation is proposed for the very first time. The SER, secrecy rate, robustness, and the anti-interception performance are analyzed, simulated and verified, which indicates it has the advantages of power efficiency and the information beam-width security for the proposed scheme compared with the conventional AN aided system. Moreover, it is of considerable interest to extend to the multi-beam DM system.

APPENDIX

In this appendix, the derivation of Eq. (11) will be given. Using the property in Eq. (9), we have

$$\begin{aligned} F_M^{(-\alpha,\mathbf{V})}[S_0(n)] &= F_M^{(-\alpha,\mathbf{V})}[F_M^{(\alpha,\mathbf{V})}[X_0(n)]] \\ &= F_M^{(-\alpha+\alpha,\mathbf{V})}[X_0(n)] \\ &= F_M^{(0,\mathbf{V})}[X_0(n)]. \end{aligned} \tag{52}$$

By inserting Eq. (8) into Eq. (52), we have

$$F_M^{(-\alpha,\mathbf{V})}[S_0(n)] = X_0(n). \tag{53}$$

The DFT can also be expressed as the DFT matrix, a Vandermonde matrix, introduced by Sylvester as follow.

$$X_1(n) = T^1[X_0(n)] = \mathbf{F}X_0, \tag{54}$$

where $\mathbf{F}$ is the transformation matrix, which is given by

$$\mathbf{F} = \frac{1}{\sqrt{N}} \begin{bmatrix} \mathrm{w}_N^{0\cdot 0} & \mathrm{w}_N^{0\cdot 1} & \cdots & \mathrm{w}_N^{0\cdot(N-1)} \\ \mathrm{w}_N^{1\cdot 0} & \mathrm{w}_N^{1\cdot 1} & \cdots & \mathrm{w}_N^{1\cdot(N-1)} \\ \vdots & \vdots & \ddots & \vdots \\ \mathrm{w}_N^{(N-1)\cdot 0} & \mathrm{w}_N^{(N-1)\cdot 1} & \cdots & \mathrm{w}_N^{(N-1)\cdot(N-1)} \end{bmatrix}, \tag{55}$$

where $\mathrm{w}_N = e^{-\mathrm{j}2\pi/N}$. Therefore, we can rewrite Eq. (1) as

$$S_0 = F_M^{(\alpha,\mathbf{V})}[X_0] = \sum_{l=0}^{M-1} \omega_l \mathbf{F}^l X_0. \tag{56}$$

Then, let $\mathbf{S} = [S_0, S_1, \ldots, S_{M-1}]^{\mathrm{T}}$, $\mathbf{X} = [X_0, X_1, \ldots, X_{M-1}]^{\mathrm{T}}$, we have

$$\begin{aligned} \mathbf{S} = \begin{bmatrix} S_0 \\ S_1 \\ \vdots \\ S_{M-1} \end{bmatrix} &= \mathbf{W}\mathbf{X} \begin{bmatrix} \omega_0 & \omega_1 & \cdots & \omega_{M-1} \\ \omega_{M-1} & \omega_0 & \cdots & \omega_{M-2} \\ \vdots & \vdots & \ddots & \vdots \\ \omega_1 & \omega_2 & \cdots & \omega_0 \end{bmatrix} \\ &\times \begin{bmatrix} X_0 \\ X_1 \\ \vdots \\ X_{M-1} \end{bmatrix}. \end{aligned} \tag{57}$$

It is noted that the coefficients matrix $\mathbf{W}$ is a unitary matrix, which satisfies

$$\mathbf{W}^{-1}(\alpha, \mathbf{V}) = \mathbf{W}^{\mathrm{H}}(\alpha, \mathbf{V}) = \mathbf{W}(-\alpha, \mathbf{V}). \tag{58}$$

Because of the inverse property expressed in Eq. (58), X_0 can be obtained by the $-\alpha$ order MP-WFRFT of S_0 easily.

The proof is completed.

ACKNOWLEDGMENT

Feng Liu thanks Dr. Wei Zhang for useful discussions. The help of Fei Xu is appreciated. The authors also would like to thank the anonymous reviewers for their valuable comments and suggestions.

REFERENCES

[1] X. Chen, D. W. K. Ng, W. Gerstacker, and H. H. Chen, "A survey on multiple-antenna techniques for physical layer security," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 2, pp. 1027–1053, 2nd Quart., 2016.
[2] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A survey on wireless security: Technical challenges, recent advances, and future trends," *Proc. IEEE*, vol. 104, no. 9, pp. 1727–1765, Sep. 2016.
[3] Y. Ding and V. Fusco, "A review of directional modulation technology," *Int. J. Microw. Wireless Technol.*, vol. 8, no. 7, pp. 981–993, Nov. 2016.
[4] J. L. Massey, "An introduction to contemporary cryptology," *Proc. IEEE*, vol. 76, no. 5, pp. 533–549, May 1988.
[5] R. A. Mollin, *An Introduction to Cryptography*, 2nd ed. Boca Raton, FL, USA: CRC Press, 2006.
[6] W. Stallings, *Cryptography and Network Security: Priciples and Practice*. Upper Saddle River, NJ, USA: Prentice-Hall, 2003.
[7] C. E. Shannon, "Communication theory of secrecy systems," *Bell Labs Tech. J.*, vol. 28, no. 4, pp. 656–715, Oct. 1949.
[8] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[9] W. Trappe, "The challenges facing physical layer security," *IEEE Commun. Mag.*, vol. 53, no. 6, pp. 16–20, Jun. 2015.
[10] H. Mahdavifar and A. Vardy, "Achieving the secrecy capacity of wiretap channels using polar codes," *IEEE Trans. Inf. Theory*, vol. 57, no. 10, pp. 6428–6443, Oct. 2011.
[11] D. Klinc, J. Ha, S. W. McLaughlin, J. Barros, and B.-J. Kwak, "LDPC codes for the Gaussian wiretap channel," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 532–540, Sep. 2011.
[12] H. Niu, M. Iwai, K. Sezaki, L. Sun, and Q. Du, "Exploiting fountain codes for secure wireless delivery," *IEEE Commun. Lett.*, vol. 18, no. 5, pp. 777–780, May 2014.
[13] A. Babakhani, D. B. Rutledge, and A. Hajimiri, "Transmitter architectures based on near-field direct antenna modulation," *IEEE J. Solid-State Circuits*, vol. 43, no. 12, pp. 2674–2692, Dec. 2008.
[14] A. Babakhani, D. B. Rutledge, and A. Hajimiri, "Near-field direct antenna modulation," *IEEE Microw. Mag.*, vol. 10, no. 1, pp. 36–46, Feb. 2009.
[15] A. H. Chang, A. Babakhani, and A. Hajimiri, "Near-field direct antenna modulation (NFDAM) transmitter at 2.4 GHz," in *Proc. IEEE APSURSI*, Charleston, SC, USA, Jun. 2009, pp. 1–4.
[16] M. P. Daly and J. T. Bernhard, "Beamsteering in pattern reconfigurable arrays using directional modulation," *IEEE Trans. Antennas Propag.*, vol. 58, no. 7, pp. 2259–2265, Jul. 2010.
[17] M. P. Daly and J. T. Bernhard, "Directional modulation technique for phased arrays," *IEEE Trans. Antennas Propag.*, vol. 57, no. 9, pp. 2633–2640, Sep. 2009.
[18] M. P. Daly, E. L. Daly, and J. T. Bernhard, "Demonstration of directional modulation using a phased array," *IEEE Trans. Antennas Propag.*, vol. 58, no. 5, pp. 1545–1550, May 2010.
[19] S. HongZhe and A. Tennant, "Direction dependent antenna modulation using a two element array," in *Proc. IEEE EuCAP*, Rome, Italy, Apr. 2011, pp. 812–815.
[20] H. Z. Shi and A. Tennant, "An experimental two element array configured for directional antenna modulation," in *Proc. IEEE EuCAP*, Prague, Czech Republic, Mar. 2012, pp. 1624–1626.
[21] Y. Ding and V. Fusco, "BER-driven synthesis for directional modulation secured wireless communication," *Int. J. Microw. Wireless Technol.*, vol. 6, no. 2, pp. 139–149, Oct. 2013.
[22] Y. Ding and V. Fusco, "Directional modulation transmitter synthesis using particle swarm optimization," in *Proc. IEEE LAPC*, Loughborough, U.K., Nov. 2013, pp. 500–503.
[23] Y. Ding and V. F. Fusco, "Constraining directional modulation transmitter radiation patterns," *IET Microw., Antennas Propag.*, vol. 8, no. 15, pp. 1408–1415, Dec. 2014.
[24] Y. Ding and V. F. Fusco, "Directional modulation far-field pattern separation synthesis approach," *IET Microw., Antennas Propag.*, vol. 9, no. 1, pp. 41–48, Jan. 2015.
[25] N. Valliappan, A. Lozano, and R. W. Heath, Jr., "Antenna subset modulation for secure millimeter-wave wireless communication," *IEEE Trans. Commun.*, vol. 61, no. 8, pp. 3231–3245, Aug. 2013.
[26] T. Hong, M.-Z. Song, and Y. Liu, "RF directional modulation technique using a switched antenna array for physical layer secure communication applications," *Prog. Electromagn. Res.*, vol. 116, no. 1, pp. 363–379, 2011.
[27] T. Hong, X.-P. Shi, and X.-S. Liang, "Synthesis of sparse linear array for directional modulation via convex optimization," *IEEE Trans. Antennas Propag.*, vol. 66, no. 8, pp. 3959–3972, Aug. 2018.
[28] F. Liu, L. Wang, and J. Xie, "Directional modulation technique for linear sparse arrays," *IEEE Access*, vol. 7, pp. 13230–13240, 2019.
[29] W.-Q. Wang, "DM using FDA antenna for secure transmission," *IET Microw., Antennas Propag.*, vol. 11, no. 3, pp. 336–345, Apr. 2017.
[30] Q. Cheng, J. Zhu, T. Xie, J. Luo, and Z. Xu, "Time-invariant angle-range dependent directional modulation based on time-modulated frequency diverse arrays," *IEEE Access*, vol. 5, pp. 26279–26290, 2017.
[31] O. N. Alrabadi and G. F. Pedersen, "Directional space-time modulation: A novel approach for secured wireless communication," in *Proc. IEEE ICC*, Ottawa, ON, Canada, Jun. 2012, pp. 3554–3558.
[32] Y. Ding and V. F. Fusco, "A vector approach for the analysis and synthesis of directional modulation transmitters," *IEEE Trans. Antennas Propag.*, vol. 62, no. 1, pp. 361–370, Jan. 2014.
[33] Y. Ding and V. Fusco, "Orthogonal vector approach for synthesis of multi-beam directional modulation transmitters," *IEEE Antennas Wireless Propag. Lett.*, vol. 14, pp. 1330–1333, 2015.
[34] J. S. Hu, F. Shu, and J. Li, "Robust synthesis method for secure directional modulation with imperfect direction angle," *IEEE Commun. Lett.*, vol. 20, no. 6, pp. 1084–1087, Jun. 2016.
[35] F. Shu, X. Wu, J. Li, R. Chen, and B. Vucetic, "Robust synthesis scheme for secure multi-beam directional modulation in broadcasting systems," *IEEE Access*, vol. 4, pp. 6614–6623, 2016.
[36] F. Shu, X. Wu, J. Hu, J. Li, R. Chen, and J. Wang, "Secure and precise wireless transmission for random-subcarrier-selection-based directional modulation transmit antenna array," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 4, pp. 890–904, Apr. 2018.
[37] J. Hu, S. Yan, F. Shu, J. Wang, J. Li, and Y. Zhang, "Artificial-noise-aided secure transmission with directional modulation based on random frequency diverse arrays," *IEEE Access*, vol. 5, pp. 1658–1667, 2017.
[38] B. Qiu, J. Xie, L. Wang, and Y. Wang, "Artificial-noise-aided secure transmission for proximal legitimate user and eavesdropper based on frequency diverse arrays," *IEEE Access*, vol. 6, pp. 52531–52543, 2018.
[39] S. Ji, W.-Q. Wang, H. Chen, and Z. Zheng, "Secrecy capacity analysis of AN-aided FDA communication over Nakagami-*m* fading," *IEEE Wireless Commun. Lett.*, vol. 7, no. 6, pp. 1034–1037, Dec. 2018.
[40] V. Namias, "The fractional order Fourier transform and its application to quantum mechanics," *IMA J. Appl. Math.*, vol. 25, no. 3, pp. 241–265, 1980.
[41] C.-C. Shih, "Fractionalization of Fourier transform," *Opt. Commun.*, vol. 118, nos. 5–6, pp. 495–498, Aug. 1995.
[42] J. Lang, R. Tao, Q. Ran, and Y. Wang, "The multiple-parameter fractional Fourier transform," *Sci. In China Ser. F-Inf. Sci.*, vol. 51, no. 8, pp. 1010–1024, Aug. 2008.
[43] L. Mei, X. Sha, Q. Ran, and N. Zhang, "Research on the application of 4-weighted fractional Fourier transform in communication system," *Sci. China Inf. Sci.*, vol. 53, no. 6, pp. 1251–1260, Jun. 2010.
[44] L. Mei, X. Sha, and N. Zhang, "Covert communication based on waveform overlay with weighted fractional Fourier transform signals," in *Proc. IEEE ICWC*, Beijing, China, Jun. 2010, pp. 472–475.
[45] X. Qiu, X. Sha, and M. Lin, "Hybrid carrier spread spectrum system based on 4-weighted fractional Fourier transform," *China Commun.*, vol. 9, no. 1, pp. 13–19, Jan. 2012.
[46] L. Mei, Q. Zhang, X. Sha, and N. Zhang, "WFRFT precoding for narrowband interference suppression in DFT-based block transmission systems," *IEEE Commun. Lett.*, vol. 17, no. 10, pp. 1916–1919, Oct. 2013.
[47] X. Fang, X. Sha, and Y. Li, "Secret communication using parallel combinatory spreading WFRFT," *IEEE Commun. Lett.*, vol. 19, no. 1, pp. 62–65, Jan. 2015.
[48] Z. Luo, H. Wang, K. Zhou, and W. Lv, "Combined constellation rotation with weighted FRFT for secure transmission in polarization modulation based dual-polarized satellite communications," *IEEE Access*, vol. 5, pp. 27061–27073, 2017.
[49] Y. Liang, X. Da, R. Xu, L. Ni, D. Zhai, and Y. Pan, "Research on constellation-splitting criterion in multiple parameters WFRFT modulations," *IEEE Access*, vol. 6, pp. 34354–34364, 2018.
[50] Q. Cheng, J. Zhu, and J. Luo, "Secure spatial modulation based on dynamic multi-parameter WFRFT," *IEICE Trans. Commun.*, vol. E101.B, no. 11, pp. 2304–2312, May 2018.
[51] M. C. Soriano, P. Colet, and C. R. Mirasso, "Security implications of open- and closed-loop receivers in all-optical chaos-based communications," *IEEE Photon. Technol. Lett.*, vol. 21, no. 7, pp. 426–428, Apr. 1, 2009.
[52] L. Zhang, X. Xin, B. Liu, and Y. Wang, "Secure OFDM-PON based on chaos scrambling," *IEEE Photon. Technol. Lett.*, vol. 23, no. 14, pp. 998–1000, Jul. 15, 2011.
[53] S.-L. Chen, T. T. Hwang, and W.-W. Lin, "Randomness enhancement using digitalized modified logistic map," *IEEE Trans. Circuits Syst., II, Exp. Briefs*, vol. 57, no. 12, pp. 996–1000, Dec. 2010.
[54] F. Liu, L. Wang, and J. Xie, "Directional modulation via weighted fractional Fourier transform—A way to enhance security," in *Proc. IEEE EuCAP*, London, U.K., Apr. 2018, pp. 1–4.
[55] S. Stein and J. J. Jones, *Modern Communication Principle With Application to Digital Signaling*. New York, NY, USA: McGraw-Hill, 1967.