DOI: 10.11918/202011077

基于二维加权分数傅里叶变换的安全传输方法

黄永新[1,2],房宵杰[1,2],沙学军[1]

(1. 哈尔滨工业大学 通信技术研究所,哈尔滨 150001;2. 通信网信息传输与分发技术重点实验室,石家庄 050081)

摘 要: 从无线通信系统的安全性角度出发,为了进一步提升传统加权分数傅里叶(weighted fractional Fourier transform, WFRFT)的抗截获性能,引入二维加权分数傅里叶变换(two-dimensional weighted fractional Fourier transform, 2DWFRFT)。2DWFRFT 在原有一维变换基础上,其核心算法通过进行多次不同参数的横纵维度变换以进一步提升单参数加权分数傅里叶变换的抗扫描特性。本文给出了信号的生成方法,推导出特定情况下的矩阵表达式,并详细阐述了本方案的实现计算复杂度以及星座旋转特征优势。理论分析方面,为了充分说明本方案的抗截获性能,从物理层安全信息理论角度分析了 MISO 窃听信道模型下的遍历安全容量。仿真结果表明:相比于单参数一维加权分数傅立叶变换,2DWFRFT 变换阶数由多个参数向量组成,仅以有限的计算复杂度为代价便可获得抗截获性能的有效提升,同时在星座混淆方面可突破原点数限制,提供更加丰富的星座变换特征。相比于传统物理层安全领域中的人工噪声方法,本文方案具有安全容量高、无需额外消耗噪声信号功率等优势。

关键词: 物理层安全;一维加权分数傅里叶变换;二维加权分数傅里叶变换;星座旋转;抗截获;遍历安全容量

中图分类号: TN918.91 **文献标志码:** A **文章编号:** 0367-6234(2022)05-0011-07

A secure transmission method based on two-dimensional weighted fractional Fourier transform

HUANG Yongxin[1,2], FANG Xiaojie[1,2], SHA Xuejun[1]

(1. Communication Research Center, Harbin Institute of Technology, Harbin 150001, China;
2. Science and Technology on Communication Networks Laboratory, Shijiazhuang 050081, China)

Abstract: To further enhance the anti-interception performance of traditional weighted fractional Fourier transform (WFRFT) from the perspective of security of wireless communication system, the two-dimensional weighted fractional Fourier transform (2DWFRFT) was introduced. Based on the original one-dimensional transform, the kernel algorithm of 2DWFRFT further improved the anti-scanning property of the single-parameter WFRFT by taking advantage of multiple horizontal and vertical dimensional transforms with different parameters. First, the signal generation method was given, and the matrix expressions for specific cases were derived. Then, the implementation complexity of the proposed scheme and the advantages of constellation rotation characteristics were described. In order to fully illustrate the anti-interception performance of the scheme from the perspective of physical layer security information theory, the ergodic secrecy capacity was analyzed under the multiple-input single-output (MISO) wiretap channel model. Simulation results show that compared with the one-dimensional WFRFT, the order of 2DWFRFT consisted of multiple parameter vectors, which could effectively improve the interception resistance only at the cost of limited computational complexity, and provide richer constellation features by breaking the point limits of constellation scrambling. Finally, compared with the traditional artificial noise method, the proposed scheme had a higher security capacity without additional signal power consumption.

Keywords: physical layer security; one-dimensional weighted fractional Fourier transform; two-dimensional weighted fractional Fourier transform; constellation rotation; anti-interception; ergodic secrecy capacity

加权分数傅里叶变换(weighted fractional Fourier transform, WFRFT)作为一种广义的傅里叶变换近来受到学者的关注,其变换本身具有完备的数学理论支撑,信号调制方式在通信系统下具有明确的物理含义,可以实现单载波体制与多载波体制的无缝切换[1];在同时具有大多普勒和多径的双选信道下具备出色的抗衰落性能[2]。此外由于 WFRFT 内部 4 个分量可互相形成自干扰信号,且其中多载波分量具备高斯化特征,作为一种独特的信

收稿日期: 2020-11-17
基金项目: 国家自然科学基金(61901140);中国博士后科学基金资助项目(2019M650067);通信网信息传输与分发技术重点实验室基金(6142104190203);黑龙江省自然科学基金(YQ2021F003)
作者简介: 黄永新(1992—),男,博士研究生;
沙学军(1966—),男,教授,博士生导师
通信作者: 沙学军,shaxuejun@hit.edu.cn

号隐藏技术被应用于物理层安全领域中[3]。文献表明 WFRFT 安全应用可从利用 WFRFT 自身特性[4]、WFRFT 与扩频等传统加密技术结合[5]、WFRFT 信息论理论安全[6]三个角度出发。然而,在目前检索的 WFRFT 安全算法文献当中,无论是多参数加权分数傅里叶变换[7](multiple parameter weighted fractional Fourier transform, MP-WFRFT)还是广义多项分数傅里叶变换[8](general multi-fractional Fourier transform, GMFRFT),其数学机理均来源于 Shih[9]于 1995 年提出的多系列态函数加权叠加的分数傅里叶变换。该变换中各项加权系数仅由一个阶数因子决定,故在实际安全领域中存在单参数抗扫描性差以及具有周期性等弊端。

最初的 WFRFT 通信系统应用由光学上的傅里叶变换得来,受此启发,本文利用二维分数傅里叶变换在图像加密上的特殊性质将一维 WFRFT 扩展至二维以进一步增强安全性能。

1 二维离散分数傅里叶变换的定义与性质

从变换的定义形式上看,分数傅里叶变换可以分为两大类。一类是以 Chirp 信号为基底的 Chirp 类分数傅里叶变换,另一类则为多态函数组合的加权类分数傅里叶变换。Chirp 类分数傅里叶变换因其以连续信号为“基”而广泛应用于雷达、测距系统;而加权类分数傅里叶变换虽然与 Chirp 类分数傅立叶变换相比出现较晚,但其离散算法和实现方式都更为简单,因而在信息光学、图像加密等领域得到了广泛应用。

二维加权分数傅里叶变换(two-dimensional weighted fractional Fourier transform, 2DWFRFT)可看作一维加权分数傅里叶的扩展变换,首先给出一维单参数 4-WFRFT 的定义。

任意复数向量 $\boldsymbol{x}=[x(0),x(1),\cdots,x(N-1)]^{\mathrm{T}}$ 的 N 点 α 阶 WFRFT 变换可表示为

$$\mathscr{F}_{\omega}^{\alpha}[\boldsymbol{x}]=\boldsymbol{F}^{\alpha}\boldsymbol{x}=(\omega_0^{\alpha}\boldsymbol{I}+\omega_1^{\alpha}\boldsymbol{F}+\omega_2^{\alpha}\boldsymbol{P}+\omega_3^{\alpha}\boldsymbol{P}\boldsymbol{F})\boldsymbol{x} \quad (1)$$

式中 $\boldsymbol{F}^{\alpha}$ 为 $N\times N$ 阶 WFRFT 矩阵,$[\boldsymbol{F}]_{k,n}=(1/\sqrt{N})\exp(-\mathrm{j}2\pi kn/N)$,符号 $[\cdot]_{k,n}(k,n=0,1,\cdots,N-1)$ 代表取矩阵的第 k 行第 n 个元素,$\boldsymbol{I}$ 为 $N\times N$ 大小的单位矩阵,移位矩阵 $\boldsymbol{P}$ 如文献[1]中定义满足 $[\boldsymbol{P}]_{k,m}=\delta(<k+m>_N)$,符号 $<\cdot>_N$ 代表取 N 模值计算,δ 为冲击函数。同时,α 为 WFRFT 的变换阶数。

ω_{α}^{l} 加权系数的具体形式为

$$\omega_{\alpha}^{l}=\frac{1}{4}\sum_{k=0}^{3}\exp\left[\frac{2\pi\mathrm{j}}{4}(\alpha-l)k\right] \quad (2)$$

式中 $l=0,1,2,3$;j、π 分别为虚数单位与圆周率。

下面介绍二维离散分数傅里叶的定义及性质。

根据文献[10]的描述,可以扩展出大小为 $N\times N$ 的多参数离散分数傅里叶矩阵:

$$\boldsymbol{F}^{\bar{\alpha}}=\sum_{k=0}^{N-1}\lambda_k^{\alpha_k}\boldsymbol{e}_k\boldsymbol{e}_k^{\mathrm{T}},0\leqslant m,n\leqslant N-1 \quad (3)$$

式中:$\lambda_k^{\alpha_k}$ 与 $\boldsymbol{e}_k$ 为 DFT 矩阵的特征值与特征向量,$\bar{\boldsymbol{\alpha}}=[\alpha_1,\alpha_2,\cdots,\alpha_M]$ 为长度 $1\times M$ 的参数向量,进而对于维度为 $M\times N$ 的矩阵信号 $\boldsymbol{M}$,其带有参数向量 $(\bar{\boldsymbol{\alpha}},\bar{\boldsymbol{\beta}})$ 的二维离散分数傅里叶变换为

$$\mathscr{F}_{2\mathrm{D}}^{\bar{\alpha},\bar{\beta}}(\boldsymbol{M})=\boldsymbol{F}^{\bar{\alpha}}\cdot\boldsymbol{M}\cdot\boldsymbol{F}^{\bar{\beta}} \quad (4)$$

式中 $\bar{\boldsymbol{\beta}}=[\beta_1,\beta_2,\cdots,\beta_N]$ 为长度 $1\times N$ 的参数向量。

二维离散分数傅里叶变换具有幺正性、边界性、可加性、周期性。

1)幺正性:

$$(\boldsymbol{F}^{\bar{\alpha}})^{\mathrm{H}}(\boldsymbol{F}^{\bar{\alpha}})=(\boldsymbol{V}\boldsymbol{\Lambda}^{\bar{\alpha}}\boldsymbol{V}^{\mathrm{T}})^{\mathrm{H}}(\boldsymbol{V}\boldsymbol{\Lambda}^{\bar{\alpha}}\boldsymbol{V}^{\mathrm{T}})=(\boldsymbol{V}\boldsymbol{\Lambda}^{-\bar{\alpha}}\boldsymbol{V}^{\mathrm{T}})(\boldsymbol{V}\boldsymbol{\Lambda}^{\bar{\alpha}}\boldsymbol{V}^{\mathrm{T}})=\boldsymbol{V}\boldsymbol{V}^{\mathrm{T}}=\boldsymbol{I} \quad (5)$$

2)边界性:

当 $\bar{\boldsymbol{\alpha}}$ 为零向量,即 $\bar{\boldsymbol{\alpha}}=\bar{\boldsymbol{0}}=[0,0,\cdots,0]$ 时,存在性质 $\boldsymbol{F}^{\bar{\alpha}}=\boldsymbol{V}\boldsymbol{\Lambda}^{\bar{0}}\boldsymbol{V}^{\mathrm{T}}=\boldsymbol{V}\boldsymbol{V}^{\mathrm{T}}=\boldsymbol{I}$;当 $\bar{\boldsymbol{\alpha}}=\bar{\boldsymbol{1}}=[1,1,\cdots,1]$ 时,存在性质 $\boldsymbol{F}^{\bar{\alpha}}=\boldsymbol{V}\boldsymbol{\Lambda}^{\bar{1}}\boldsymbol{V}^{\mathrm{T}}=\boldsymbol{V}\boldsymbol{\Lambda}\boldsymbol{V}^{\mathrm{T}}=\boldsymbol{F}$。

3)可加性:

$$\boldsymbol{F}^{\bar{\alpha}_1}\cdot\boldsymbol{F}^{\bar{\alpha}_2}=(\boldsymbol{V}\boldsymbol{\Lambda}^{\bar{\alpha}_1}\boldsymbol{V}^{\mathrm{T}})(\boldsymbol{V}\boldsymbol{\Lambda}^{\bar{\alpha}_2}\boldsymbol{V}^{\mathrm{T}})=\boldsymbol{V}\boldsymbol{\Lambda}^{\bar{\alpha}_1+\bar{\alpha}_2}\boldsymbol{V}^{\mathrm{T}}=\boldsymbol{F}^{\bar{\alpha}_1+\bar{\alpha}_2} \quad (6)$$

4)周期性:对所有整数 k 来说,$\boldsymbol{F}^{\bar{\alpha}}$ 以 4 为周期,即

$$\begin{cases}\mathrm{e}^{-\mathrm{j}\frac{\pi}{2}k\left(\alpha_k+\frac{4}{k}\right)}=\mathrm{e}^{-\mathrm{j}\frac{\pi}{2}k\alpha_k}, & k\neq 0\\ \mathrm{e}^{-\mathrm{j}\frac{\pi}{2}k}=1, & k=0\end{cases} \quad (7)$$

可以看出,性质 1)代表多参数变换具有酉变换特性;而根据边界性可推导出当 $\bar{\boldsymbol{\alpha}}=\bar{\boldsymbol{1}},\bar{\boldsymbol{\beta}}=\bar{\boldsymbol{1}}$ 时,二维离散分数傅里叶变换退化为二维傅里叶变换。

需要说明的是,虽然多参数变换的周期性使得二维离散分数傅里叶变换仍具有以 4 为周期的重复特性,但横纵多个参数的引入确实增加了抗参数扫描的难度,为应用于物理层安全奠定了理论基础。

2 基于2DWFRFT的安全信号设计方案

2.1 可行性分析与系统模型

现有文献中已有一些将 WFRFT 用于抗截获手段的方法,但无论是单参数加权变换还是多参数加权变换、多项加权变换,其数学机理均为一维 WFRFT,而2DWFRFT将原有的一维 WFRFT 信号扩展至二维,采用信号矩阵横、纵两个维度的不同参数四项加权变换对信号进行加密重组,对于非合作接收机而言,需要在 $M\times N$ 维数轴上同时搜索截获多个参数才能正确恢复出数据;直观地讲,相较于原先

的单参数破解参数搜索次数提升至 $M \times N$ 倍。结合前文公式阐述 2DWFRFT 的信号构建可行性，并将算法应用于实际通信系统中。

考虑一列数字基带映射调制后的向量信号 $\boldsymbol{x} = [x(0), x(1), \cdots, x(N-1)]^{\mathrm{T}}$，将其重组为 M 路 N 点的矩阵信号 $\boldsymbol{S}$。之后以 $\boldsymbol{S}$ 的每行数据为原始序列进行 N 点 4-WFRFT，且每行变化的参数分别设置为 $\alpha_1, \alpha_2, \cdots, \alpha_M$，见图 1，每个行向量的变换过程可表示为

$$\mathscr{F}^{\alpha_i}(F_i) = \omega_0^{\alpha_i} F_i + \omega_1^{\alpha_i} F_i' + \omega_2^{\alpha_i} F_i'' + \omega_3^{\alpha_i} F_i''', \quad i = 1, 2, 3, \cdots, M \tag{8}$$

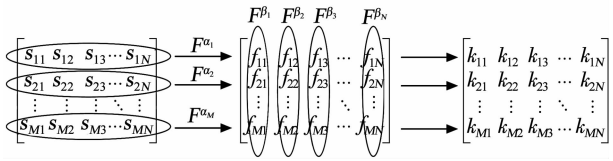


图 1　2DWFRFT 正变换原理示意

Fig. 1　Schematic of 2DWFRFT

同理，如图 2 所示对每个列向量按参数 $\overline{\boldsymbol{\beta}}$ 进行 M 点 WFRFT，变换过程表示为

$$\mathscr{F}^{\beta_i}(F_i) = \omega_0^{\beta_i} F_i + \omega_1^{\beta_i} F'_i + \omega_2^{\beta_i} F''_i + \omega_3^{\beta_i} F'''_i, \quad i = 1, 2, 3, \cdots, N \tag{9}$$

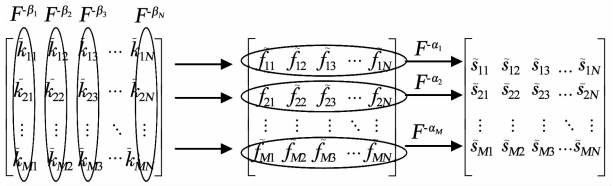


图 2　2DWFRFT 反变换原理示意

Fig. 2　Schematic of two-dimensional inverse weighted fractional Fourier transform

上述 2 项中等式右边首项为原始向量，第 2 项为原始向量经过傅里叶变换后的向量，第 3 项为原始向量的反转向量，尾项为第 2 项的反转向量。

由于收发两端皆为合作方，共享变换参数，合法接收端可通过二维离散分数傅里叶逆变换进行解调恢复原始数据，流程见图 3，其中列与行的参数（$\overline{\boldsymbol{\beta}'}$ 与 $\overline{\boldsymbol{\alpha}'}$）分别为：$\overline{\boldsymbol{\beta}'} = (-\beta_1, -\beta_2, -\beta_3, \cdots, -\beta_N)$，$\overline{\boldsymbol{\alpha}'} = (-\alpha_1, -\alpha_2, -\alpha_3, \cdots, -\alpha_M)$。

需要注意的是，以任意向量参数（$\overline{\boldsymbol{\alpha}}$ 与 $\overline{\boldsymbol{\beta}}$）进行的 2DWFRFT 无矩阵表达式，只能以式（8）、（9）进行信号处理过程描述。但若每行与每列加权变换参数取值分别相同，即 $\alpha_1 = \cdots = \alpha_M = \alpha$，$\beta_1 = \cdots = \beta_N = \beta$ 时，2DWFRFT 具有类似式（6）的简洁表达式，形如：

$$\boldsymbol{k} = (\boldsymbol{F}^{\beta} \otimes \boldsymbol{F}^{\alpha})\boldsymbol{x} \tag{10}$$

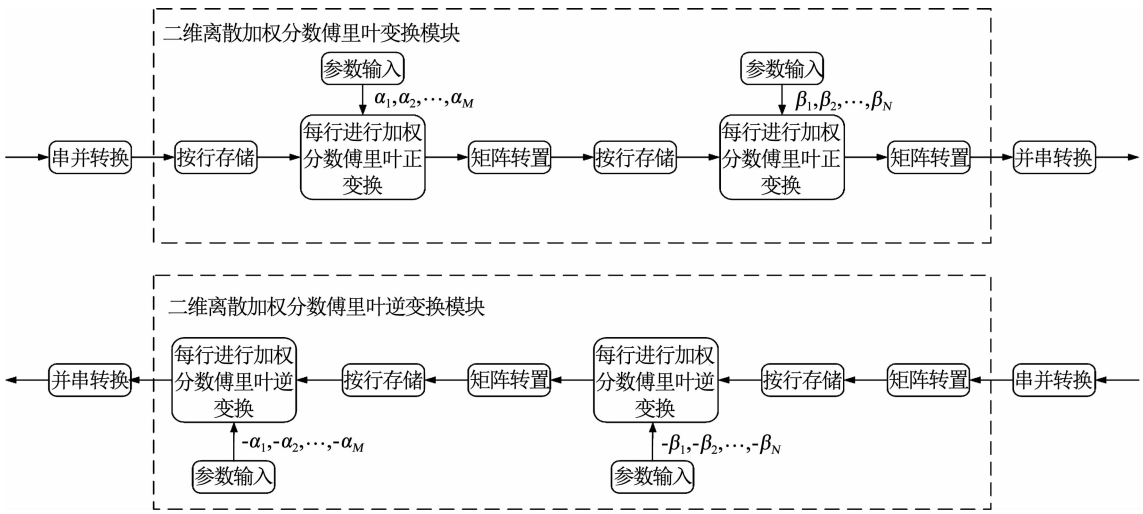


图 3　2DWFRFT 模块流程示意

Fig. 3　Schematic of 2DWFRFT modules

式中⊗为克罗内克乘积。同理，反变换表达式为

$$\boldsymbol{x} = (\boldsymbol{F}_N^{-\beta} \otimes \boldsymbol{F}_M^{-\alpha})\boldsymbol{k} \tag{11}$$

2.2　复杂度分析

在实际通信系统中，考虑硬件的时间资源消耗，通常采用浮点数乘法次数来衡量某种算法的实现复杂度。由文献[1]得知，一维 4-WFRFT 在系统实现时主要由 FFT 模块、反转模块及加权系数合并模块构成，其中 FFT 模块所需实现复杂度为 $O(N \log N)$，四项加权系数合并模块所需实现复杂度为 $O(4N)$。在忽略加法运算的前提下，对于具有维度 $M \times N$ 的矩阵信号，其进行一维 WFRFT 的计算复杂度为 $O(MN \log MN + 4MN)$，算法相应的计算自由度为 $\Theta_{1D} = M \times N$。二维分数傅里叶变换可表示成两次一维 WFRFT 的级联形式，其计算复杂度为 $O(MN \log MN + 8MN)$，计算自由度 $\Theta_{2D} = 2MN$，计算自由度带来 2 倍的提升，而计算自由度是衡量变换安全水平的标准之一[11]；从安全性角度来说，当变换的计算自由度越大时，可为所在的信息系统

提供越高的安全保障。以现在 5G 常规波形，调制子载波数目 2 048 为例，$O(MN\log MN+4MN)=30\,720$，$O(MN\log MN+8MN)=38\,912$，计算复杂度增加 26%，计算自由度增加 100%。而本文所提算法复杂度的提升不高，在现有系统中完全可以接受。

表 1 为各主要模块所需复杂度对比，由表 1 可见，本文算法相较于原一维加权算法以牺牲少量复杂度的代价换取安全性能的提升，后续将对其安全性能方面的收益进行定量分析。

表 1 信号实现复杂度对比

Tab. 1 Implementation complexity comparison of signals

系统	FFT 次数	复数乘法次数	复杂度
WFRFT	1	$4MN$	$MN\log MN+4MN$
2DWFRFT	$M+N$	$8MN$	$MN\log MN+8MN$

2.3 安全性能分析

物理层安全作为目前一个基于香农理论扩展出的保密领域受到了越来越广泛的关注，其核心参数指标安全容量由香农定义。本节基于 MISO 窃听信道模型分析所提安全传输方案的安全容量。

考虑如图 4 所示的常规物理层 MISO 窃听信道模型，其中发送端（配置多天线）与合法接收端（配置单天线）通过合法信道 $\boldsymbol{h}_k$ 进行通信，并且在发送端的广播范围内存在某个多天线窃听端对信号进行侦听，窃听信道表述为 $\boldsymbol{G}_k$；假设两信道均满足平坦瑞利衰落信道分布，且相互独立。令 x 表示合法端发送信息的基带符号映射，则合法接收端与窃听端接收信号模型可分别表示为：

$$y_k=\boldsymbol{h}_k\mathscr{F}^{\bar{\boldsymbol{\alpha}},\bar{\boldsymbol{\beta}}}_{\mathrm{2DWFRFT}}[x_k]+\boldsymbol{v}_k \tag{12}$$

$$\boldsymbol{z}_k=\boldsymbol{G}_k\mathscr{F}^{\bar{\boldsymbol{\alpha}},\bar{\boldsymbol{\beta}}}_{\mathrm{2DWFRFT}}[x_k]+\boldsymbol{e}_k \tag{13}$$

其中 $\boldsymbol{v}_k\sim CN(0,\sigma_b^2)$ 及 $\boldsymbol{e}_k\sim CN(0,\sigma_e^2\boldsymbol{I}_{N_e})$ 为方差 σ_b^2 与 σ_e^2 的零均值循环复高斯随机噪声。

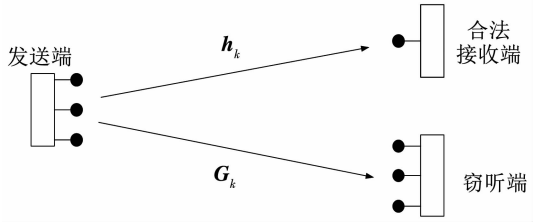


图 4 基于 2DWFRFT 的 MISO 窃听信道模型

Fig. 4 2DWFRFT-based MISO wiretap channel model

这里直接考虑最坏的情况，即假设窃听端已知本文采用了 2DWFRFT 对信号进行加密，但具体变换参数未知，同时窃听端已知全局信道信息（即 $\boldsymbol{h}_k$、$\boldsymbol{G}_k$），则合法接收端与窃听端对源数据符号序列的解调信号分别为

$$r_{\mathrm{B}k}=\mathscr{F}^{-\bar{\boldsymbol{\alpha}},-\bar{\boldsymbol{\beta}}}_{\mathrm{2DWFRFT}}[\boldsymbol{h}_k^*y_k]=\mathscr{F}^{-\bar{\boldsymbol{\alpha}},-\bar{\boldsymbol{\beta}}}_{\mathrm{2DWFRFT}}[|\boldsymbol{h}_k|^2\mathscr{F}^{\bar{\boldsymbol{\alpha}},\bar{\boldsymbol{\beta}}}_{\mathrm{2DWFRFT}}[x_k]]+\boldsymbol{h}_k^*v_k=|\boldsymbol{h}_k|^2x_k+\boldsymbol{h}_k^*v_k \tag{14}$$

$$r_{\mathrm{E}k}=\mathscr{F}^{-\bar{\boldsymbol{\alpha}},-\bar{\boldsymbol{\beta}}}_{\mathrm{2DWFRFT}}[\boldsymbol{G}_k^*z_k]=\mathscr{F}^{-\bar{\boldsymbol{\alpha}},-\bar{\boldsymbol{\beta}}}_{\mathrm{2DWFRFT}}[\|\boldsymbol{G}_k\|_{\mathrm{F}}^2\mathscr{F}^{\bar{\boldsymbol{\alpha}},\bar{\boldsymbol{\beta}}}_{\mathrm{2DWFRFT}}[x_k]]+\boldsymbol{G}_k^*e_k=\|\boldsymbol{G}_k\|_{\mathrm{F}}^2\mathscr{F}^{\Delta\bar{\boldsymbol{\alpha}},\Delta\bar{\boldsymbol{\beta}}}_{\mathrm{2DWFRFT}}[x_k]+\boldsymbol{G}_k^*e_k \tag{15}$$

根据文献[12]，3 点窃听模型下安全容量定义为主信道（合法收发两端）及窃听信道（发送与窃听两端）所能承载的最大互信息量之差：

$$C_{\mathrm{sec}}=\underset{\boldsymbol{h}_k,\boldsymbol{G}_k}{E}[\log_2(1+\gamma_{\mathrm{B}})-\log_2(1+\gamma_{\mathrm{E}})]^+ \tag{16}$$

式中：$E[\cdot]$ 用于求取输入信号的均值期望，$[\cdot]^+=\max(\cdot,0)$，符号 γ_{B} 与 γ_{E} 分别为接收端以及窃听端处的信干噪比。在推导这两处的信干噪比时，为了方便书写参数差异，假设所有二维信号进行变换时行数与列数的加权阶数取值相同。

根据一维 WFRFT 的定义，参数匹配差异下的加权变换 $\mathscr{F}^{\Delta\alpha}[x_k]$ 可表示为

$$\mathscr{F}^{\Delta\alpha}[x_k]=\omega_0^{\Delta\alpha}x_k+\omega_1^{\Delta\alpha}F[x_k]+\omega_2^{\Delta\alpha}F'[x_k]+\omega_3^{\Delta\alpha}F''[x_k] \tag{17}$$

式中：F、F'、F'' 分别表示对原序列进行 1 ~ 3 次傅里叶变换；$\Delta\alpha=\alpha-\alpha'$，$\Delta\beta=\beta-\beta'$ 表示因加权参数保密性造成的窃听端与发送端参数匹配差异；$\omega_p^{\Delta\alpha}$ 满足如下等式：

$$\omega_p^{\Delta\alpha}=\omega_0(\alpha)\omega_p(\beta)+\omega_1(\alpha)\omega_{p+3}(\beta)+\omega_2(\alpha)\omega_{p+2}(\beta)+\omega_3(\alpha)\omega_{p+1}(\beta)\quad p=0,1,2,3 \tag{18}$$

由式(18)可进一步推导 $\mathscr{F}^{\Delta\alpha,\Delta\beta}_{\mathrm{2DWFRFT}}[x_k]$ 为

$$\mathscr{F}^{\Delta\alpha,\Delta\beta}_{\mathrm{2DWFRFT}}[x_k]=\mathscr{F}^{\Delta\beta}_{\mathrm{column}}[\mathscr{F}^{\Delta\alpha}_{\mathrm{row}}[x_k]]=\omega_0^{\Delta\beta}\mathscr{F}^{\Delta\alpha}_{\mathrm{row}}[x_k]+\omega_1^{\Delta\beta}F_{\mathrm{column}}[\mathscr{F}^{\Delta\alpha}_{\mathrm{row}}[x_k]]+\omega_2^{\Delta\beta}F'_{\mathrm{column}}[\mathscr{F}^{\Delta\alpha}_{\mathrm{row}}[x_k]]+\omega_3^{\Delta\beta}F''_{\mathrm{column}}[\mathscr{F}^{\Delta\alpha}_{\mathrm{row}}[x_k]] \tag{19}$$

由式(17)可知，在一维加权分数傅里叶框架下，窃听端对原始数据的估算解调由 4 个子信号加权构成。当 $\Delta\alpha\neq0$ 时，各信号分量之间相互干扰。因此，只有部分原始信号的能量被窃听端收集用于信息内容截获，而其余部分信号能量则以干扰形式存在。式(19)中的 $\mathscr{F}_{\mathrm{column}}$ 与 $\mathscr{F}_{\mathrm{row}}$ 算子分别表示对列向量与行向量实施的加权变换，它可反映出二维加权变换使得可窃听到的有效信息能量进一步降低，第 1 项原始信号能量在经过横纵维度的多次变换后扩散到其他行列以形成干扰。假设原始信号发射功率为 P_0，则窃听端信干噪比表达式为式(21)，公式形式为解调信号期望与总干扰信号期望之比。其中分子部分 $\|\boldsymbol{G}_k\|_{\mathrm{F}}^2\cdot|\omega_0^{\Delta\alpha}\omega_0^{\Delta\beta}x_k|^2$ 为式(18)首项，代表解调信号；分母部分为式(18)中其余 3 项之和，代表由本安全方案带来的干扰。

而对于合法接收端而言，$\mathscr{F}^{0,0}_{\text{2DWFRFT}}[x_k]=x_k$。即 2DWFRFT 的实施不会对目标端信号的正确接收造成任何影响。因此，通信系统中合法接收端的信干噪比 γ_{B} 为

$$\gamma_{\text{Bob}}=\|h_k\|^2P_0/\sigma_b^2 \tag{20}$$

$$\gamma_{\text{Eve}}=\frac{E[\|\boldsymbol{G}_k\|_{\text{F}}^2\cdot|\omega_0^{\Delta\alpha}\omega_0^{\Delta\beta}x_k|^2]}{E[|(\omega_1^{\Delta\beta}F_{\text{column}}[\mathscr{F}^{\Delta\alpha}_{\text{row}}[x_k]]+\omega_2^{\Delta\beta}F'_{\text{column}}[\mathscr{F}^{\Delta\alpha}_{\text{row}}[x_k]]+\omega_3^{\Delta\beta}F''_{\text{column}}[\mathscr{F}^{\Delta\alpha}_{\text{row}}[x_k]])\cdot\|\boldsymbol{G}_k\|_{\text{F}}^2+\boldsymbol{G}_k^*e_k|^2]}=\frac{\|\boldsymbol{G}_k\omega_0^{\Delta\alpha}\omega_0^{\Delta\beta}\|^2P_0}{\sigma_e^2+\|\boldsymbol{G}_k\|_{\text{F}}^2(1-|\omega_0^{\Delta\alpha}\omega_0^{\Delta\beta}|^2)P_0} \tag{21}$$

3　数值模拟

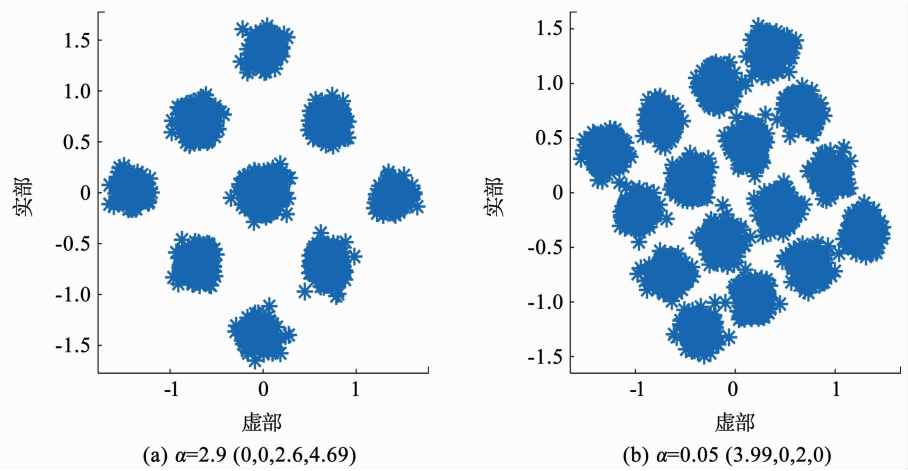
3.1　星座图特征

图 5 是正交相移键控（quadrature phase shift keying，QPSK）调制信号经过一维多参数4-WFRFT变换后在分数域的星座图，可以看出一维变换具有将原星座点进行旋转、扩散的作用。仿真参数设置见表 2，其中 v_k 为多参数加权变换系数因子；图 5（a）中星座分裂为 9 个星座团，而图 5（b）中可分裂为 16 个星座团。图 6 则展示相同的 QPSK 信号在经过 2DWFRFT 后可进一步对星座进行旋转、分裂，在不同参数下星座团个数可分别扩展至 36、64，突破原一维变换的星座点特征限制，这表明 2DWFRFT 方案在干扰非合作接收机检测星座方面可提供更丰富的星座特征。

表 2　各星座图变换参数

Tab. 2　Parameters selection under different constellations

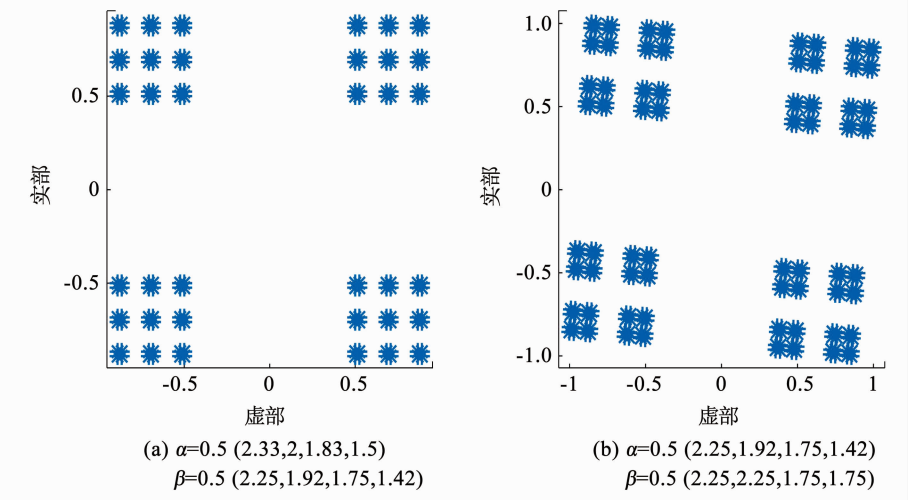
图序	变换参数	(v_0,v_1,v_2,v_3)
图 5（a）	$\alpha=2.9$	(0,0,2.6,4.69)
图 5（b）	$\alpha=0.05$	(3.99,0,2,0)
图 6（a）	$\alpha=0.5$	(2.33,2,1.83,1.5)
	$\beta=0.5$	(2.25,1.92,1.75,1.42)
图 6（b）	$\alpha=0.5$	(2.25,1.92,1.75,1.42)
	$\beta=0.5$	(2.25,2.25,1.75,1.75)



(a) α=2.9 (0,0,2.6,4.69)　　(b) α=0.05 (3.99,0,2,0)

图 5　QPSK 不同参数下 WFRFT 星座

Fig. 5　Constellation of WFRFT-QPSK signals under different parameter conditions



(a) α=0.5 (2.33,2,1.83,1.5)
β=0.5 (2.25,1.92,1.75,1.42)

(b) α=0.5 (2.25,1.92,1.75,1.42)
β=0.5 (2.25,2.25,1.75,1.75)

图 6　QPSK 不同参数下 2DWFRFT 星座

Fig. 6　Constellation of 2DWFRFT-QPSK signals under different parameter conditions

3.2 安全性能

图 7 是考虑在不同信道条件(高斯信道、平坦瑞利衰落信道)下,窃听端已知所采用的传输模式但解调参数有误差情况下的误码率(bit error rate, BER)性能曲线。其中信号采用 QPSK 调制,子载波个数为 1 024,行向量与列向量的加权参数分别统一,并分别为 0.1、0.5。当窃听端未知所采用的传输模式时,对接收信号直接解调的误比特率为 0.5,即窃听端只能对数据序列进行随机猜测。合作接收端采用相应的参数能够进行正确解调并且误码率与理论曲线相重合。当假设窃听端已知所采用的传输模式并尝试进行搜索时,相比于单参数的 WFRFT 在 15 dB 下的安全性能表现,行向量与列向量参数只相差 $\Delta\alpha = \Delta\beta = 0.1$ 时,误码率就会由 10^{-4} 恶化至 10^{-2},足以证明其对参数的敏感性。

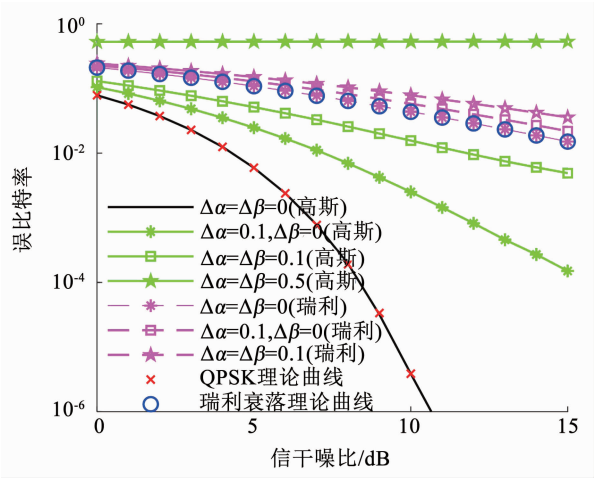


图 7 窃听端随 $\Delta\alpha$、$\Delta\beta$ 变化误码率性能曲线

Fig. 7 BER performance of the eavesdropper with varying $\Delta\alpha$, $\Delta\beta$

图 8 以通信系统的安全容量作为评价指标对 2DWFRFT 物理层安全通信系统的安全性能进行分析。仿真中信道服从独立同分布瑞利衰落,且其信道增益满足 $\boldsymbol{h}_k \sim CN(0,1)$,$\boldsymbol{G}_k \sim CN(0,\boldsymbol{I}_{N_e})$,并假设合法接收端与窃听端处的噪声功率相同,即 $\sigma_e^2 = \sigma_b^2$。当窃听端天线数目为 1 时,2DWFRFT 物理层安全通信系统由信噪比、$\Delta\alpha$ 及 $\Delta\beta$ 决定。系统可达安全容量随信噪比的增加而单调上升,与此同时,相比于一维 WFRFT 单参数 $\Delta\alpha$ 的安全性能,引入 $\Delta\beta$ 后安全容量进一步提升,且提升部分的容量随 $\Delta\beta$ 增大而增加。

图 9 是 2DWFRFT 与文献[13]中人工噪声方法在安全性能上的对比,仿真中发射天线数固定为 8,接收天线数设置为 1、2、4、6 且此时假设最坏情况,即窃听端噪声干扰为 0 dB,人工噪声功率分配系数(即人工噪声功率与发射总功率占比)为 0.5。由于受限于空间自由度,人工噪声方法的安全容量会随着窃听天线数增加而减小,这源于窃听信道容量随窃听端天线数目增加而增大;而此时本文所提方法由于不依赖信道零空间的提取,其安全容量在阶数差值较大时对窃听端天线数目具有鲁棒性,在不需要额外消耗干扰功率的条件下可以有效抑制窃听端对信息的获取,达到较高的安全可达速率。同时值得注意的是,2DWFRFT 作为一种通用的基带数字信号处理方法,理论上可以与人工噪声方法结合使用。

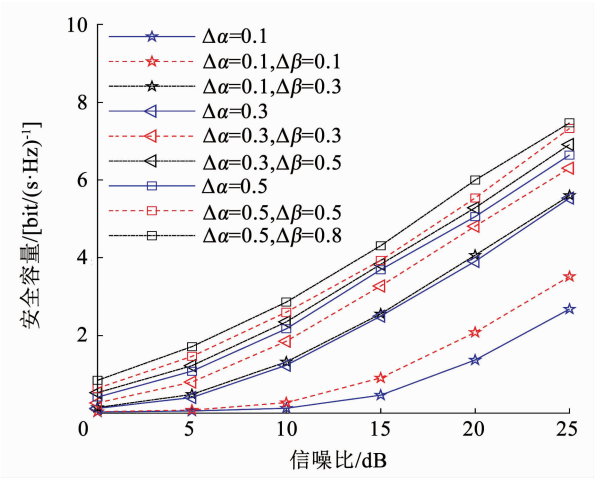


图 8 不同参数下 2DWFRFT 安全容量

Fig. 8 Secrecy capacity of 2DWFRFT under different parameter conditions

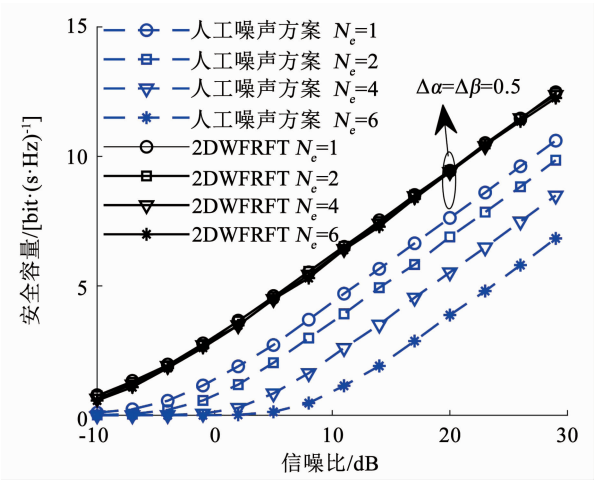


图 9 2DWFRFT 安全容量随窃听天线数 N_e 变化趋势

Fig. 9 Secrecy capacity of 2DWFRFT with varying N_e

4 结 论

本文开展了 2DWFRFT 的研究,对一维单参数 4-WFRFT 进行了二维扩展,并将其应用于通信系统当中,最后针对抗截获性能,在 MISO 窃听信道下对安全容量进行了定量分析。主要结论如下:

1) 2DWFRFT 阶数由多个参数向量决定,相比一维 WFRFT 的单参数,在抗参数扫描方面具备机

理优势。

2）2DWFRFT 可表示成两次一维 WFRFT 的级联形式，仅以部分计算复杂度的代价换来计算自由度的 2 倍提升。

3）在变换后的星座图混淆方面，2DWFRFT 可突破一维变换的分裂点数限制，提供更加丰富的星座变换特征。

4）在安全性能方面，与传统人工噪声方法相比，2DWFRFT 方案不仅继承了一维变换不依赖信道特性、无需消耗额外干扰功率的优点，同时由于多参量的引入其安全容量可进一步提升。

参考文献

[1] MEI Lin, SHA Xuejun, RAN Qinwen, et al. Research on the application of 4-weighted fractional Fourier transform in communication system[J]. Science China Information Sciences, 2010, 53(6): 1251. DOI: 10.1007/s11432-010-0073-1

[2] LIN Xu, MEI Lin, FANG Xiaojie, et al. HCM successive transmission scheme with banded MMSE equalization based on fast convolution over doubly-selective fading channels[J]. IEEE Communications Letters, 2020, 24(2): 451. DOI: 10.1109/LCOMM.2019.2954309

[3] CHENG Qian, FUSCO V, ZHU Jiang, et al. WFRFT-aided power-efficient multi-beam directional modulation schemes based on frequency diverse array[J]. IEEE Transactions on Wireless Communications, 2019, 18(11): 5211. DOI: 10.1109/TWC.2019.2934462

[4] 梁源，达新宇. 基于多参数加权分数阶傅里叶变换的星座预编码系统研究与实现[J]. 电子与信息学报，2018，40(4)：825
LIANG Yuan, DA Xinyu. Analysis and implementation of constellation precoding system based on multiple parameters weighted type fractional Fourier transform[J]. Journal of Electronics & Information Technology, 2018, 40(4): 825

[5] FANG Xiaojie, SHA Xuejun, LI Yong. Secret communication using parallel combinatory spreading WFRFT[J]. IEEE Communications Letters, 2015, 19(1): 62. DOI: 10.1109/LCOMM.2014.2359200

[6] FANG Xiaojie, ZHANG Ning, ZHANG Shan, et al. On physical layer security: Weighted fractional Fourier transform based user cooperation[J]. IEEE Transactions on Wireless Communications, 2017, 16(8): 5498. DOI: 10.1109/TWC.2017.2712158

[7] RAN Qiwen, ZHAO Tieyu, YUAN Lin, et al. Vector power multiple-parameter fractional Fourier transform of image encryption algorithm[J]. Optics & Lasers in Engineering, 2014, 62: 80. DOI: 10.1016/j.optlaseng.2014.05.008

[8] RAN Qiwen, YEUNG D S, TSANG E C C, et al. General multifractional Fourier transform method based on the generalized permutation matrix group[J]. IEEE Transactions on Signal Processing, 2005, 53(1): 83. DOI: 10.1109/TSP.2004.837397

[9] SHIH C C. Fractionalization of Fourier transform[J]. Optics Communications, 1995, 118(5/6): 495. DOI: 10.1016/0030-4018(95)00268-D

[10] HSUE Wenliang. Enhancing security of double random phase encryption schemes based on discrete fractional Fourier transforms[J]. IEEE Transactions on Circuits and Systems II: Express Briefs, 2018, 66(9): 1602. DOI: 10.1109/TCSII.2018.2889968

[11] YOUSSEF A M. On the security of a cryptosystem based on multiple-parameters discrete fractional Fourier transform[J]. IEEE Signal Processing Letters, 2008, 15(1): 77. DOI: 10.1109/LSP.2007.910299

[12] SHANNON C E. Communication theory of secrecy systems[J]. The Bell System Technical Journal, 1949, 28(4): 656. DOI: 10.1002/j.1538-7305.1949.tb00928.x

[13] ZHOU Xiangyun, MCKAY M R. Secure transmission with artificial noise over fading channels: Achievable rate and optimal power allocation[J]. IEEE Transactions on Vehicular Technology, 2010, 59(8): 3831. DOI: 10.1109/TVT.2010.2059057

（编辑　苗秀芝）