无简并超混沌驱动三维星座加密的EWFRFT通信方法

贠彦直,孟庆微*,王 晗,马志强
(空军工程大学信息与导航学院,陕西西安 710077)

摘 要: 为进一步增强无线通信的安全性,提出了一种无简并超混沌驱动三维星座加密的扩展加权分数傅里叶变换(Extended Weighted Fractional Fourier Transform, EWFRFT)通信方法. 该方法构建了一种无简并超混沌,运用其产生的混沌序列控制缩放、罗德里格斯旋转的参数,生成随机的缩放矩阵、罗德里格斯旋转矩阵,对每个星座点实施先缩放再旋转的三维星座加密;随后,将加密星座点组合为I/Q信号,再进行EWFRFT处理. 同时,给出了三维星座加密的数学模型和密码原语,证明了其具有完全保密性,且每个星座点均有8个相互独立的因素控制加密,变换后的位置更加随机不可预测. 仿真结果表明,所提方法加密后不仅扰乱了原本分布规律的星座图,提升了无线信号的抗截获能力,而且传输信息呈现良好的随机性分布,能够对抗穷举、统计等常见攻击.

关键词: 物理层安全;无简并超混沌;三维缩放;罗德里格斯旋转;扩展加权分数傅里叶变换
基金项目: 国家自然科学基金(No.62101591)
中图分类号: TN918.91 **文献标识码:** A **文章编号:** 0372-2112(2025)09-3245-11
电子学报URL:http://www.ejournal.org.cn **DOI:**10.12263/DZXB.20250135

EWFRFT Communication Method Using Non-Degenerate Hyperchaos-Driven Three-Dimensional Constellation Encryption

YUN Yan-zhi, MENG Qing-wei*, WANG Han, MA Zhi-qiang
(*School of Information and Navigation*, *Air Force Engineering University*, *Xi'an*, *Shaanxi* 710077, *China*)

Abstract: To further enhance the security of wireless communication, an extended weighted fractional Fourier transform (EWFRFT) communication method using non-degenerate hyperchaos-driven three-dimensional constellation encryption is proposed. The method constructs a non-degenerate hyperchaos and utilizes its generated sequences to control the parameters of scaling and Rodrigues' rotation. It generates randomized scaling matrices and Rodrigues' rotation matrices, applying 3D constellation encryption through sequential scaling followed rotation to each constellation point. Then, the encrypted constellation points are combined into I/Q signals for EWFRFT processing. Furthermore, the mathematical model and cryptographic primitives for 3D constellation encryption are presented, which demonstrates its perfect confidentiality. Each constellation point is controlled by 8 mutually factors for encryption, resulting in more randomized and unpredictable transformed positions. Simulation results show that the proposed method not only disrupts the original structured constellation distribution, improving the anti-interception capability of wireless signals, but also presents excellent randomness in transmitted information, effectively resisting common attacks such as exhaustive attack and statistical attack.

Key words: physical layer security; non-degenerate hyperchaos; three-dimensional scaling; Rodrigues' rotation; extended weighted fractional Fourier transform
Foundation Item(s): National Natural Science Foundation of China (No.62101591)

收稿日期:2025-02-22;录用日期:2025-09-18;责任编辑:朱梅玉
*通讯作者:孟庆微

1 引言

无线通信技术给人们生活带来了极大便利,但信道的开放性和广播性致使重要敏感信息面临着安全风险,亟需采取有效措施以保护信息安全. 传统加密技术主要作用于通信协议栈上层,对调制方式等保护存在短板,为攻击者提供了可乘之机. 调制加密作为一种新型物理层安全技术,将通信信号处理与密码技术有机结合,从信号发射源头消除特征可识别性,实现抗截获、防破解的主动防御,成为了近年来国内外研究热点[1].

在通信信号处理领域,加权分数傅里叶变换(Weighted Fractional Fourier Transform, WFRFT)作为一种混合载波调制方案,其引入了调制阶数的自由度,可以实现星座上的混淆与置乱,已广泛应用于信号隐蔽传输[2~4]. 然而,WFRFT是由周期性态函数加权叠加得到,存在参数维度低、周期特征显著等天然缺陷,容易被循环相关法[5]、高阶累积量[6]等识别破解. 为此,学者从两个方面对WFRFT系统进行了改进. 一方面,充分发挥WFRFT的良好兼容性,将其与直扩通信[7]、星座加密[8]、人工噪声[9]等技术有效结合,设计多维防护的调制信号. 另一方面,从WFRFT能够提供丰富的信号形式出发,结构层面,构建多层WFRFT、二维WFRFT[10],增加信号的复杂度和随机性;理论层面,突破传统变换阶数对WFRFT的限制,提出了扩展加权分数傅里叶变换(Extended WFRFT, EWFRFT)[11],进一步拓展了信号的表现形式和特性. 然而,EWFRFT变换参数敏感性较低,单纯利用其进行数据传输时,难以对抗穷举攻击. 因此,利用EWFRFT的良好兼容性,将其与星座加密相结合以设计复合调制加密信号,对于提升系统的安全性至关重要.

星座加密是一种在密钥控制下对星座点进行旋转、平移等置乱操作的技术[12],能够有效提高无线信号的抗截获、信息的抗破解能力. 目前,按照星座映射方式,其可分为二维[13,14]与三维[15~20]两种,其中,三维星座加密因其在频谱效率与能量效率方面的显著优势而备受关注. 然而现有方法存在一定的局限,文献[16]通过绕坐标轴旋转实现加密,每个星座点需进行三次矩阵乘法,计算复杂度较高;文献[17]基于四元数的三维星座旋转加密方法,其旋转轴与角度间存在关联性,限制了加密维度的扩展;文献[18~20]将旋转与平移相结合,即由3个旋转角和1个平移量控制星座加密,安全性有所提升,但仍未解决旋转操作复杂和加密灵活性不高的问题. 实际上,三维星座加密的过程与三维空间中物体的刚性运动相类似,其安全性与运动模型的数学表达密不可分. 因此,引入更高效、更灵活的刚性运动模型[21]设计加密算法,是提升星座加密安全性能的有效途径.

在具体实现时,密钥的生成机制是星座加密的关键环节,其中,混沌映射因其初值敏感性、伪随机性等优良特性而被广泛应用[15~20]. 然而,数字混沌系统会发生动力学退化现象[22],许多一维和二维混沌映射存在密钥空间有限、迭代周期短以及控制参数取值不当易陷入周期窗口等缺陷,迭代生成的混沌序列不适合直接作为数据加密密钥. 为此,设计随机性更强的混沌映射成为当前混沌密码研究的重点. 文献[23,24]给出了无简并超混沌的定义、设计与实现方法,其是指正的Lyapunov指数个数与混沌维度相同的一类超混沌. 相对经典混沌,该类混沌具备更大的控制参数范围和更优的随机性. 因此,基于星座加密密钥取值范围,设计无简并超混沌,是提升星座加密安全性能的重要策略.

本文将EWFRFT与三维星座加密相结合,提出了一种无简并超混沌驱动三维星座加密的EWFRFT通信方法,主要工作如下.

(1)按照三维星座加密密钥有效取值范围,构建了一种无简并超混沌,利用Lyapunov指数、相图、谱熵等验证了其具有良好的随机性.

(2)针对三维星座加密的灵活性不足,引入三维缩放和罗德里格斯旋转模型,提出了一种无简并超混沌控制星座点先缩放再旋转的三维星座加密方法,并给出了该方法的数学模型及密码原语,证明了其具有完全保密性.

(3)进一步地,先将信息序列映射为三维星座点并实施三维星座加密,再将加密星座点组合为I/Q信号,进行EWFRFT二次加密. 所提方法加密后不仅扰乱了原本分布规律的星座图,提升了无线信号的抗截获能力,而且传输信息呈现良好的随机性分布,能够对抗穷举、统计等常见攻击.

2 问题的提出

2.1 扩展加权分数傅里叶变换

WFRFT在物理层安全领域已获广泛应用,然而随着研究的深入,受限于单一变换阶数,其抗检测能力存在瓶颈. 文献[11]突破这一约束,提出了EWFRFT,其定义为

$$\mathcal{F}_E^{\pm}[\boldsymbol{X}]=w_0(\boldsymbol{\theta})\boldsymbol{X}+w_1(\boldsymbol{\theta})\boldsymbol{X}_1+w_2(\boldsymbol{\theta})\boldsymbol{X}_2+w_3(\boldsymbol{\theta})\boldsymbol{X}_3 \quad (1)$$

其中,$\boldsymbol{X}=\left[x_1,x_2,\cdots,x_m\right]$为离散信号;$\boldsymbol{X}_j$为$\boldsymbol{X}$的第$j$次离散傅里叶变换,$j=1,2,3$;$\boldsymbol{\theta}=\left[\theta_0,\theta_1,\theta_2,\theta_3\right]$为变换参数,$\theta_p\in[0,2\pi),p=0,1,2,3$;$w_n(\boldsymbol{\theta})$为第$n$项加权系数,

$$w_n(\boldsymbol{\theta})=\frac{1}{4}\sum_{p=0}^{3}\exp\left[\left(\theta_p-\frac{2\pi}{4}np\right)\mathrm{i}\right],n=0,1,2,3 \quad (2)$$

其中,i为虚数单位.

EWFRFT具有参数可加性,对变换参数$\boldsymbol{\theta}$取反即可得逆变换$\mathcal{F}_E^{-}[\boldsymbol{X}]$.

$$\mathcal{F}_E^{-}[\boldsymbol{X}]=w_0(-\boldsymbol{\theta})\boldsymbol{X}+w_1(-\boldsymbol{\theta})\boldsymbol{X}_1+w_2(-\boldsymbol{\theta})\boldsymbol{X}_2+w_3(-\boldsymbol{\theta})\boldsymbol{X}_3 \tag{3}$$

相比WFRFT,EWFRFT作为分数傅里叶变换的最新理论成果,在保留适用于通信系统基本性质的同时,通过解耦变换参数的关联性,构建多维独立参数空间,一定程度上增强了系统的抗参数扫描性能.

2.2　三维星座调制

采用高速率、高性能的调制解调技术是提升通信系统性能的重要途径之一,其中扩展信号维度是提升调制解调性能的直接方法. 相应地,星座图由二维扩展至高维,其中三维星座调制是指在三维空间内设计星座点分布,将传输信息按照一定的规则映射到星座点上. 通常传输信息每t个比特映射到一个星座点,2^t个星座点分布在球面上. 图1展示了星座点为正四面体、正方体的三维星座图,其中图1(a)星座点的坐标分别为

$$S_0=(0,0,1),\quad S_1=\left(-\frac{\sqrt{2}}{3},-\frac{2}{\sqrt{6}},-\frac{1}{3}\right),$$

$$S_2=\left(-\frac{\sqrt{2}}{3},\frac{2}{\sqrt{6}},-\frac{1}{3}\right),\quad S_3=\left(\frac{2\sqrt{2}}{3},0,-\frac{1}{3}\right).$$

传输信息与星座点的映射关系为

$$00\rightleftharpoons S_0,01\rightleftharpoons S_1,10\rightleftharpoons S_2,11\rightleftharpoons S_3.$$

图1(b)星座点的坐标分别为

$$S_0=\left(\frac{1}{\sqrt{3}},\frac{1}{\sqrt{3}},\frac{1}{\sqrt{3}}\right),\quad S_1=\left(-\frac{1}{\sqrt{3}},-\frac{1}{\sqrt{3}},\frac{1}{\sqrt{3}}\right),$$

$$S_2=\left(\frac{1}{\sqrt{3}},-\frac{1}{\sqrt{3}},-\frac{1}{\sqrt{3}}\right),\quad S_3=\left(-\frac{1}{\sqrt{3}},\frac{1}{\sqrt{3}},-\frac{1}{\sqrt{3}}\right),$$

$$S_4=\left(\frac{1}{\sqrt{3}},-\frac{1}{\sqrt{3}},\frac{1}{\sqrt{3}}\right),\quad S_5=\left(-\frac{1}{\sqrt{3}},\frac{1}{\sqrt{3}},\frac{1}{\sqrt{3}}\right),$$

$$S_6=\left(\frac{1}{\sqrt{3}},\frac{1}{\sqrt{3}},-\frac{1}{\sqrt{3}}\right),\quad S_7=\left(-\frac{1}{\sqrt{3}},-\frac{1}{\sqrt{3}},-\frac{1}{\sqrt{3}}\right).$$

传输信息与星座点的映射关系为

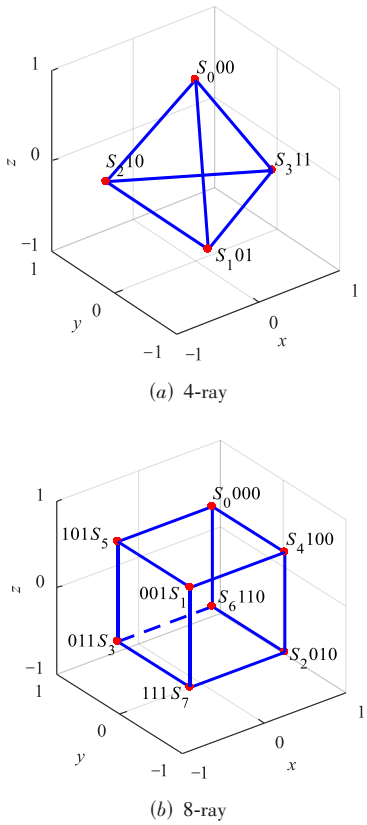
$$000\rightleftharpoons S_0,001\rightleftharpoons S_1,010\rightleftharpoons S_2,011\rightleftharpoons S_3,$$

$$100\rightleftharpoons S_4,101\rightleftharpoons S_5,110\rightleftharpoons S_6,111\rightleftharpoons S_7.$$

在星座点数目相同的情况下,分布在三维空间的信号较二维空间能获得更大的最小欧氏距离,从而实现更低的误码率,同时,三维空间赋予星座加密更高的灵活性和自由度,为加密算法优化提供了便利条件.

2.3　三维空间物体运动的数学表示

三维星座加密的本质在于密钥的控制下对原始星座点进行旋转、平移等几何置乱,其过程类似于三维空间中物体的刚性运动. 为此,本文引入三维空间中缩放变换和罗德里格斯旋转来实现星座加密,旨在进一步提升加密方法的灵活性与安全性.



(a) 4-ray

(b) 8-ray

图1　三维星座

2.3.1　三维缩放

三维空间中,过原点的向量$\boldsymbol{w}$沿着单位向量$\boldsymbol{n}$的方向缩放,数学表达式为

$$\boldsymbol{w}_s=\boldsymbol{w}\cdot\boldsymbol{S}(\boldsymbol{n},k) \tag{4}$$

其中,$\boldsymbol{w}_s$为缩放后的向量;k为缩放因子;$\boldsymbol{S}(\boldsymbol{n},k)$为缩放矩阵.

$$\boldsymbol{S}(\boldsymbol{n},k)=\begin{bmatrix}1+(k-1)n_x^2 & (k-1)n_xn_y & (k-1)n_xn_z\\ (k-1)n_xn_y & 1+(k-1)n_y^2 & (k-1)n_yn_z\\ (k-1)n_xn_z & (k-1)n_yn_z & 1+(k-1)n_z^2\end{bmatrix} \tag{5}$$

其中,n_x,n_y,n_z分别为单位矢量$\boldsymbol{n}$的x,y,z轴坐标.

2.3.2　罗德里格斯旋转

罗德里格斯旋转能够表达三维空间中物体绕任意轴旋转任意角度,数学表达式为

$$\boldsymbol{v}_{\mathrm{rot}}=\boldsymbol{v}\cdot\boldsymbol{Q}(\boldsymbol{u},\theta) \tag{6}$$

其中,$\boldsymbol{v}_{\mathrm{rot}}$是旋转后的向量;$\boldsymbol{v}$是原始向量;$\theta$是旋转角度;$\boldsymbol{u}$是单位旋转轴向量;$\boldsymbol{Q}(\boldsymbol{u},\theta)$为旋转矩阵,由罗德里格斯旋转公式(Rodrigues' rotation formula)给出:

$$\boldsymbol{Q}(\boldsymbol{u},\theta)=\boldsymbol{I}+\boldsymbol{U}\sin\theta+\boldsymbol{U}^2(1-\cos\theta) \tag{7}$$

其中,$\boldsymbol{I}$是3×3单位矩阵;$\boldsymbol{U}$是反对称矩阵($\boldsymbol{U}^{\mathrm{T}}=-\boldsymbol{U}$):

$$\boldsymbol{U}=\begin{pmatrix}0 & -u_z & u_y\\ u_z & 0 & -u_x\\ -u_y & u_x & 0\end{pmatrix} \tag{8}$$

其中，$\boldsymbol{U}^{\mathrm{T}}$ 为矩阵的转置；u_x,u_y,u_z 分别是 $\boldsymbol{u}$ 的 x,y,z 轴坐标.

旋转矩阵 $\boldsymbol{Q}(\boldsymbol{u},\theta)$ 是正交矩阵，即 $\boldsymbol{Q}^{-1}(\boldsymbol{u},\theta)=\boldsymbol{Q}^{\mathrm{T}}(\boldsymbol{u},\theta)$ 且 $\left|\boldsymbol{Q}(\boldsymbol{u},\theta)\right|=1$.

由上述数学表达式可以看出，三维缩放与罗德里格斯旋转在描述三维空间运动时，分别表征平移与旋转操作，且均由4个独立参数控制. 将两者结合应用于三维星座加密，仅需两次矩阵乘法即可实现旋转与平移复合加密，不仅可以降低计算复杂度，更通过独立参数组合能够提升加密的灵活性.

3 三维星座加密的EWFRFT通信方法

本文提出一种无简并超混沌驱动三维星座加密的EWFRFT通信方法，具体通信模型见图2. 该方法构建无简并超混沌以生成数据加、解密密钥. 发送端将信息序列映射为三维星座点，对其实施先缩放再旋转的三维星座加密，接着，加密星座点组合为I/Q信号，再依次进行EWFRFT、添加循环前缀(Cycic Prefix，CP)等后由无线信道发送. 合法接收端执行相反的处理过程，即去除CP、EWFRFT逆变换、反I/Q转换、三维星座解密、解调等，恢复出原始信息.

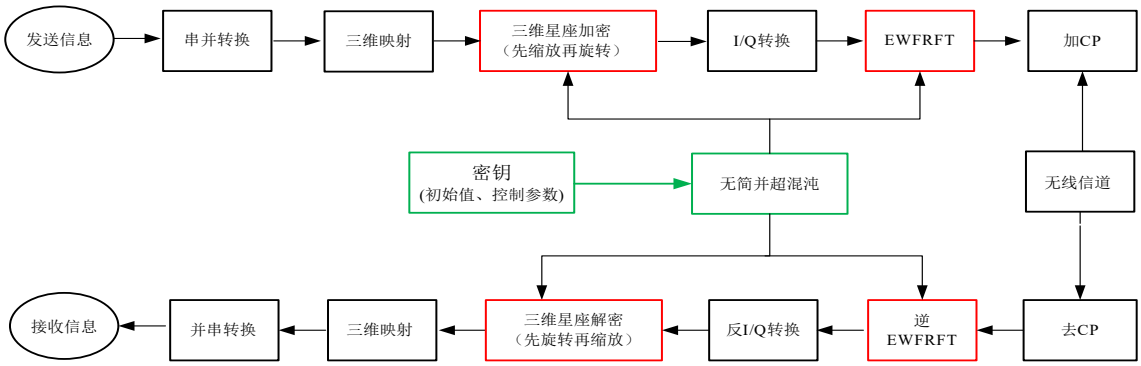


图2 三维星座加密的EWFRFT通信系统模型

3.1 密钥生成

按照三维星座加密密钥和EWFRFT参数的取值范围，构建无简并超混沌，其差分方程为

$$\begin{cases}x_{i+1}=\sin(ra_{11}x_i+a_{12}y_i^2+a_{13}z_i^2)\\ y_{i+1}=\sin(ra_{22}y_i)\\ z_{i+1}=(a_{32}y_i^2+ra_{33}z_i)\bmod 2\end{cases} \tag{9}$$

其中，状态变量 $x_i,y_i\in[-1,1]$，$z_i\in[0,2)$ 且初值不为0；控制参数 $r\in(0,+\infty)$，$a_{ij}\in(0,+\infty)$，$1\leqslant i,j\leqslant 3$.

3.2 加密方法

加密方法如下：

步骤1 明文信息经三维星座调制形成 N_s 个星座点，第 i 个星座点 M_i 的坐标为 (x_i,y_i,z_i)，则调制信号 $\boldsymbol{M}$ 为

$$\boldsymbol{M}=\begin{pmatrix}x_1 & y_1 & z_1\\ x_2 & y_2 & z_2\\ \vdots & \vdots & \vdots\\ x_{N_s} & y_{N_s} & z_{N_s}\end{pmatrix} \tag{10}$$

步骤2 设无简并超混沌的初值为 (x_0,y_0,z_0)、控制参数为 $(r,a_{11},a_{12},a_{13},a_{22},a_{32},a_{33})$，迭代生成长度分别为 $2N_s$ 的混沌序列 $\boldsymbol{x},\boldsymbol{y},\boldsymbol{z}$，组合成 N_s 个方向矢量，并从序列 $\boldsymbol{z}$ 中筛选出 $[0.7,1.7]$ 数值 N_s 个，作为缩放因子. 其中，第 i 个缩放因子为 k_i，方向矢量 $\boldsymbol{n}_i$ 的坐标 $(\boldsymbol{n}_{i,x},\boldsymbol{n}_{i,y},\boldsymbol{n}_{i,z})$ 为

$$\begin{cases}\boldsymbol{n}_{i,x}=\boldsymbol{x}_i\\ \boldsymbol{n}_{i,y}=\boldsymbol{y}_i\\ \boldsymbol{n}_{i,z}=\boldsymbol{z}_i\end{cases}\quad(i=1,2,\cdots,N_s) \tag{11}$$

依据式(5)生成 N_s 个缩放矩阵，第 i 个缩放矩阵为 $\boldsymbol{S}_i(\boldsymbol{n}_i,k_i)$.

选取混沌序列作为旋转轴和旋转角度，第 i 个旋转角度 θ_i 及旋转轴 $\boldsymbol{u}_i$ 的坐标 $(\boldsymbol{u}_{i,x},\boldsymbol{u}_{i,y},\boldsymbol{u}_{i,z})$ 为

$$\begin{cases}\boldsymbol{u}_{i,x}=\boldsymbol{x}_{i+N_s}\\ \boldsymbol{u}_{i,y}=\boldsymbol{y}_{i+N_s}\\ \boldsymbol{u}_{i,z}=\boldsymbol{z}_{i+N_s}\\ \theta_i=\left|\boldsymbol{x}_i\right|\times\pi\end{cases}\quad(i=1,2,\cdots,N_s) \tag{12}$$

依据式(7)和式(8)构造 N_s 个旋转矩阵，第 i 个旋转矩阵为 $\boldsymbol{Q}_i(\boldsymbol{u}_i,\theta_i)$. 计算缩放矩阵和旋转矩阵时需对方向矢量和旋转轴单位化.

步骤3 每个星座点先缩放，再旋转，完成三维星座加密.

$$M_i'=M_i\cdot\boldsymbol{S}_i(\boldsymbol{n}_i,k_i)\cdot\boldsymbol{Q}_i(\boldsymbol{u}_i,\theta_i) \tag{13}$$

M_i' 表示第 i 个星座点 M_i 加密后的点，三维星座加密信号 $\boldsymbol{M}'$ 为

$$\boldsymbol{M}'=\begin{pmatrix} x_1' & y_1' & z_1' \\ x_2' & y_2' & z_2' \\ \vdots & \vdots & \vdots \\ x_{N_s}' & y_{N_s}' & z_{N_s}' \end{pmatrix} \tag{14}$$

步骤4　按照式(15)将$\boldsymbol{M}'$转换为I/Q信号.

$$\boldsymbol{M}''=\begin{pmatrix} x_1'+\mathrm{i}y_1' \\ z_1'+\mathrm{i}x_2' \\ y_2'+\mathrm{i}z_2' \\ \vdots \\ z_{N_s-1}'+\mathrm{i}x_{N_s}' \\ y_{N_s}'+\mathrm{i}z_{N_s}' \end{pmatrix}^{\mathrm{T}} \tag{15}$$

步骤5　信号$\boldsymbol{M}''$分组后每部分进行EWFRFT,其中变换参数$\boldsymbol{\theta}$由混沌序列$\boldsymbol{z}$中每个元素乘以π组合,则加密信号$\boldsymbol{M}'''$为

$$\boldsymbol{M}'''=\mathrm{EWFRFT}\left\{\boldsymbol{M}'',(\theta_1,\theta_2,\theta_3,\theta_4)\right\} \tag{16}$$

加密信号添加循环前缀等后经无线信道发送.

3.3　解密方法

解密方法如下:

步骤1　接收端运用共享的密钥迭代生成无简并超混沌序列,按照同发送端一样的方式构造缩放矩阵、旋转矩阵及选取EWFRFT的变换参数.

步骤2　接收信号$\boldsymbol{R}$分组后每部分进行逆EWFRFT,待解密信号$\boldsymbol{R}'$为

$$\boldsymbol{R}'=\mathrm{EWFRFT}\left\{\boldsymbol{R},(-\theta_1,-\theta_2,-\theta_3,-\theta_4)\right\} \tag{17}$$

步骤3　提取信号$\boldsymbol{R}'$的实部和虚部,转换成如式(15)的待解密三维星座信号,并对每个点先反向旋转再反向缩放:

$$\begin{aligned} R_i''&=R_i'\cdot\left[\boldsymbol{Q}_i(\boldsymbol{u}_i,\theta_i)\right]^{-1}\cdot\left[\boldsymbol{S}_i(\boldsymbol{n}_i,k_i)\right]^{-1} \\ &=R_i'\cdot\left[\boldsymbol{Q}_i(\boldsymbol{u}_i,\theta_i)\right]^{\mathrm{T}}\cdot\left[\boldsymbol{S}_i(\boldsymbol{n}_i,k_i)\right]^{-1} \end{aligned} \tag{18}$$

其中,R_i'为第i个待解密三维星座点,R_i''为第i个三维星座解密点. 式(18)运用了旋转矩阵的正交性,提高了计算效率.

步骤4　计算解密符号R_i''与原始星座图中各个星座点的欧氏距离,按照三维星座映射关系,将距离最小星座点恢复为接收信息.

4　性能分析

本文加密方法融合了无简并超混沌、三维星座加密以及EWFRFT等多种技术,因此,将分别从混沌动力学特性、三维星座加密的完全保密性等方面重点加以分析.

4.1　无简并超混沌的动力学特性

4.1.1　Lyapunov指数

无简并超混沌存在不动点(0,0,0),雅可比矩阵$\boldsymbol{J}$如式(19)所示:

$$\boldsymbol{J}=\begin{bmatrix} ra_{11}\cos(ra_{11}x_i+a_{12}y_i^2+a_{13}z_i^2) & 2a_{12}y_i\cos(ra_{11}x_i+a_{12}y_i^2+a_{13}z_i^2) & 2a_{13}z_i\cos(ra_{11}x_i+a_{12}y_i^2+a_{13}z_i^2) \\ 0 & ra_{22}\cos(ra_{22}y_i) & 0 \\ 0 & 2a_{32}y_i & ra_{33} \end{bmatrix} \tag{19}$$

通过高斯消元法将$\boldsymbol{J}$变换为主对角线元素保持不变的上三角矩阵,得到特征值构成的对角阵$\boldsymbol{D}$:

$$\boldsymbol{D}=\begin{bmatrix} ra_{11}\cos(ra_{11}x_i+a_{12}y_i^2+a_{13}z_i^2) & 0 & 0 \\ 0 & ra_{22}\cos(ra_{22}y_i) & 0 \\ 0 & 0 & ra_{33} \end{bmatrix} \tag{20}$$

因此,该混沌的Lyapunov指数分别为$\ln\left|ra_{11}\cos(ra_{11}x_i+a_{12}y_i^2+a_{13}z_i^2)\right|$,$\ln\left|ra_{22}\cos(ra_{22}y_i)\right|$,$\ln\left|ra_{33}\right|$. 只要控制参数$r,a_{11},a_{22},a_{33}$的乘积越大,则混沌的Lyapunov指数越大,更能保证进入超混沌状态. 图3展示了Lyapunov指数随控制参数的变化情况,可见,随着控制参数的增大,Lyapunov指数均变大,表明该混沌对初值的微小变化敏感. 同时,该混沌参数取值范围大.

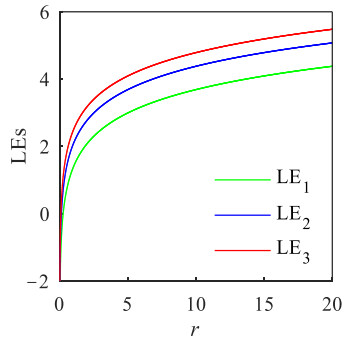
4.1.2　相图

模运算及正弦函数实现了无简并超混沌状态点的运动轨迹折叠,确保了在相空间内全局有界. 当$r=5$时,该混沌不同参数下对应的三维相图如图4所示,可见,混沌吸引子遍布于整个状态变量取值空间,混沌序列具有广泛遍历性.

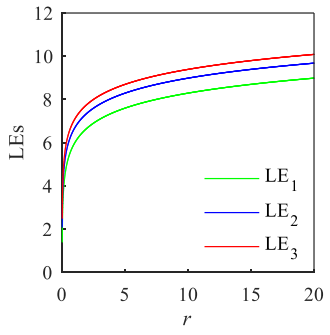
4.1.3　谱熵

谱熵(Spectral Entropy, SE)能够从整体上刻画混沌序列的复杂度,其测度值越高,复杂度越大. 无简并超混沌的谱熵值如图5所示,可见,在控制参数取值内,每条混沌序列均保持了较高的谱熵值,显示出强不可预测性.

进一步对比分析本文所设计的无简并超混沌与文献[24]超混沌的动力学特性,随机选取两个混沌相对应的参数,其中,无简并超混沌的初值$(x_0,y_0,z_0)=(0.8,0.9,1.2)$,控制参数$(a_{11},a_{12},a_{13},a_{22},a_{32},a_{33})=(400,4,4,800,4,1\,200)$,文献[24]中初值$(x_0,y_0,z_0)=(0.8,2.9,4.2)$,控制参数$(a,b,c)=(3,7,11)$. 两个混沌的控制参数$r\in(0,20]$,迭代生成长度为1 000的序列,分别计算每条序列的谱熵及Lyapunov指数平均值,如表1所示,与文献[24]设计的混沌相比,本文设计的混沌x,z序列谱熵平均值略高,对应序列的Lyapunov指数平均值相对较大,表明本文无简并超混沌具有良好的随机性.

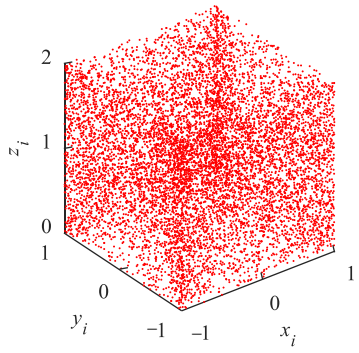


(a) $a_{11}=4, a_{22}=8, a_{33}=12$

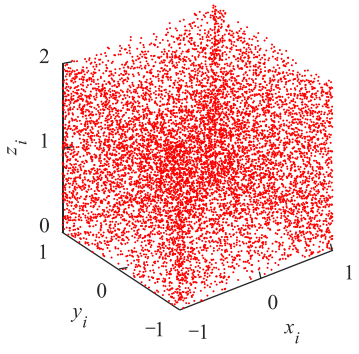


(b) $a_{11}=400, a_{22}=800, a_{33}=1200$

图3 Lyapunov指数



(a) $a_{11}=4, a_{22}=8, a_{33}=12$



(b) $a_{11}=400, a_{22}=800, a_{33}=1200$

图4 相图

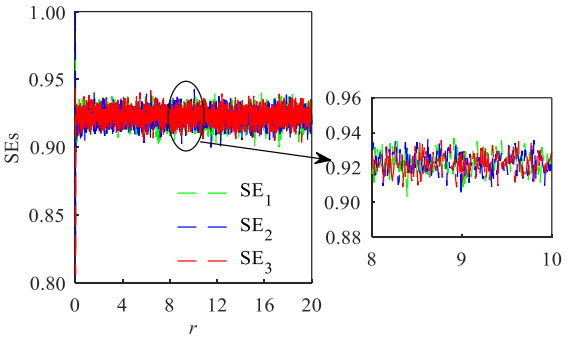


图5 谱熵

表1 混沌性能对比

评价指标	SE			LE		
	x	y	z	x	y	z
本文混沌	0.925 4	0.921 6	0.926 1	7.548 6	8.241 8	8.647 2
文献[24]	0.923 0	0.922 4	0.923 2	7.356 2	7.135 7	6.176 6

4.2 三维星座加密的完全保密性

为便于表述,将三维星座加密公式(13)表示为

$$c=E_{k_e}(m)=m\cdot\boldsymbol{S}\cdot\boldsymbol{Q}=m\cdot\boldsymbol{Z} \tag{21}$$

其对应的通信结构如图6所示,密码原语如下:三维星座点为明文m,所有星座点的集合称为明文空间$\boldsymbol{M}$;变换后的星座点为密文c,所有变换后的星座点集合称为密文空间$\boldsymbol{C}$;可变参数称为加密密钥k_e,数学变换称为加密算法,表示为$c=E_{k_e}(m)$. 加密算法的逆变换称为解密算法,表示为$m=D_{k_d}(c)$,其中k_d是解密时使用的可变参数,称为解密密钥.

相应地,三维星座加密的概率模型如下:(1)三维星座点m是明文空间$\boldsymbol{M}$上服从概率分布$p(m=x)$的一个随机变量;(2)密钥k是密钥空间$\boldsymbol{K}$上服从概率分布$p(k=x)$的一个随机变量;(3)变换后的星座点c是密文空间$\boldsymbol{C}$上服从概率分布$p(c=x)$的一个随机变量.

香农运用信息论原理,给出了密码算法完全性保密的定义.

定义1 一个密码算法是完全保密的,是指明文与密文相互独立,即$\forall a\in\boldsymbol{M},\forall b\in\boldsymbol{C}$,只要$p(m=a)\neq 0$,就有$p(c=b\mid m=a)=p(c=b)$.

定理1 三维星座加密是双射.

证明 首先证明三维星座加密是单射.

假设有两个不同的调制星座点a和b,经过相同的缩放和旋转运算后得到相同的星座点c,设缩放矩阵为$\boldsymbol{S}$,旋转矩阵为$\boldsymbol{Q}$,则:

$$a\cdot\boldsymbol{S}\cdot\boldsymbol{Q}=c \tag{22}$$

$$b\cdot\boldsymbol{S}\cdot\boldsymbol{Q}=c \tag{23}$$

两式相减得:

$$(a-b)\cdot\boldsymbol{S}\cdot\boldsymbol{Q}=0 \tag{24}$$

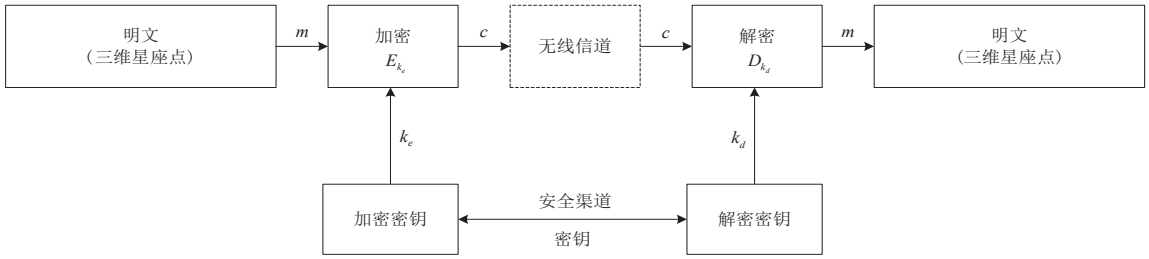


图6　三维星座加密的通信结构

由于缩放因子 $k\neq 0$,则 $\boldsymbol{S}$ 可逆. 同时,旋转角度 $\theta\in(0,\pi]$,$\boldsymbol{Q}$ 也可逆. 因此,$\boldsymbol{S}\cdot\boldsymbol{Q}$ 可逆,则有

$$a-b=0 \tag{25}$$

即 $a=b$,与假设矛盾. 故三维星座置乱加密是单射.

其次,证明三维星座置乱加密是满射,即对于任意密文符号 c,需要找到一个点 a 经过缩放和旋转运算后得到 c.

设 $a=c\cdot\boldsymbol{Q}^{-1}\cdot\boldsymbol{S}^{-1}$,则有

$$\begin{aligned}a\cdot\boldsymbol{S}\cdot\boldsymbol{Q}&=c\cdot\boldsymbol{Q}^{-1}\cdot\boldsymbol{S}^{-1}\cdot\boldsymbol{S}\cdot\boldsymbol{Q}\\&=c\cdot\boldsymbol{Q}^{-1}\cdot\boldsymbol{Q}=cS\end{aligned} \tag{26}$$

故三维星座加密是满射.

综上,三维星座加密既是单射又是满射,即三维星座加密是双射.

定理2　三维星座加密是完全保密的.

证明　设密钥 $\boldsymbol{Z}\in\boldsymbol{K}$,明文 $a\in\boldsymbol{M}$ 对应的密文 $b=E_{k_g}(a)=a\cdot\boldsymbol{Z}$.

根据全概率公式有

$$p(c=b\,|\,m=a)=\sum_{\boldsymbol{D}\in\boldsymbol{K}}p(k=\boldsymbol{D})p(c=b\,|\,m=a,k=\boldsymbol{D}) \tag{27}$$

由定理1可知,三维星座加密是双射,则使用密钥 $\boldsymbol{D}$ 只能将明文 a 唯一地加密成密文 b,且将明文 a 加密成密文 b 的密钥 $\boldsymbol{D}$ 也是唯一的,只能为 $\boldsymbol{Z}$,即

$$p(c=b\,|\,m=a,k=\boldsymbol{D})=1 \tag{28}$$

此外,密钥空间 $\boldsymbol{K}$ 由混沌序列生成的随机矩阵构成,那么密钥在 $\boldsymbol{K}$ 上均匀分布,即

$$p(k=\boldsymbol{Z})=\frac{1}{|\boldsymbol{K}|} \tag{29}$$

其中,$|\boldsymbol{K}|$ 为密钥空间 $\boldsymbol{K}$ 的元素数目. 所以:

$$\begin{aligned}p(c=b\,|\,m=a)&=\sum_{\boldsymbol{D}\in\boldsymbol{K}}p(k=\boldsymbol{D})p(c=b\,|\,m=a,k=\boldsymbol{D})\\&=p(k=\boldsymbol{Z})=\frac{1}{|\boldsymbol{K}|}\end{aligned} \tag{30}$$

另一方面,由全概率公式可得:

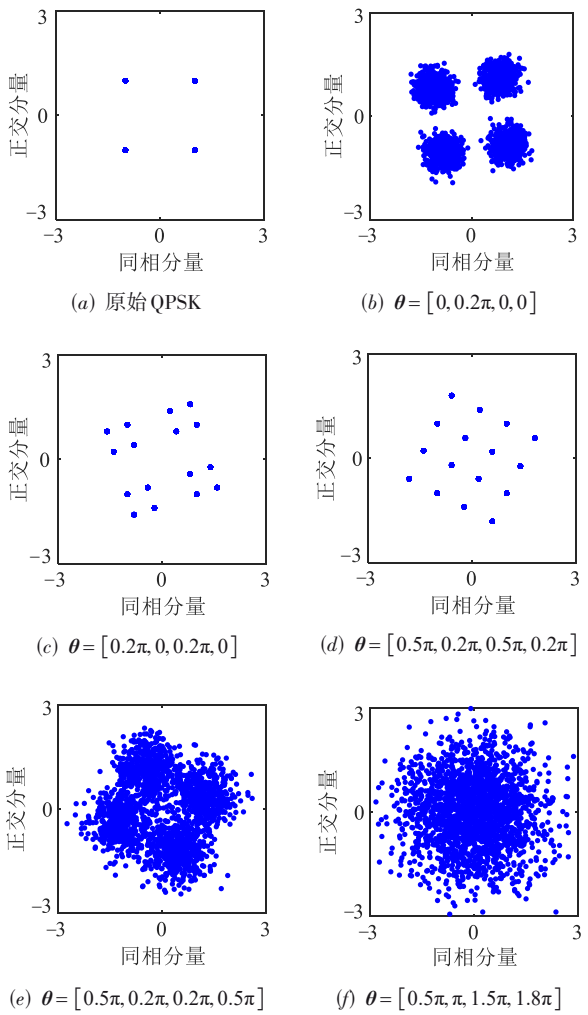
$$\begin{aligned}p(c=b)&=\sum_{a\in\boldsymbol{M}}p(m=a)p(c=b\,|\,m=a)\\&=\sum_{a\in\boldsymbol{M}}p(m=a)p(k=\boldsymbol{Z})\\&=\frac{1}{|\boldsymbol{K}|}\sum_{a\in\boldsymbol{M}}p(m=a)=\frac{1}{|\boldsymbol{K}|}\end{aligned} \tag{31}$$

所以 $p(c=b\,|\,m=a)=p(c=b)$,由定义1可知三维星座加密是完全保密的.

4.3　EWFRFT的保密性

QPSK信号经EWFRFT处理后,星座图如图7所示,可见,随着变换参数的不同,调制信号呈现不同形式的星座图,这将使得非法接收方难以检测到信号.

衡量EWFRFT安全性的另一指标是,当非法接收方已知发送端采用EWFRFT技术但未知具体参数时,



(a) 原始QPSK　(b) $\boldsymbol{\theta}=[0,0.2\pi,0,0]$

(c) $\boldsymbol{\theta}=[0.2\pi,0,0.2\pi,0]$　(d) $\boldsymbol{\theta}=[0.5\pi,0.2\pi,0.5\pi,0.2\pi]$

(e) $\boldsymbol{\theta}=[0.5\pi,0.2\pi,0.2\pi,0.5\pi]$　(f) $\boldsymbol{\theta}=[0.5\pi,\pi,1.5\pi,1.8\pi]$

图7　QPSK信号经EWFRFT处理的星座图

通过参数扫描破解系统的代价较大. 如图8所示,变换参数偏差超过0.1π时,解调的误码率快速上升,说明非法窃听者即使侦测到EWFRFT信号,在变换参数未知的情况下也无法准确解调信号. 然而,EWFRFT的变换参数计算精度不足10^{-2},单纯的EWFRFT系统密钥空间最大为$(10^2)^4=10^8\approx 2^{27}$,无法对抗穷举攻击.

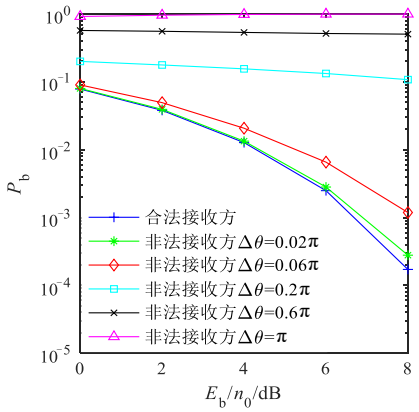


图8 EWFRFT变换参数敏感性分析

4.4 计算复杂度

由于乘法运算直接关联硬件资源消耗与时间成本,因而在密码算法的实现复杂度评估中,通常以乘法运算次数为关键指标. 本文加密方法基于三维星座加密和EWFRFT,主要运算不含高复杂度的循环嵌套. 对于星座点长度为N的调制信号,加密过程需要每个星座点分别与三维缩放矩阵及旋转矩阵执行乘法操作,据此,三维星座加密的复杂度为$o(18N)$. 同时,引用文献[11],EWFRFT的复杂度为$o(N\log N+4N)$. 因此,本文加密方法的时间复杂度为$o(N\log N+22N)$.

5 仿真实验

通过星座加密特性、抗统计攻击、抗穷举攻击、误比特率等仿真评估本文加密方法的安全性和有效性,仿真实验平台如下:CPU Intel Core i3-5005U 4G,GPU NVDIA GeForce 920A 4G,Windows 10家庭版,Matlab R2016. 随机选取混沌状态下的参数进行仿真,如表2所示.

表2 仿真参数

类别	参数
信道类别	AWGN
混沌初值(x_0,y_0,z_0)	(0.8,0.9,1.2)
混沌控制参数$(r,a_{11},a_{12},a_{13},a_{22},a_{32},a_{33})$	(5,400,4,4,800,4,1 200)

5.1 星座加密特性分析

发送信息经三维调制、加密处理的星座图如图9所示. 信息经三维调制后形成规则的星座图,攻击者容易通过比对星座图等手段掌握调制方式,进而为破解系统找到突破口. 但三维星座加密后,无论是4-ray还是8-ray星座图,星座点均随机分布在球体内,再经EWFRFT处理后,信号变得毫无规律,类似随机噪声,这让攻击者难以检测到加密信号,即便侦收到加密信号,也无法从中分析出调制方式,从而显著提升了系统的抗截获能力. 此外,每个星座点有8个相互独立的因素完成三维星座加密,极大增强了加密的灵活性和安全性.

5.2 抗统计攻击分析

基于统计特征的盲信号检测技术广泛应用于调制类型识别,但难以应对高斯或类高斯信号. 分析本文方法加密后信号统计结果,并与瑞利分布、概率密度为1/2π的均匀分布对比,如图10所示,其中,瑞利分布的均值、方差与加密信号复包络的幅度均值、方差相等. 调制信号经本文方法加密后,幅度与瑞利分布吻合,相位分布接近均匀分布,表明能够有效对抗依赖于统计特征的调制识别.

运用图像信息熵定量分析该方法加密信息的统计特性,其计算表达式为

$$H(\boldsymbol{G})=\sum_{i=0}^{2^N-1}p(\boldsymbol{G}_i)\log_2\frac{1}{p(\boldsymbol{G}_i)} \tag{32}$$

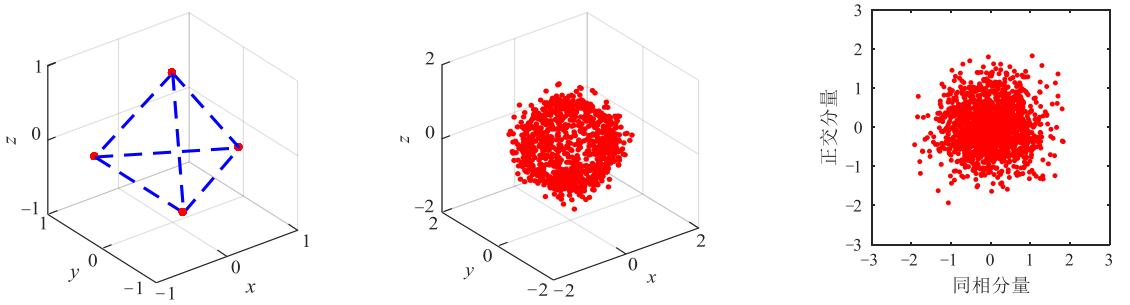
其中,$\boldsymbol{G}$为灰度图像,$p(\boldsymbol{G}_i)$为像素概率分布,N为像素阶数.

采用本文方法分别对三幅大小为256 × 256的Cammera、Peppers、Baboon灰度图像加密,计算加密图像的信息熵,同时与二维星座幅相加密的MPWFRFT安全通信方法[8]、三维星座旋转加密算法[16]、三维星座先绕轴旋转再平移的加密方法[18]及混沌图像加密方法[25]作对比,如表3所示. 本文方法对三幅图像加密后的信息熵均接近理想值8,显著优于文献[16,18]方法,也比部分图像加密方法更优,与文献[8]方法相近.

综上所述,本文加密方法不仅使信号能够成功对抗基于特征参数的调制识别,而且确保了加密信息呈现出优异的随机性分布特性.

5.3 抗穷举攻击分析

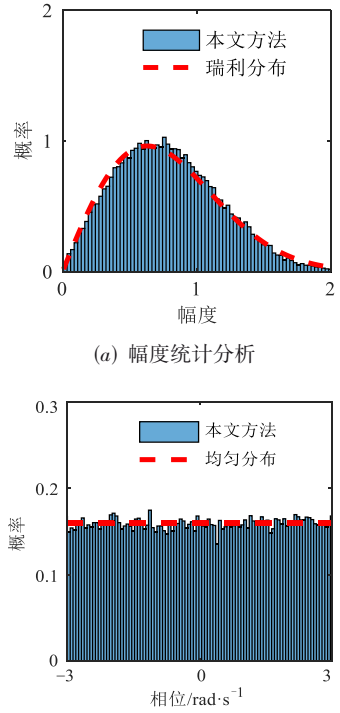
为防止攻击者利用暴力手段破译密码算法,一个良好的加密算法必须具备足够庞大的密钥空间,并对密钥的任何微小变动极为敏感. 本文加密方法的密钥包括无简并超混沌的初值(x_0,y_0,z_0)和控制参数$(r,a_{11},a_{12},a_{13},a_{22},a_{32},a_{33})$,构成复杂,确保了高度的安全性. 逐一分析密钥的敏感性,如图11所示,即便分别使用与正确密钥x_0、y_0偏差10^{-16},z_0、r偏差10^{-15},a_{12}、a_{13}偏差10^{-14},a_{11}、a_{22}、a_{32}偏差10^{-13},a_{33}偏差10^{-12}的密钥去尝试解密同一加密信息,所得的误比特率曲线依然稳定保持在0.5左右,表明攻击者无法从解密结果中获取任何有价值的信息,故本文加密方法的密钥空间为$10^{16}\times10^{16}\times10^{15}\times10^{15}\times10^{13}\times10^{14}\times10^{14}\times10^{13}\times10^{13}\times10^{12}$



(a) 原始4-ray星座图　(b) 三维星座加密图　(c) EWFRFT加密图

(d) 原始8-ray星座图　(e) 三维星座加密图　(f) EWFRFT加密图

图9　星座加密图

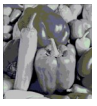


(a) 幅度统计分析

(b) 相位统计分析

图10　加密信号的统计分析

表3　不同加密图像的信息熵

图 像			
本文方法	7.997 2	7.997 3	7.997 1
文献[8]方法	7.997 2	7.997 0	7.997 1
文献[16]方法	7.887 5	7.956 5	7.955 1
文献[18]方法	7.878 5	7.953 8	7.954 9
文献[25]方法	7.994 4	—	—

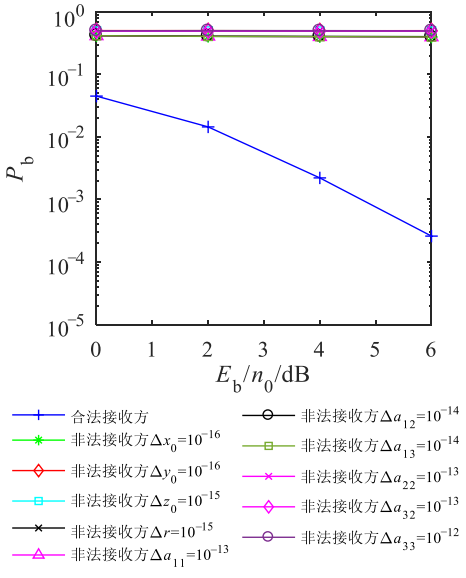


图11　密钥敏感性分析

$=10^{141}\approx 2^{470}$. 而文献[16, 18, 19]的密钥空间分别为10^{133}、1.2×10^{73}、10^{119},均小于本文加密方法. 因此,本文加密方法不仅拥有巨大的密钥空间,且对密钥的变动极为敏感,在现有技术条件下,能够抵御穷举攻击.

5.4 误比特率分析

信号在空间传播时难免受到噪声干扰,在发射相同能量的条件下,由于三维星座的最小欧氏距离更大,解调时更容易区分不同的信号点,有效降低了因噪声干扰而导致的误判概率. 本文方法加密 4-ray、8-ray 三维调制,并与 QPSK、8QAM 的理论误比特率对比,如图 12 所示,在星座点数量相同时,本文加密方法的误比特率低于二维调制,且在相同信噪比时,8-ray 与 QPSK 理论误比特率非常接近.

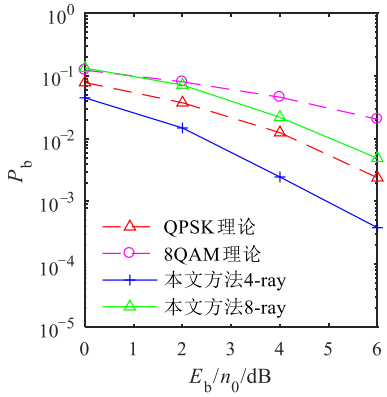


图 12 误比特率分析

6 结束语

本文提出了一种无简并超混沌驱动三维星座加密的 EWFRFT 通信方法. 根据三维星座加密密钥取值需要,构建了一个随机性良好的无简并超混沌,运用其产生的混沌序列分别控制方向矢量、缩放因子及旋转轴、旋转角度,进而生成随机的缩放矩阵、罗德里格斯旋转矩阵,对每个三维星座点实施先缩放再旋转的三维星座加密,证明了该方法具有理论上的完全保密性,同时有 8 个相互独立的因素控制加密,确保了三维星座加密的灵活性. 接着,将加密后的星座点组合为 I/Q 信号,再进行 EWFRFT 加密,进一步扰乱信号分布规律. 仿真结果表明,本文所提方法加密后,扰乱了原本规律分布的星座图,提升了信号的抗截获能力,同时,传输信息呈现随机性分布,能够对抗常见的攻击.

参考文献

[1] JIN L, HU X Y, LOU Y M, et al. Introduction to wireless endogenous security and safety: Problems, attributes, structures and functions[J]. China Communications, 2021, 18(9): 88-99.

[2] DONG H, GAO R B, LI J Z, et al. Physical layer security communication for IOT-aided intelligent transport systems: An approach in WFRFT signal domain[J]. Computers and Electrical Engineering, 2024, 118: 109309.

[3] DONG H, FANG X J, ZHAO J, et al. Secure communication for RSMA systems: Integrating spatial and WFRFT signal domains[J]. IEEE Communications Letters, 2024, 28(11): 2498-2502.

[4] ZHOU Z, LUO J S, WANG S L, et al. Security-enhanced directional modulation based on two-dimensional M-WFRFT[J]. China Communications, 2024, 21(5): 229-248.

[5] 张笑宇, 宋碧雪, 王洋, 等. 基于循环相关的加权分数阶傅里叶变换信号旋转因子估计方法[J]. 兵工学报, 2022, 43(7): 1646-1654.
ZHANG X Y, SONG B X, WANG Y, et al. An estimation method for rotation factor of weighted fractional Fourier transform signals based on cyclic correlation[J]. Acta Armamentarii, 2022, 43(7): 1646-1654. (in Chinese)

[6] LIANG Y, XIANG X, SUN Y, et al. Novel modulation recognition for WFRFT-based system using 4th-order cumulants[J]. IEEE Access, 2019, 7: 86018-86025.

[7] 杨宇晓, 高萍. 多层多参数多项加权分数阶傅里叶变换复合调制通信信号设计方法[J]. 电子与信息学报, 2023, 45(4): 1192-1200.
YANG Y X, GAO P. Design method of multi-layer multi-parameter multi-term weighted-type fractional Fourier transform composite modulation communication Signal[J]. Journal of Electronics and Information Technology, 2023, 45(4): 1192-1200. (in Chinese)

[8] 孟庆微, 王西康, 齐子森, 等. 基于余幂-激活离散超混沌加密的多参数加权分数傅里叶变换安全通信方法[J]. 电子与信息学报, 2023, 45(5): 1688-1696.
MENG Q W, WANG X K, QI Z S, et al. Multiple parameters weighted-type fractional Fourier transform secure communication method based on cosine power-activation discrete hyperchaotic encryption[J]. Journal of Electronics & Information Technology, 2023, 45(5): 1688-1696. (in Chinese)

[9] 达新宇, 翟东, 梁源, 等. 联合多层 WFRFT 与人工噪声的抗截获通信技术[J]. 华中科技大学学报(自然科学版), 2018, 46(10): 86-91.
DA X Y, ZHAI D, LIANG Y, et al. Anti-interception communication technology combining multi-layers WFRFT and artificial noise[J]. Journal of Huazhong University of Science and Technology: Nature Science Edition, 2018, 46(10): 86-91. (in Chinese)

[10] HUANG Y X, SHA X J, FANG X J, et al. Secure spatial modulation based on two-dimensional generalized weighted fractional Fourier transform encryption[J]. Eurasip Journal on Wireless Communications and Networking, 2023, 2023(1): 13.

[11] SONG G, FANG X J, SHA X J. Guaranteeing wireless communication reliability via an extended hybrid carrier system[J]. China Communications, 2023, 20(7): 192-202.

[12] LI W, MCLERNON D, LEI J, et al. Cryptographic primitives

and design frameworks of physical layer encryption for wireless communications[J]. IEEE Access, 2019, 7: 63660-63673.

[13] 鲁信金, 雷菁, 施育鑫. 基于旋转置乱的索引跳频抗干扰加密方法[J]. 通信学报, 2021, 42(12): 27-34.
LU X J, LEI J, SHI Y X. Index modulation aided frequency hopping anti-jamming and encryption method based on rotation scrambling[J]. Journal on Communications, 2021, 42(12): 27-34. (in Chinese)

[14] HU X Y, WAN Z, HUANG K Z, et al. Modulated symbol-based one-time pad secure transmission scheme using physical layer keys[J]. Science China Information Sciences, 2023, 67(1): 112303.

[15] WU T W, ZHANG C F, CHEN C, et al. Security enhancement for OFDM-PON using Brownian motion and chaos in cell[J]. Optics Express, 2018, 26(18): 22857-22865.

[16] ZHANG Y Q, JIANG N, ZHAO A K, et al. Security enhancement in coherent OFDM optical transmission with chaotic three-dimensional constellation scrambling[J]. Journal of Lightwave Technology, 2022, 40(12): 3749-3760.

[17] 于浩洋, 孟庆微, 负彦直, 等. 混沌驱动四元数旋转三维星座加密的WFRFT通信方法[J]. 兵工学报, 2024, 45(8): 2531-2541.
YU H Y, MENG Q W, YUN Y Z, et al. Chaos driven quaternion rotation three-dimensional constellation encryption for WFRFT communication method[J]. Acta Armamentarii, 2024, 45(8): 2531-2541. (in Chinese)

[18] REN J X, LIU B, WU X Y, et al. Security-enhanced 3D-CAP-PON based on two-stage spherical constellation masking[J]. IEEE Access, 2020, 8: 111966-111973.

[19] WU M J, LIU B, REN J X, et al. 3D PCDM probabilistic shaping transmission scheme based on chaotic constellation mapping[J]. IEEE Photonics Journal, 2023, 15(3): 1-7.

[20] CHEN G Y, LIU B, REN J X, et al. Three-dimensional non-orthogonal multiple access high-security seven-core transmission system based on constellation chaotic selection mapping[J]. Journal of Lightwave Technology, 2024, 42(17): 5910-5917.

[21] FLETCHER D, IAN P. 3D Math Primer for Graphics and Game Development[M]. USA: CRC Press, 2011.

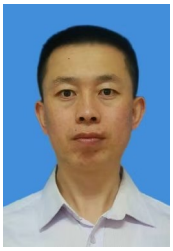
[22] 赵耿, 吴锐, 马英杰, 等. 基于多层元胞自动机的动态随机耦合映像格系统性能分析[J]. 电子学报, 2024, 52(9): 3111-3122.
ZHAO G, WU R, MA Y J, et al. Performance analysis of dynamic random coupled map lattices system based on multilayer elementary cellular automata[J]. Acta Electronica Sinica, 2024, 52(9): 3111-3122. (in Chinese)

[23] 禹思敏, 吕金虎, 李澄清. 混沌密码及其在多媒体保密通信中应用的进展[J]. 电子与信息学报, 2016, 38(3): 735-752.
YU S M, LYU J H, LI C Q. Some progresses of chaotic cipher and its applications in multimedia secure communications[J]. Journal of Electronics & Information Technology, 2016, 38(3): 735-752. (in Chinese)

[24] LIU H J, LIU J, MA C. Construction dynamic strong S-box using 3D chaotic map and application to image encryption[J]. Multimedia Tools and Applications, 2023, 82(16): 23899-23914.

[25] 刘思聪, 李春彪, 李泳新. 基于指数-余弦离散混沌映射的图像加密算法研究[J]. 电子与信息学报, 2022, 44(5): 1754-1762.
LIU S C, LI C B, LI Y X. A novel image encryption algorithm based on exponent-cosine chaotic mapping[J]. Journal of Electronics & Information Technology, 2022, 44(5): 1754-1762. (in Chinese)

作者简介



负彦直　男,1988年出生于甘肃省定西市. 硕士研究生. 主要研究方向为物理层安全、混沌加密.
E-mail: 337949142@qq.com

王　晗　女,1989年出生于陕西省西安市. 博士、讲师. 主要研究方向为通信信号处理、网络层协议.
E-mail: whan@mail.nwpu.edu.cn

孟庆微　男,1980年出生于黑龙江省安达市. 博士、教授. 主要研究方向为物理层安全、通信信号处理.
E-mail: qingw_meng@163.com

马志强　男,1968年出生于山东省威海市. 博士、副教授. 主要研究方向为信息与通信工程.
E-mail: 110558171@qq.com