超混沌驱动对偶四元数置乱三维星座加密的 2D-EWFRFT 通信方法

贠彦直，孟庆微，李嘉悦，王可青，王聃
（空军工程大学信息与导航学院，陕西 西安 710077）

摘要：为提升无线通信信号的安全保密性，提出了一种超混沌驱动对偶四元数置乱三维星座加密的二维扩展加权分数傅里叶变换（2D-EWFRFT）通信方法。以正弦、指数函数为核心变换，构造出一种动力学特性优良的超混沌映射。基于对偶四元数理论，设计了三维星座旋转与平移复合加密算法，有效降低了计算复杂度。构建2D-EWFRFT，多个参数相互作用进一步丰富了信号形式。进而提出了超混沌控制三维调制信号先星座加密再2D-EWFRFT级联加密的方法，弥补了单一星座加密扰乱能力有限和EWFRFT参数敏感性较弱的缺陷。仿真结果表明，所提方法可扰乱调制信号的分布特征，混淆与扩散传输信息，增强了无线通信的安全传输能力。

关键词：物理层安全；三维星座加密；对偶四元数；二维扩展加权分数傅里叶变换；超混沌
中图分类号：TN918.91
文献标志码：A
doi：10.11959/j.issn.1000–436x.TXXB260361

2D-EWFRFT communication method based on hyperchaos-driven dual quaternion scrambling for 3D constellation encryption

Yun Yanzhi, Meng Qingwei, Li Jiayue, Wang Keqing, Wang Dan
Information and Navigation College, Air Force Engineering University, Xi'an 710077, China

Abstract: To enhance the security and confidentiality of wireless communication signals, a novel two dimensional extended weighted fractional Fourier transform (2D-EWFRFT) communication method based on hyperchaos-driven dual quaternion scrambling for 3D constellation encryption was proposed. A hyperchaotic map with superior dynamic performance was constructed by employing the sine and exponential function. On the basis of dual quaternion theory, a 3D constellation encryption algorithm with joint rotation and translation was designed, effectively reducing computational complexity. The 2D-EWFRFT was constructed, where the interaction of multiple transform parameters further enriched signal forms. Furthermore, a cascade encryption strategy controlled by hyperchaos was presented, in which the 3D modulated signal was first encrypted via constellation scrambling and then processed by 2D-EWFRFT. The limitations of insufficient scrambling in single constellation encryption and weak parameter sensitivity of the conventional EWFRFT were overcome. Simulation results demonstrate that the proposed method can disrupt the distribution characteristics of modulated signals, scramble and diffuse the transmitted information, and enhance the secure transmission capability of wireless communications.

Key words: physical layer security, 3D constellation encryption, dual quaternion, 2D-EWFRFT, hyperchaos

收稿日期：2026–06–19；**修回日期：**2026–08–12
通信作者：王可青，372661139@qq.com
基金项目：国家自然科学基金资助项目（No.62301599）
Foundation Item：The National Natural Science Foundation of China (No.62301599)

0　引言

随着无线通信技术的广泛应用，工业控制、物联网、智慧医疗等重要敏感数据经开放信道传输，易遭受信号窃听与非法截获。传统上层密码技术可实现信息比特的安全防护，但无法对信号调制特征实施保护，易被窃听者利用实施攻击。融合密码学与信号处理技术的物理层调制加密，通过扰动调制信号底层特征消除信号可识别性，实现信号抗截获和信息防破解的主动防御，为构建端到端无线安全传输链路提供新方案，已成为近年来无线安全领域的研究热点[1]。

在信号处理领域，加权分数傅里叶变换（weighted fractional Fourier transform, WFRFT）凭借时频域变换特性与阶数自由度，可实现信号伪装与高斯化传输，降低被截获和检测的概率[2-3]。已有研究通过多层变换[4]、二维扩展[5]等方式拓展WFRFT系统处理结构，多维参数相互作用不断丰富WFRFT的信号形式。与此同时，许多研究将WFRFT与人工噪声[6]、直扩通信[7]、星座加密[8]等技术融合，进一步提升了信号的抗侦测能力。然而，WFRFT受固有周期特性与单一阶数限制，易被特征识别与破解[9-10]。为此，文献[11]从通信信号处理的变换可逆性与系统信噪比不降低的基本要求出发，将传统单一变换阶数推广至4个独立参数，提出了扩展WFRFT（extended WFRFT, EWFRFT）。EWFRFT虽提升了信号设计的灵活性，但参数敏感性偏低的问题仍制约着其抗参数扫描攻击性能。因此，重构EWFRFT的二维变换结构[12]，并与星座加密协同，成为突破单一变换安全瓶颈的重要方向，也是本文研究的基本出发点。

星座加密通过对星座点实施旋转、平移等变换，扰乱原有分布规律，增强了信号的安全传输能力[13]。根据星座结构，可将其分为二维星座加密[14-15]与三维星座加密[16-18]两类，其中，三维星座加密不仅具备优良的频谱效率，而且加密更具灵活性，成为近年来的研究热点。现有三维星座加密方案多采用绕坐标轴旋转或四元数旋转实现星座置乱，但绕坐标轴旋转需要3次矩阵乘法，计算复杂度高，且旋转加密仅由3个旋转角度控制，自由度受限。部分研究尝试引入平移操作，实施旋转与平移两步操作构建了复合变换[19-21]，但仅有4个参数控制星座加密，仍未解决星座加密复杂度高和加密不充分的问题。从几何角度来看，三维星座加密的本质是在欧氏空间内对星座符号的可控刚体运动。因此，构建既高效又灵活自由的三维运动模型，提升星座加密的抗破解能力，是本文的核心研究对象。

序列密码依托移位寄存器电路产生伪随机序列以构造数据加解密密钥，实现比特级数据置乱。但该类伪随机序列存在线性结构缺陷，攻击者可截获部分序列重构密钥。混沌系统具备初值与参数敏感性，微小初始偏差将生成完全不同的序列，难以逆向预测。因此，在星座加密实现过程中，常利用混沌系统迭代生成混沌序列，驱动星座点实施空间变换[22]。然而，低维混沌系统普遍存在动力学退化问题，难以满足高安全场景的应用需求[23]。为此，构建性能优良的新型混沌映射成为混沌密码学的研究重点。已有研究通过低维混沌耦合[24]、时空动态扰动[25]、引入非线性变换[26]等方式构造混沌系统，有效增强了混沌动力学特性，为混沌密码学的发展提供了新的支撑。

针对现有三维星座加密算法计算复杂度高、EWFRFT参数敏感性低的不足，本文采用多级联架构实现优势互补，提出了一种超混沌驱动对偶四元数置乱三维星座加密的二维EWFRFT（two dimensional EWFRFT, 2D-EWFRFT）通信方法。首先，按照星座加密密钥取值范围，以正弦函数为核心非线性变换，并引入指数项扰动混沌迭代过程，构建了三维sine-exponent（three dimensional sine-exponent, 3D-SEXP）超混沌映射。其次，基于对偶四元数设计了7个参数协调控制的三维星座旋转与平移复合加密算法，在有效降低星座加密复杂度的同时，提升了星座加密的安全性。最后，构造了2D-EWFRFT变换结构，并与三维星座加密相融合，形成了星座加密与变换域安全的级联方法。在该方法中，超混沌迭代生成混沌序列，为星座加密和EWFRFT处理提供随机参数；对偶四元数实现三维星座一体化置乱；2D-EWFRFT完成信号域二次扰乱。各模块各司其职，能够在可控计算开销下弥补单一加密方法的固有缺陷，有效改善了单一星座加密置乱效果有限和EWFRFT抗参数扫描攻击不足的缺陷，显著提升了无线通信系统的抗截获与抗破解能力。

1 问题的提出

1.1 基于对偶四元数的三维星座加密

三维星座加密是由密钥控制三维星座符号旋转、平移等置乱的加密技术，其过程类似于刚体运动，其中一般性刚体运动包括一个绕某个轴的旋转和一个沿相同轴的平移。对偶四元数是刻画一般性刚体运动的最简洁和最有效的数学工具。为此，本文运用其构建了三维星座加密算法。

对偶四元数是元素为四元数的对偶数，其一般形式为：

$$\hat{\boldsymbol{q}} = \dot{\boldsymbol{q}}_r + \varepsilon\dot{\boldsymbol{q}}_d \tag{1}$$

其中，$\boldsymbol{q}_r$和$\boldsymbol{q}_d$分别为对偶四元数的原部和对偶部，ε为对偶单元，满足$\varepsilon \neq 0$且$\varepsilon^2 = 0$。对偶四元数的乘法及共轭运算规则如下。

对偶四元数的乘法运算形式为：

$$\hat{\boldsymbol{q}}_1 \circ \hat{\boldsymbol{q}}_2 = \dot{\boldsymbol{q}}_{r1}\odot\dot{\boldsymbol{q}}_{r2} + \varepsilon(\dot{\boldsymbol{q}}_{r1}\odot\dot{\boldsymbol{q}}_{d2} + \dot{\boldsymbol{q}}_{d1}\odot\dot{\boldsymbol{q}}_{r2}) \tag{2}$$

其中，$\odot$表示四元数的乘法运算，其规则为：

$$\dot{\boldsymbol{q}}_1\odot\dot{\boldsymbol{q}}_2 = \begin{bmatrix} h_1h_2 - w_{1x}w_{2x} - w_{1y}w_{2y} - w_{1z}w_{2z} \\ h_1w_{2x} + h_2w_{1x} + w_{1y}w_{2z} - w_{2y}w_{1z} \\ h_1w_{2y} - w_{1x}w_{2z} + h_2w_{1y} + w_{2x}w_{1z} \\ h_1w_{2z} + w_{1x}w_{2y} - w_{2x}w_{1y} + h_2w_{1z} \end{bmatrix}^{\mathrm{T}} \tag{3}$$

其中，$\dot{\boldsymbol{q}}_1 = [h_1,\boldsymbol{w}_1]$和$\dot{\boldsymbol{q}}_2 = [h_2,\boldsymbol{w}_2]$分别为四元数；$h_1,h_2 \in \mathbb{R}$为实部，$\boldsymbol{w}_1 = [w_{1x},w_{1y},w_{1z}] \in \mathbb{R}^3$和$\boldsymbol{w}_2 = [w_{2x},w_{2y},w_{2z}] \in \mathbb{R}^3$为虚部向量。

对偶四元数共轭是同时对原部、对偶部四元数取共轭，并对ε取反，即：

$$\hat{\boldsymbol{q}}^* = \dot{\boldsymbol{q}}_r^* - \varepsilon\dot{\boldsymbol{q}}_d^* \tag{4}$$

其中，$\dot{\boldsymbol{q}}^* = [h,-\boldsymbol{w}]$表示四元数共轭，满足归一化约束$\hat{\boldsymbol{q}} \circ \hat{\boldsymbol{q}}^* = 1 + 0\varepsilon$的对偶四元数为单位对偶四元数，用于表征一般性刚体运动。

在三维空间中，设初始点$\boldsymbol{v} = (\boldsymbol{v}_x,\boldsymbol{v}_y,\boldsymbol{v}_z)$绕单位轴$\boldsymbol{k} = (\boldsymbol{k}_x,\boldsymbol{k}_y,\boldsymbol{k}_z)$旋转角度$\alpha$，并沿该轴平移向量$\boldsymbol{t} = (\boldsymbol{t}_x,\boldsymbol{t}_y,\boldsymbol{t}_z)$，得到目标点$\boldsymbol{p} = (\boldsymbol{p}_x,\boldsymbol{p}_y,\boldsymbol{p}_z)$，可由对偶四元数实现该过程，具体如下。

首先，构造一般性刚体运动的变换对偶四元数$\hat{\boldsymbol{q}} = \dot{\boldsymbol{q}}_r + \varepsilon\dot{\boldsymbol{q}}_d$。

$$\dot{\boldsymbol{q}}_r = [\cos\frac{\alpha}{2},\boldsymbol{k}\sin\frac{\alpha}{2}] \tag{5}$$

$$\dot{\boldsymbol{q}}_d = \frac{1}{2}\dot{\boldsymbol{t}}_q\odot\dot{\boldsymbol{q}}_r \tag{6}$$

其中，$\dot{\boldsymbol{q}}_r$为旋转分量，需单位化；$\dot{\boldsymbol{t}}_q = [0,\boldsymbol{t}]$为平移分量的纯四元数。

其次，将点拓展为点对偶四元数$\hat{\boldsymbol{v}} = 1 + \varepsilon\dot{\boldsymbol{v}}_q$，其中$\dot{\boldsymbol{v}}_q = [0,\boldsymbol{v}]$。

最后，经单位对偶四元数$\hat{\boldsymbol{q}}$变换后，得到目标点$\boldsymbol{p}$为：

$$\boldsymbol{p} = \mathcal{D}(\hat{\boldsymbol{q}} \circ \hat{\boldsymbol{v}} \circ \hat{\boldsymbol{q}}^*) \tag{7}$$

其中，$\mathcal{D}(\cdot)$为对偶四元数的对偶部提取算子。

在设计三维星座加密算法时，还要考虑到解密算法易于实现，即由点$\boldsymbol{p}$恢复至初始点$\boldsymbol{v}$，其过程为：

$$\boldsymbol{v} = \mathcal{D}(\hat{\boldsymbol{q}}_{\mathrm{inv}} \circ \hat{\boldsymbol{p}} \circ \hat{\boldsymbol{q}}_{\mathrm{inv}}^*) \tag{8}$$

其中，$\hat{\boldsymbol{q}}_{\mathrm{inv}} = \dot{\boldsymbol{q}}_r^* - \varepsilon\frac{1}{2}\dot{\boldsymbol{q}}_r^*\odot\dot{\boldsymbol{t}}_q$为逆变换对偶四元数；$\hat{\boldsymbol{p}} = 1 + \varepsilon\dot{\boldsymbol{p}}_q$，$\dot{\boldsymbol{p}}_q = [0,\boldsymbol{p}]$。

综上所述，现有三维星座旋转加密仅配置3个角度控制参数，可调自由度受限，且绕坐标轴旋转需要3次矩阵乘法，计算复杂度较高。旋转与平移分步式复合变换虽引入平移运算进行改进，但仅拥有4个独立参数，扰动形式拓展程度有限，分离式运算也难以消除计算冗余。对偶四元数表示一般性刚体运动可将旋转和平移统一为单一代数结构，仅存储旋转轴、旋转角度及平移矢量7个标量。当将其应用于星座加密时，相较于现有方法，更多独立参数能够构造多样化星座扰动，保障加密灵活性，旋转与平移一体化运算省去了分步变换流程，有效降低了计算复杂度。后续将通过复杂度分析与仿真实验，验证该方法的综合性能。

1.2 2D-EWFRFT

离散信号$\boldsymbol{X} = [x_1,x_2,\cdots,x_m]$的EWFRFT定义为：

$$\mathcal{F}_E^{\boldsymbol{\theta}}[\boldsymbol{X}] = w_0(\boldsymbol{\theta})\boldsymbol{X} + w_1(\boldsymbol{\theta})\boldsymbol{X}_1 + w_2(\boldsymbol{\theta})\boldsymbol{X}_2 + w_3(\boldsymbol{\theta})\boldsymbol{X}_3 \tag{9}$$

其中，$\boldsymbol{X}_j$为$\boldsymbol{X}$的第j次离散傅里叶变换，$j = 1,2,3$；$\boldsymbol{\theta} = [\theta_0,\theta_1,\theta_2,\theta_3]$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。

$$w_n(\boldsymbol{\theta}) = \frac{1}{4}\sum_{p=0}^{3}\exp\left[\left(\theta_p - \frac{2\pi}{4}np\right)\mathrm{i}\right],n = 0,1,2,3 \tag{10}$$

其中，i为虚数单位。

EWFRFT逆变换为：

$$\mathcal{F}_E^{-\boldsymbol{\theta}}[\boldsymbol{X}] = w_0(-\boldsymbol{\theta})\boldsymbol{X} + w_1(-\boldsymbol{\theta})\boldsymbol{X}_1 + w_2(-\boldsymbol{\theta})\boldsymbol{X}_2 + w_3(-\boldsymbol{\theta})\boldsymbol{X}_3 \tag{11}$$

为进一步提升EWFRFT的参数抗破解能力，文献[12]提出了2D-EWFRFT，其是指将长度为lm的一维调制信号转化成$l \times m$的二维信号矩阵$\boldsymbol{S}$，之后对每行数据进行m点的EWFRFT处理生成行变换信号矩阵$\boldsymbol{P}$，再对矩阵$\boldsymbol{P}$的每列数据进行l点的EWFRFT处理生成最终的变换矩阵$\boldsymbol{Q}$，其中行和列变换参数分别为$\vec{\boldsymbol{\theta}} = \{\boldsymbol{\theta}_1, \boldsymbol{\theta}_2, \cdots, \boldsymbol{\theta}_l\}$和$\vec{\boldsymbol{\eta}} = \{\boldsymbol{\eta}_1, \boldsymbol{\eta}_2, \cdots, \boldsymbol{\eta}_m\}$。其逆变换是将接收信号转化为$l \times m$的二维信号矩阵$\boldsymbol{R}$，之后对每列数据进行$l$点的EWFRFT逆变换，再对列变换矩阵的每行数据进行m点的EWFRFT逆变换。不难看出，将EWFRFT拓展至二维结构后，可在横向与纵向两个维度分别配置相互独立的变换参数，增强系统对抗暴力破解的能力，进一步拓展了加权分数变换理论在信息安全领域的应用。

2　三维星座加密的2D-EWFRFT通信方法

本文提出了一种超混沌驱动对偶四元数置乱三维星座加密的2D-EWFRFT通信方法，其通信模型如图1所示，采用单发单收（single-input single-output, SISO）方法配置。该方法首先构建超混沌映射，通过超混沌迭代生成混沌序列，实现对三维星座点的加密控制。待发送信息经三维调制后形成原始星座点，再利用对偶四元数对每个星座点执行置乱加密。将加密后的星座点组合为I/Q信号并转换为二维矩阵，依次经过2D-EWFRFT、并串转换、添加循环前缀（cyclic prefix, CP）等处理后，由无线信道完成传输。接收方执行与发送方相反的过程，依次去除CP、串并转换、2D-EWFRFT逆变换、三维星座解密、三维解调等，合法接收方凭借共享密钥可准确恢复出原始信息。

2.1　密钥生成

本文运用正弦和指数函数构建一个三维超混沌映射，迭代生成混沌序列直接作为数据加密密钥，驱动三维星座点实施空间变换。该混沌映射简称3D-SEXP，其差分方程组为：

$$\begin{cases} x_{i+1} = \sin\left(2^a\left(r + x_i^2 + y_i^2\right)\right) \\ y_{i+1} = \sin\left(2^b\left(r + y_i^2 + z_i^2\right)\right) \\ z_{i+1} = \sin\left(2^c\left(r + x_i^2 + z_i^2\right)\right) \end{cases} \tag{12}$$

其中，状态变量$x_i, y_i, z_i \in [-1,1]$；控制参数$r \in (0,+\infty)$，$a,b,c \in [3,+\infty)$且$a \neq b \neq c$。该映射以正弦函数为核心非线性变换，将相空间中发散的状态轨迹反复折叠至有界区间，形成复杂缠绕的混沌吸引子，同时引入指数项对迭代自变量进行放大，使初始值或迭代过程中的微小误差呈指数级增长，加速相邻轨道分离，有效提升了系统初值敏感性。

2.2　加密方法

本文提出的加密方法具体如下。

步骤1　明文信息经三维调制后，在星座图中形成N_s个原始星座点，其中第i个星座点M_i的坐标为(x_i, y_i, z_i)，则明文信号$\boldsymbol{M}$可表示为：

$$\boldsymbol{M} = \begin{pmatrix} x_1 & y_1 & z_1 \\ x_2 & y_2 & z_2 \\ \vdots & \vdots & \vdots \\ x_{N_S} & y_{N_S} & z_{N_S} \end{pmatrix} \tag{13}$$

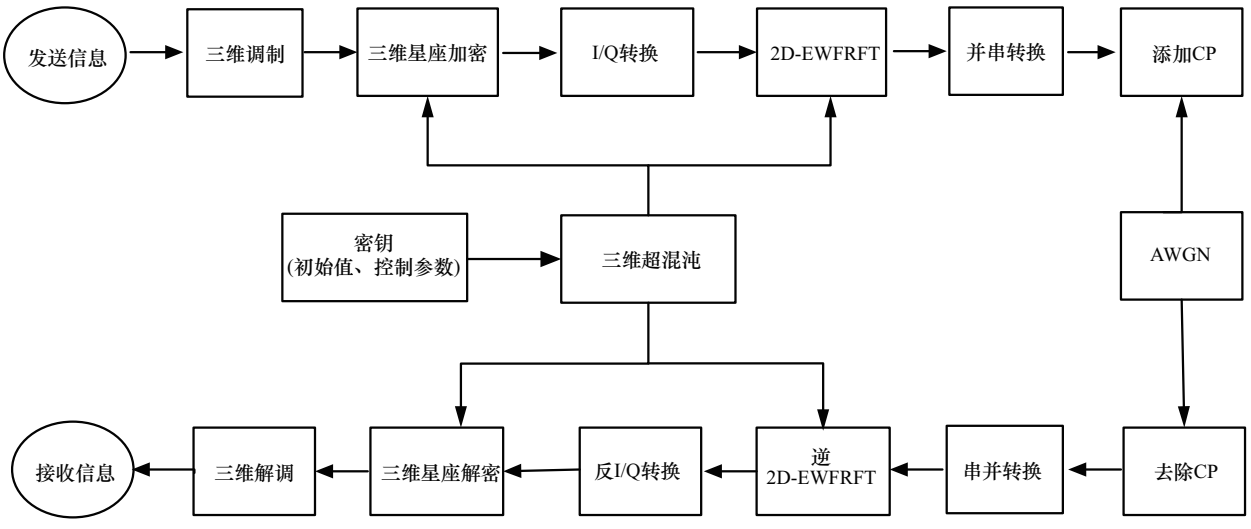


图1　三维星座加密的2D-EWFRFT通信模型

步骤2 设混沌映射3D-SEXP的初值为(x_0,y_0,z_0)，控制参数为(r,a,b,c)，式(12)迭代$2N_s$次生成3条序列$\boldsymbol{x},\boldsymbol{y},\boldsymbol{z}$，选取序列$\boldsymbol{x},\boldsymbol{y}$中的值构造$N_s$个随机平移矢量，其中第$i$个平移矢量$\boldsymbol{p}_i$的坐标$\left(\boldsymbol{p}_{ix},\boldsymbol{p}_{iy},\boldsymbol{p}_{iz}\right)$为：

$$\begin{cases}\boldsymbol{p}_{ix}=(\rho_1-\rho_2)\sin(\pi\boldsymbol{x}_i)\sin(\pi\boldsymbol{y}_i)\\ \boldsymbol{p}_{iy}=(\rho_1-\rho_2)\sin(\pi\boldsymbol{x}_i)\cos(\pi\boldsymbol{y}_i)\\ \boldsymbol{p}_{iz}=(\rho_1-\rho_2)\cos(\pi\boldsymbol{x}_i)\end{cases}\tag{14}$$

选取序列$\boldsymbol{x},\boldsymbol{y},\boldsymbol{z}$中的值作为随机旋转轴和旋转角度，其中第$i$个旋转轴和旋转角度分别为$\boldsymbol{k}_i,\alpha_i$。$\boldsymbol{k}_i$的坐标$\left(\boldsymbol{k}_{ix},\boldsymbol{k}_{iy},\boldsymbol{k}_{iz}\right)$为：

$$\begin{cases}\boldsymbol{k}_{ix}=\boldsymbol{x}_{i+N_S}\\ \boldsymbol{k}_{iy}=\boldsymbol{y}_{i+N_S}\\ \boldsymbol{k}_{iz}=\boldsymbol{z}_{i+N_S}\\ \alpha_i=\boldsymbol{z}_i\times\pi\end{cases}\tag{15}$$

根据式(5)和式(6)将平移矢量、旋转轴和旋转角度构造成N_s个变换对偶四元数，其中第i个变换对偶四元数为$\hat{\boldsymbol{T}}_i$。

步骤3 运用对偶四元数对每个星座点进行置乱加密。星座点M_i转换为对偶四元数$\hat{M}_i=1+\varepsilon\dot{M}_q$，其中$\dot{M}_q=[0,x_i,y_i,z_i]$，则第$i$个星座加密点$M_i'$为：

$$M_i'=\mathcal{D}(\hat{\boldsymbol{T}}_i\circ\hat{M}_i\circ\hat{\boldsymbol{T}}_i^{*})\tag{16}$$

即得星座加密信号$\boldsymbol{M}'$。

$$\boldsymbol{M}'=\begin{pmatrix}x_1' & y_1' & z_1'\\ x_2' & y_2' & z_2'\\ \vdots & \vdots & \vdots\\ x_{N_s}' & y_{N_s}' & z_{N_s}'\end{pmatrix}\tag{17}$$

步骤4 依据式(18)将星座加密信号$\boldsymbol{M}'$转换为I/Q信号。

$$\boldsymbol{M}''=\begin{pmatrix}x_1'+\mathrm{i}y_1'\\ z_1'+\mathrm{i}x_2'\\ y_2'+\mathrm{i}z_2'\\ \vdots\\ z_{N_s-1}'+\mathrm{i}x_{N_s}'\\ y_{N_s}'+\mathrm{i}z_{N_s}'\end{pmatrix}^{\mathrm{T}}\tag{18}$$

步骤5 将信号$\boldsymbol{M}''$转换成$l\times m$的二维信号矩阵，并对其进行2D-EWFRFT加密，其中行和列变换参数$\boldsymbol{\theta}=\{\boldsymbol{\theta}_1,\boldsymbol{\theta}_2,\cdots,\boldsymbol{\theta}_l\}$和$\boldsymbol{\eta}=\{\boldsymbol{\eta}_1,\boldsymbol{\eta}_2,\cdots,\boldsymbol{\eta}_m\}$由序列$\boldsymbol{z}$的值乘以π得到，则加密信号$\boldsymbol{M}'''$为：

$$\boldsymbol{M}'''=\text{2D-EWFRFT}\{\boldsymbol{M}'',\boldsymbol{\theta},\boldsymbol{\eta}\}\tag{19}$$

加密信号经并串转换、添加CP等后由无线信道发送。

为清晰描述该加密方法的执行流程，给出超混沌驱动对偶四元数置乱三维星座加密的2D-EWFRFT通信方法的伪代码，如算法1所示。

算法1 加密方法

输入 明文信号$\boldsymbol{M}$，密钥(x_0,y_0,z_0,r,a,b,c)，平移量(ρ_1,ρ_2)，二维信号矩阵行数l、列数m

输出 加密信号$\boldsymbol{M}'''$

1) for i=1:1:$2N_s$
2) 根据式(12)生成混沌序列$\boldsymbol{x},\boldsymbol{y},\boldsymbol{z}$
3) end for
4) for i=1:1:N_s
5) 根据式(14)和式(15)随机化旋转轴、旋转角度及平移矢量，其中旋转轴、平移矢量各3个参数，旋转角度1个参数，共7个参数
6) 按照对偶四元数运算规则编写星座点变换函数，根据式(16)调用函数对每个星座点加密，该函数输入为单个明文星座点及步骤5)的随机参数，输出为星座加密信号$\boldsymbol{M}'$
7) end for
8) 根据式(18)将星座加密信号$\boldsymbol{M}'$转换为I/Q信号$\boldsymbol{M}''$
9) 将信号$\boldsymbol{M}''$转换成$l\times m$的二维信号矩阵，行和列数据分别进行EWFRFT处理

2.3 解密方法

该方法对应的解密步骤如下。

步骤1 接收方依托双方共享的密钥迭代生成3D-SEXP混沌序列，再遵循与发送方相同的步骤，构建逆变换对偶四元数并完成2D-EWFRFT参数的选取。

步骤2 将接收信号$\boldsymbol{R}$转化为$l\times m$的二维信号矩阵并进行逆2D-EWFRFT，得到待解密信号$\boldsymbol{R}'$为：

$$\boldsymbol{R}'=\text{2D-EWFRFT}\{\boldsymbol{R},-\boldsymbol{\eta},-\boldsymbol{\theta}\}\tag{20}$$

步骤3 分离$\boldsymbol{R}'$的实部和虚部，转换为同式(17)的待解密星座信号，并对每个星座点进行解密。

$$R_i''=\mathcal{D}(\hat{\boldsymbol{T}}_{i\,\mathrm{inv}}\circ\hat{R}'_i\circ\hat{\boldsymbol{T}}^{*}_{i\,\mathrm{inv}}) \tag{21}$$

其中，R_i''为第i个三维星座解密点，$\hat{R}'_i$为第i个待解密三维星座点对偶四元数，$\hat{\boldsymbol{T}}_{i\,\mathrm{inv}}$为第$i$个逆对偶四元数。

步骤4　测算解密星座点R_i''同原始星座图上所有星座点的欧氏距离，依照三维星座映射规则，将距离最短的星座点对应恢复为接收信息。

解密方法伪代码如算法2所示。

算法2　解密方法

输入　密文信号$\boldsymbol{R}$，密钥(x_0,y_0,z_0,r,a,b,c)，平移量(ρ_1,ρ_2)，二维信号矩阵行数l、列数m

输出　接收信息

1) for i=1:1:2N_s
2)　根据式(12)生成混沌序列$\boldsymbol{x},\boldsymbol{y},\boldsymbol{z}$
3) end for
4) 将信号$\boldsymbol{R}$转换成$l\times m$的二维信号矩阵，列和行数据分别进行EWFRFT逆变换，得到$\boldsymbol{R}'$
5) 分离$\boldsymbol{R}'$的实部和虚部
6) for i=1:1:N_s
7)　根据式(14)和式(15)随机化旋转轴、旋转角度及平移矢量
8)　按照对偶四元数运算规则编写星座点变换逆函数，根据式(21)调用函数对每个星座点解密，该函数输入为待解密星座点及步骤7)的随机参数，输出为星座解密信号$\boldsymbol{R}''$
9)　三维星座解调
10) end for

3　性能分析

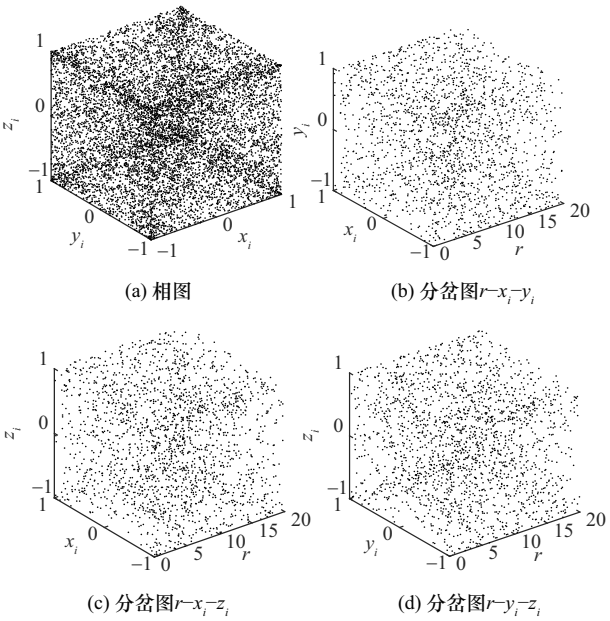
本文构建了新型超混沌及2D-EWFRFT，设计了三维星座加密算法。为此，本节将重点对各自的性能展开分析。

3.1　3D-SEXP混沌的动力学特性

非线性系统的混沌特性分析是混沌动力学研究的重要内容，采用分岔图、相图、Lyapunov指数（Lyapunov exponent, LE）、近似熵（approximate entropy, ApEN）、谱熵（spectral entropy, SE）等分析刻画3D-SEXP混沌的动力学特性，实验中混沌初值(x_0,y_0,z_0)取值为（0.3,−0.2,0.8），方程系数(a,b,c)取值为(9,6,12)，r固定取值时为7，生成的每条混沌序列长度为1 000。

3.1.1　分岔图和相图

3D-SEXP映射的三维相图如图2(a)所示，混沌吸引子以弥散点集形式填充整个相空间，这一特征反映出混沌序列在取值空间内具备良好的遍历性。图2(b)~图2(d)为3D-SEXP映射随控制参数r变化的分岔图，3组状态变量对应的分岔点集均覆盖整个取值空间，表明系统在不同控制参数下演化路径与状态序列具备高度的非周期性与类随机特性。



(a) 相图　(b) 分岔图r–x_i–y_i　(c) 分岔图r–x_i–z_i　(d) 分岔图r–y_i–z_i

图2　3D-SEXP的相图和分岔图

3.1.2　Lyapunov指数

Lyapunov指数是量化表征动力系统混沌与超混沌特性的核心指标，其数值大小与符号直接反映系统轨迹演化行为，数值越大，表明系统对初始条件的微小变化越敏感，相空间轨迹越复杂。两个及以上正LE为超混沌的关键判定依据。针对3D-SEXP映射，其雅可比矩阵$\boldsymbol{J}$为：

$$\boldsymbol{J}=\begin{bmatrix}2^{a+1}x_i\cos\left(2^a(r+x_i^2+y_i^2)\right) & 2^{a+1}y_i\cos\left(2^a(r+x_i^2+y_i^2)\right) & 0\\ 0 & 2^{b+1}y_i\cos\left(2^b(r+y_i^2+z_i^2)\right) & 2^{b+1}z_i\cos\left(2^b(r+y_i^2+z_i^2)\right)\\ 2^{c+1}x_i\cos\left(2^c(r+x_i^2+z_i^2)\right) & 0 & 2^{c+1}z_i\cos\left(2^c(r+x_i^2+z_i^2)\right)\end{bmatrix} \tag{22}$$

通过QR正交分解算法求解不同控制参数r下的LE值。由图3中LE演化曲线可知，3条LE序列值均保持非负且稳定，说明系统在演化过程中不存在收缩方向，相空间轨迹演化呈现拉伸与折叠的演化特征，该映射表现出复杂的动力学行为，属于超混沌系统。

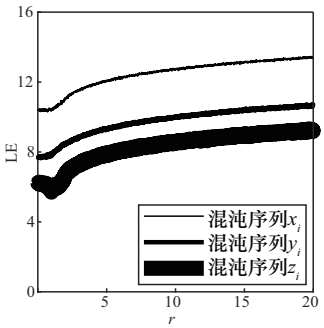


图3 Lyapunov指数

3.1.3 谱熵

作为评估混沌系统结构复杂度的重要指标，SE的大小能够直接反映混沌序列的不规则特性，其数值越高，表示系统的随机特征与不可预测性越显著。计算3D-SEXP的3组状态序列在不同控制参数r下的SE值，如图4所示，平均值分别为0.938 3、0.938 1和0.938 4，表明该混沌映射整体复杂度较高。

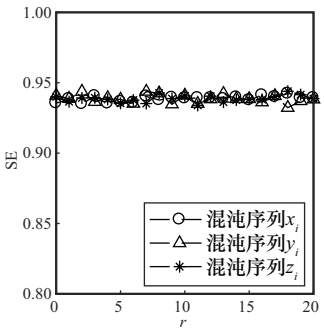


图4 谱熵

3.1.4 近似熵

ApEN作为一种常用的复杂度量化手段，可以有效表征混沌序列的动态不规则性，ApEN值越大，复杂度越高。在不同控制参数下，对3D-SEXP进行ApEN分析，计算时序列长度设定为600，嵌入维数为1，相似容限度为序列标准差的0.2倍，如图5所示，各序列ApEN平均值依次为2.185 3、2.182 0和2.178 6；同时，随控制参数r的增大，ApEN在均值附近小幅度波动，充分说明构造的混沌序列具有稳定和优异的复杂性与随机性。

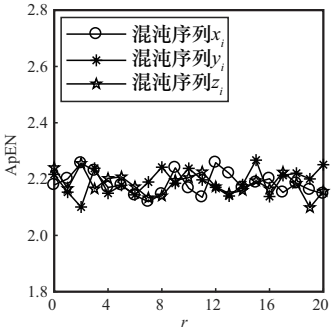


图5 近似熵

3.2 三维星座加密的安全性

星座加密使星座符号具备混淆与扩散特性。为定量刻画加密后星座符号的无序程度，本文在二维星座信息熵[13]的基础上，提出了三维星座信息熵的定义，其数学表达式为：

$$H(\Delta)=-\sum_{i=-\infty}^{\infty}\sum_{j=-\infty}^{\infty}\sum_{k=-\infty}^{\infty}\Gamma(i,j,k)\mathrm{lb}\,\Gamma(i,j,k) \quad (23)$$

其中，$\Gamma(i,j,k)=\int_{i\Delta}^{(i+1)\Delta}\int_{j\Delta}^{(j+1)\Delta}\int_{j\Delta}^{(j+1)\Delta}p(x,y,z)\mathrm{d}x\mathrm{d}y\mathrm{d}z$，$p(x,y,z)$为星座点在星座图中的联合概率密度，$\Delta$为星座划分的区间宽度。

当星座信息熵值较低时，星座点易于聚集，符号概率分布失衡，原始调制特征明显；星座信息熵值越大，星座点分布越均匀，信号越趋于随机噪声，能够有效抵御针对星座图样的统计攻击。对比4-ray、8-ray原始星座、旋转加密[16]及本文星座加密算法的信息熵，计算时$\Delta=1$，数据大小为65 536 bit。如图6所示，加密后三维星座信息熵显著提升，相较于星座旋转方法，本文方法熵值增幅更大，表明所提算法能有效增强星座混淆度，提升信号的抗侦测能力。

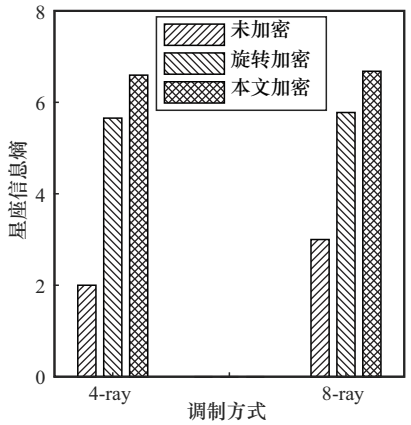


图6 三维星座信息熵

需要说明的是，星座信息熵采用以2为底的对数运算，数学量纲为bit，但该指标描述星座符号在三维星座图上网格划分后的分布不确定性，并不代表调制符号承载的业务信息比特。为避免量纲歧义，仿真图中省略星座信息熵的单位，仅对熵值进行相对大小对比。

3.3　2D-EWFRFT的安全性

EWFRFT用于物理层安全的原因是通过对变换参数的灵活调控，可生成具有不同特征的信号形式。图7为正交相移键控（quadrature phase shift keying, QPSK）信号经不同参数下的2D-EWFRFT处理后的星座图，可以看出，多参数的引入使信号形式更加丰富多样，能够有效迷惑潜在的信号窃听与分析行为，增强通信系统的物理层安全防护性能。

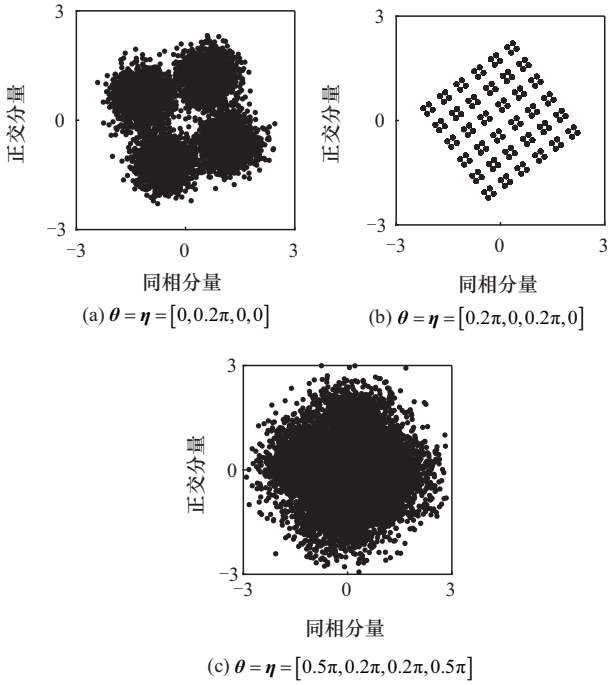


图7　QPSK信号经不同参数的2D-EWFRFT处理后的星座图

进一步分析2D-EWFRFT系统的参数敏感性，如图8所示，当变换参数仅发生0.06π的偏移时，系统解调误码率会快速上升，表明变换参数具有较好的敏感性，未掌握正确参数的非法窃听者即便截获信号，也难以完成有效解调。然而，变换参数的计算精度不足10^{-2}量级，2D-EWFRFT系统密钥空间为$(10^2)^8 = 10^{16} \approx 2^{53}$，规模有限，单一结构下无法有效抵抗参数扫描攻击。

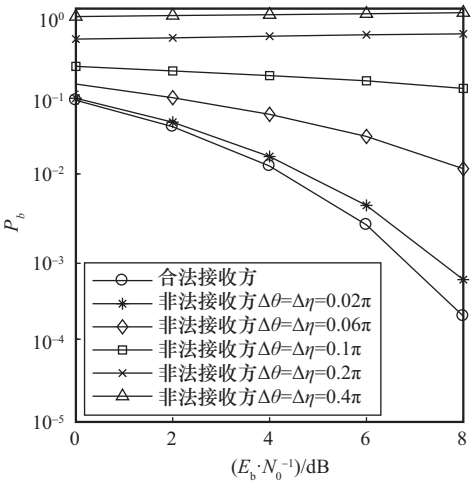


图8　2D-EWFRFT参数敏感性分析

3.4　复杂度分析

在密码算法的硬件实现与性能评估中，乘法运算量是反映硬件资源消耗与实现代价的关键量化指标。本文方法由基于对偶四元数的三维星座加密和2D-EWFRFT两部分构成，其运算流程不含高复杂度的循环嵌套。对于长度为N点的信号序列，每个星座点均需要通过对偶四元数完成置乱加密，由此可得三维星座加密的计算复杂度为$O(19N)$。该结果利用对偶四元数的结构特性与点的纯虚稀疏形式精简得到，远低于文献[16]绕轴旋转加密方法$O(27N)$、文献[19]先绕轴旋转再平移加密方法$O(36N)$的计算复杂度。依据文献[12]的相关结论，2D-EWFRFT的计算复杂度为$O(N\text{lb}N + 8N)$。因此，本文方法的计算复杂度为$O(N\text{lb}N + 27N)$，各方法的计算复杂度对比如表1所示。

表1　　计算复杂度对比

加密方法	计算复杂度
三维星座加密	$O(19N)$
2D-EWFRFT	$O(N\text{lb}N + 8N)$
本文方法	$O(N\text{lb}N + 27N)$
旋转加密方法[16]	$O(27N)$
旋转平移方法[19]	$O(36N)$

综上所述，本文方法仅以小幅增加计算开销为代价，突破了单一加密方案在安全性能上的固有局限，有效提升了系统的安全强度。下文将对该方法的安全性与抗攻击能力展开验证与分析。

4　仿真实验

无线信道的开放性易导致信号被截获与被破译，为验证本文方法的安全性，以Matlab R2016为实验平台，从信号抗检测识别、信息抗攻击破译等方面展开测试与评估。在实验过程中，在混沌系统的有效参数区间内随机选取相关参数进行仿真实验，具体仿真参数如表2所示。

表2　　仿真参数

类别	参数
数据长度	65 536
混沌初值(x_0,y_0,z_0)	（0.3,−0.2,0.8）
混沌控制参数(r,a,b,c)	(7,9,6,12)
平移最大、最小值(ρ_1,ρ_2)	（1.5,1）
二维信号矩阵维度	256×256

4.1　星座加密特性

信息首先经4-ray和8-ray三维调制，再通过本文方法进行处理，对应的星座加密分布如图9所示。在未加密状态下，无论是4-ray还是8-ray调制信号，其星座点均呈现出较强的规律性分布，攻击者可通过重构星座图等方法快速识别调制方式，进而对通信系统造成潜在的破解风险。采用本文三维星座加密后，星座点随机散布于两个球体之间，在此基础上，经2D-EWFRFT二次加密，信号原有规律被完全掩盖，整体呈现近似随机噪声的特性。该特性使窃听方难以有效捕获有用信号，即便成功截获加密信号，也无法辨识调制样式，从而提升系统的抗截获能力。此外，在本文方法中，三维星座加密和2D-EWFRFT分别由7个和8个相互独立的参数共同控制，在保证加密强度的同时，也提升了算法的灵活性。

4.2　信号统计特性

信号识别技术一般依托信号自身固有特征的统计规律，通过多种特征统计检测方法实现信号的有效检测与分类。现有研究结果证实，高斯及类高斯信号的检测与识别是该领域的突出技术难题。为此，本文对加密信号的统计特性进行深入分析，并与类高斯信号的相关特征进行对比分析，如图10所示。由图10可知，加密信号的包络幅度趋近瑞利分布，相位在0 ~ 2π区间均匀分布，同相分量幅度分布则近似高斯分布。上述统计特征进一步表明，加密信号具有明显的类高斯特性，这将有效削弱基于特征参数的调制识别算法的检测效果，降低

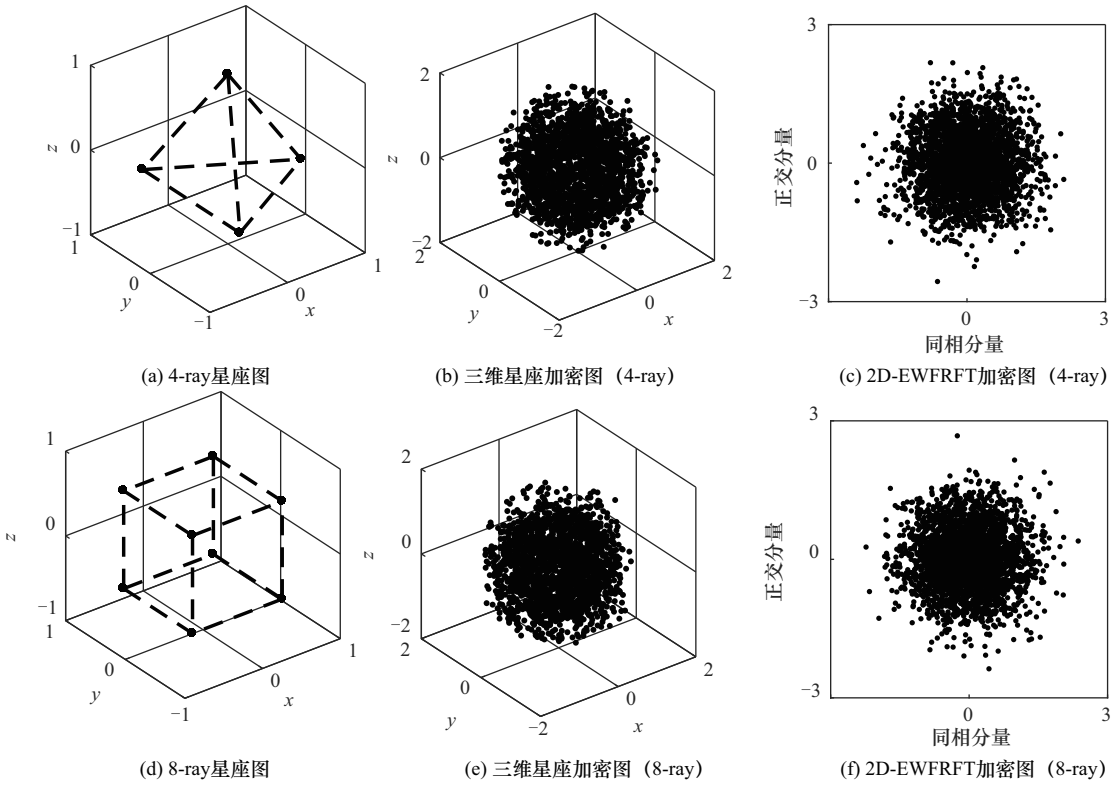
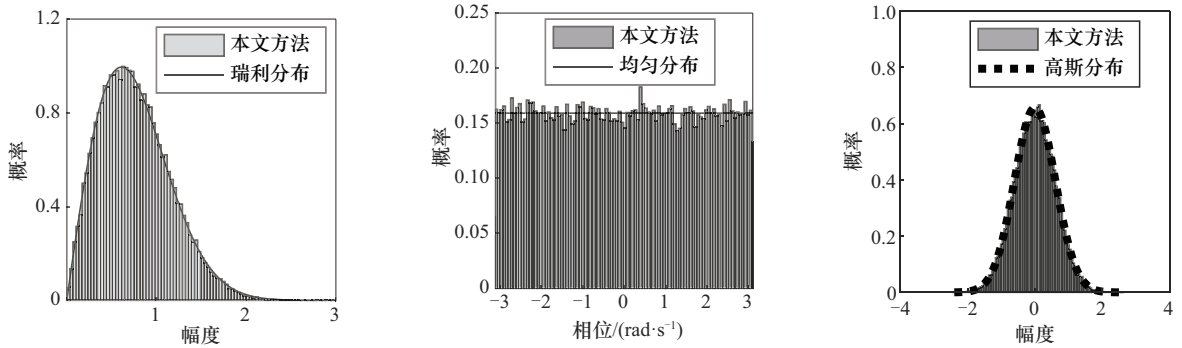


图9　星座加密分布



(a) 复包络幅度分布　(b) 相位分布　(c) 同相分量幅度分布

图10　加密信号统计规律分析

调制方式识别的准确性。

4.3　抗统计攻击性能

调制加密不仅能够对调制方式进行隐藏与混淆，提升信号的抗截获能力，还能实现传输信息的混乱与扩散，进而提升传输信息的抗攻击能力。本文选取加密图像的信息熵作为评估指标，以衡量密文数据的统计分布规律，其定义为：

$$H(\boldsymbol{Y}) = \sum_{i=0}^{2^u-1} p(\boldsymbol{Y}_i)\mathrm{lb}\frac{1}{p(\boldsymbol{Y}_i)} \tag{24}$$

其中，$\boldsymbol{Y}$为图像灰度值，u为图像灰度级总数，$p(\boldsymbol{Y}_i)$为灰度值$\boldsymbol{Y}_i$在图像中出现的概率。

对于256级灰度图像而言，因其灰度值具有2^8种可能的取值，信息熵的理想值为8 bit，加密信息熵越接近理想值，表明加密效果越好。本文方法由基于对偶四元数的三维星座加密与2D-EWFRFT级联构成。为验证本文方法的安全性，设计并开展消融实验，在相同仿真参数条件下，分别采用本文方法、单独三维星座加密模块、单独2D-EWFRFT模块对Cammera、Peppers和Baboon 3幅图像完成加密，并计算密文图像信息熵。此外，将本文方法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[19]展开对比。如表3所示，本文加密图像的信息熵均接近理想值8 bit，整体性能优于单独的三维星座加密或2D-EWFRFT模块，与二维星座加密结合WFRFT的方法性能相当，表明本文方法能够有效打乱灰度图像的原始统计分布。同时，本文三维星座加密信息熵均高于文献[16]和文献[19]，说明所提基于对偶四元数的三维星座加密算法的置乱效果更好，安全性更高。此外，现有单一星座加密方案信息熵约7.95 bit，该数值仅达到基础安全指标，置乱能力存在明显的局限性。

表3　不同方法密文图像信息熵

方法	Cammera/bit	Peppers/bit	Baboon/bit
本文方法	7.997 3	7.997 3	7.997 2
2D-EWFRFT	7.991 5	7.994 1	7.995 3
三维星座加密	7.974 5	7.986 4	7.987 1
WFRFT星座加密[8]	7.997 2	7.997 0	7.997 1
旋转加密方法[16]	7.887 5	7.956 5	7.955 1
旋转平移方法[19]	7.878 5	7.953 8	7.954 9

4.4　抗穷举攻击性能

性能优良的加密算法应同时具备足够大的密钥空间和极强的密钥敏感性。本文设计的加密方法，其密钥由3D-SEXP超混沌的初值(x_0,y_0,z_0)和控制参数(r,a,b,c)共同构成，各密钥参数的敏感性分析如图11所示。由图11可知，当密钥x_0,z_0,a,c,r分别存在10^{-15}量级、密钥y_0,b分别存在10^{-14}量级的微小变化时，解密端对应的误比特曲线始终稳定在0.5附近，表明攻击者即便采用存在细微偏差的密钥进行解密尝试，也无法从输出信号中恢复出任何有效信息。故本文方法的密钥空间为$10^{15}\times10^{15}\times10^{15}\times10^{15}\times10^{15}\times10^{14}\times10^{14}=10^{88}\approx2^{292}$。同时，在同一仿真参数条件下，分别计算单独三维星座加密模块、单独2D-EWFRFT模块的密钥空间，并与现有同领域文献进行对比，如表4所示。由表4可知，单独的三维星座加密模块的密钥空间与本文方法一致，且二者均远高于单独2D-EWFRFT模块。此外，虽然文献[8]和文献[16]给出的密钥空间优于本文方法，但该类文献并未针对每个密钥取值开展精细化计算，仅以密钥的组合数量计算了密钥空间。综上所述，本文方法具备超大的密钥空间及较高的密钥敏感性，能够有效抵御信息层面的穷举攻

击，同时在信号层面破坏星座固有分布规律，实现上层密码难以达到的抗信号检测效果。

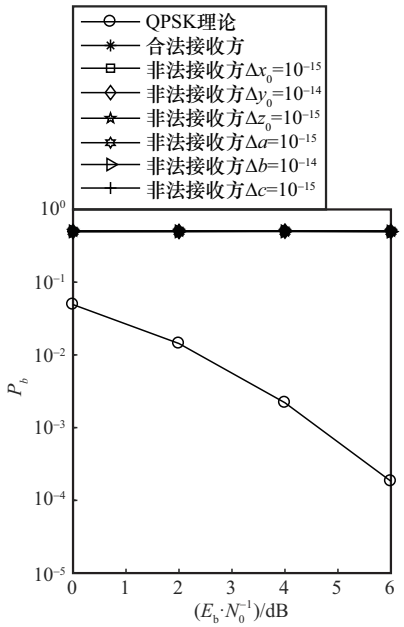


图11　密钥敏感性分析

表4　　密钥空间对比

加密方法	密钥空间
本文方法	$10^{88}\approx 2^{292}$
三维星座加密	2^{292}
2D-EWFRFT	2^{53}
WFRFT星座加密[8]	2^{332}
旋转加密方法[16]	10^{133}
旋转平移方法[19]	1.2×10^{73}

4.5　误比特率分析

无线信号在空间传播过程中易受信道噪声干扰引发误码，加密算法的引入也会对信号误比特率带来一定影响。相较于二维调制方式，三维调制星座拥有更大的空间自由度，能够耐受更强的干扰与更多解码偏差，在发射相同能量的条件下，接收方可获得更低的误比特率。图12的仿真结果也印证了三维星座的误比特率低于QPSK理论值。此外，三维星座旋转加密不会改变星座点间的距离，而本文采用的三维星座加密模块在一定程度上调整了星座点间的最小欧氏距离，进而带来了小幅的误比特率性能损耗。结合文献[11]的研究结论，EWFRFT在时频双选信道下具备优异的抗衰落性能。从图12可以看出，单一的2D-EWFRFT在加性白高斯噪声（additive white Gaussian noise, AWGN）信道下误比特率优于未加密的三维星座调制信号，也能够补偿三维星座加密带来的性能衰减，说明本文方法在实现高强度信号加密的同时，仍能保证通信传输的可靠性。

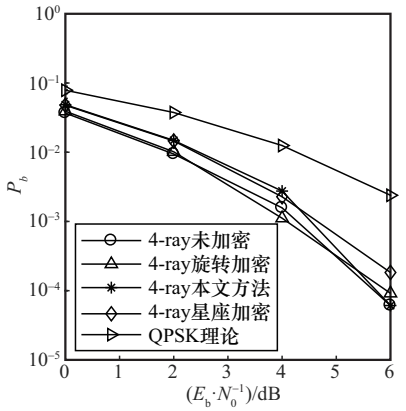


图12　误比特率分析

5　结束语

针对无线通信信号易被截获的安全问题，本文着眼于物理层，提出了一种超混沌驱动对偶四元数置乱三维星座加密的2D-EWFRFT通信方法，主要结论如下。

（1）以正弦函数为核心非线性变换，并引入指数项扰动迭代过程，加速相邻轨道分离，构建了一种动力学性能优良的3D-SEXP超混沌映射，为加密方法提供数据加密密钥。

（2）基于对偶四元数，设计了由7个相互独立参数协同控制的三维星座加密算法，实现了旋转与平移联合变换，在提高星座信息熵的同时，有效降低了计算复杂度。

（3）构建了2D-EWFRFT，从行列两个维度对信号进行变换，多个参数共同作用丰富了变换信号形式，有助于提升系统的安全性。

（4）提出了3D-SEXP超混沌控制下三维调制信号先星座加密再2D-EWFRFT二次加密的方法，有效弥补了单一星座加密置乱能力不足与EWFRFT参数敏感性较弱的缺陷。仿真结果表明，本文方法可扰乱调制信号的分布规律，增强无线信号的抗检测和抗截获能力，同时通过对传输信息进行混乱与扩散，提升了系统抵御统计和穷举攻击的能力，为无线通信物理层安全防护提供了一种有效途径。

然而，本文仅在单发单收AWGN信道下完成了所提方法的安全性与传输有效性验证，尚未研究多径衰落等复杂信道环境下的接收机设计与验证。后续将进一步强化接收机的设计，拓展至多场景衰落信道开展研究，进一步优化算法参数，提升本文方法对复杂传输环境的适配能力。

参考文献：

[1] Xu Y B, Gao M Y, Zhu H Q, et al. Physical layer encryption of OFDM-PON based on quantum noise stream cipher with polar code[J]. China Communications, 2024, 21(3): 174-188.

[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] Yang Y X, Shen X B, Xiong Z Z, et al. Secret communication in IRS-assisted MP-WFRFT systems: design, analysis, and optimization[J]. IEEE Transactions on Vehicular Technology, 2025, 74(10): 15866-15880.

[4] 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 & Information Technology, 2023, 45(4): 1192-1200.

[5] 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.

[6] 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 (Natural Science Edition), 2018, 46(10): 86-91.

[7] Gao C X, Wu Y C, Zhang Y. Secure communication using WFRFT-DSSS based on chaotic cyclic shift[C]//Proceedings of the 2023 IEEE/CIC International Conference on Communications in China (ICCC). Piscataway: IEEE Press, 2023: 1-5.

[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.

[9] 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 factors of weighted fractional Fourier transform signals based on cyclic correlation[J]. Acta Armamentarii, 2022, 43(7): 1646-1654.

[10] 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.

[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] 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: 13.

[13] 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.

[14] 鲁信金, 雷菁, 李为, 等. 一种基于酉矩阵变换的低峰均比正交时频空安全传输方法[J]. 电子与信息学报, 2023, 45(7): 2395-2405.
Lu X J, Lei J, Li W, et al. Low peak-to-average ratio secure transmission method based on U matrix transformation in orthogonal time and frequency space system[J]. Journal of Electronics & Information Technology, 2023, 45(7): 2395-2405.

[15] 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, 2024, 67: 112303.

[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] 马英杰, 刘岳恒, 赵耿, 等. OTFS通信链路构建及其三维星座加密设计[J]. 电子与信息学报, 2025, 47(10): 3826-3837.
Ma Y J, Liu Y H, Zhao G, et al. OTFS communication link construction and three-dimensional constellation encryption design[J]. Journal of Electronics & Information Technology, 2025, 47(10): 3826-3837.

[18] 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[J]. Acta Armamentarii, 2024, 45(8): 2531-2541.

[19] 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.

[20] 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): 7201607.

[21] 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.

[22] 周昂, 王世练, 陈炜宇, 等. 混沌低截获概率通信技术研究综述[J]. 通信学报, 2025, 46(10): 272-286.

Zhou A, Wang S L, Chen W Y, et al. Survey on chaos-based low probability of interception communication technology[J]. Journal on Communications, 2025, 46(10): 272-286.

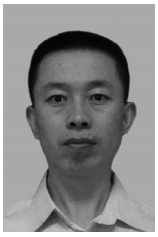
[23] 闫文浩, 姜子敬, 黄欣, 等. 广义二维多项式混沌映射及其在信息传输中的应用[J]. 通信学报, 2022, 43(9): 80-89.
Yan W H, Jiang Z J, Huang X, et al. Generalized 2D polynomial chaotic map and its application in information transmission[J]. Journal on Communications, 2022, 43(9): 80-89.

[24] Chen C F, Sun K H, Xu Q Y. A color image encryption algorithm based on 2D-CIMM chaotic map[J]. China Communications, 2020, 17(5): 12-20.

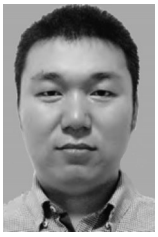
[25] 赵耿, 吴锐, 马英杰, 等. 基于多层元胞自动机的动态随机耦合映像格系统性能分析[J]. 电子学报, 2024, 52(9): 3111-3122.
Zhao G, Wu R, Ma Y J, et al. Performance analysis of dynamic random coupled map lattices system based on multilayer elementary cellular automata[J]. Acta Electronica Sinica, 2024, 52(9): 3111-3122.

[26] 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.

[作者简介]



岔彦直（1988– ），男，空军工程大学工程师，主要研究方向为物理层安全、混沌加密。



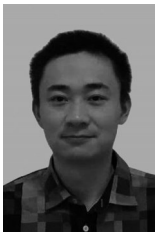
孟庆微（1980– ），男，博士，空军工程大学教授、硕士生导师，主要研究方向为物理层安全、通信信号处理。



李嘉悦（1999– ），女，空军工程大学硕士生，主要研究方向为物理层安全、混沌加密。



王可青（1988– ），女，空军工程大学讲师，主要研究方向为电子对抗。



王聃（1990– ），男，博士，空军工程大学副教授，主要研究方向为信息对抗理论与技术。