三维星座缩放加密的扩展加权分数傅里叶变换安全通信方法

孟庆微，员彦直，王晗
（空军工程大学信息与导航学院，陕西 西安 710077）

摘　要：为解决无线通信开放性带来的安全问题，从信号层面入手，提出一种三维星座缩放加密的扩展加权分数傅里叶变换安全通信方法。该方法设计了混沌三维布朗运动序列，利用其控制缩放参数生成随机缩放矩阵，进而对每个星座符号进行缩放加密。随后，将缩放加密后的星座符号组合为I/Q信号，并进行扩展加权分数傅里叶变换处理。此外，还给出了三维星座缩放加密的概率模型，并证明了其具有完全保密性。仿真结果表明，所提方法加密后有效扰乱了原本分布规律的星座图，且即使密钥空间发生微小变化，也无法解密出任何有价值的信息。

关键词：三维星座；缩放加密；扩展加权分数傅里叶变换；混沌三维布朗运动
中图分类号：TN918.91
文献标志码：A
DOI：10.11959/j.issn.1000–436x.2025012

Extended weighted fractional Fourier transform secure communication method based on 3D constellation scaling encryption

MENG Qingwei, YUN Yanzhi, WANG Han
Information and Navigation College, Air Force Engineering University, Xi’an 710077, China

Abstract: To solve the security problems caused by the openness of wireless communication, an extended weighted fractional Fourier transform secure communication method based on 3D constellation scaling encryption was proposed from the signal level. A chaotic three-dimensional Brownian motion sequence was designed to control the scaling parameters and a random scaling matrix was generated, which was used to encrypt each constellation symbol. Then, the constellation-scaled encrypted symbols were combined into I/Q signals and subjected to extended weighted fractional Fourier transform processing. Furthermore, a probabilistic model of the three-dimensional constellation scaling encryption was given, proving that it had complete confidentiality. Simulation results show that the proposed method encrypts the original constellation diagram, which is originally distributed in a regular manner, and that even a slight change in the key space cannot decrypt any valuable information.

Keywords: three-dimensional constellation, scaling encryption, extended weighted fractional Fourier transform, chaotic three-dimensional Brownian motion

0　引言

随着无人机技术的迅速发展，其在各领域的应用日益广泛。然而，无人机通信的无线特性使其面临窃听、篡改和劫持等安全威胁。物理层安全（PLS, physical layer security）能够增大信道保密容量、减小窃听信道优势，确保通信数据安全，已被

收稿日期：2024–10–09；修回日期：2025–01–06
通信作者：员彦直，337949142@qq.com
基金项目：国家自然科学基金资助项目（No.62101591）
Foundation Item：The National Natural Science Foundation of China (No.62101591)

引入无人机系统[1]。调制加密作为一种基于密钥的物理层安全方案，通过预编码加密[2]、星座置乱[3]、子载波加扰[4]等方式将信号转化为类高斯分布，消除了原始信号的统计特征，实现了通信的高隐蔽性，备受国内外学者的广泛关注[5]。

在调制加密中，星座置乱加密技术是近年来热门研究方向之一。根据星座的维数，该技术主要分为二维星座和三维星座两大类。二维星座置乱利用相位加扰[6]、幅相加密[7]、星座跳转[8]等手段，确保通信信号的安全。三维星座置乱主要通过星座旋转加密[9-11]、星座符号位置置乱[12]等方法，进一步丰富了加密的维度和效果。然而，当前三维星座置乱加密的研究尚显不足，主要集中在星座点分别绕 x、y、z 轴旋转加密及四元数旋转加密，前者完成加密需要 3 次矩阵乘法运算，计算复杂度高；四元数旋转加密受限于数学特性，单个四元数的最大旋转角度为 180°，加密效果不理想。此外，三维星座符号位置置乱大多是沿着坐标轴平移或缩放相同比例，单次加密的维度有待提升。实质上，三维星座调制加密是在密钥作用下，使星座符号在三维空间内进行旋转或平移等运动，而三维空间中物体的运动方式不仅包括旋转和平移，还有缩放[13]。目前，三维星座加密中沿着任意矢量方向的缩放处理尚属空白。

在具体实现方面，星座置乱加密主要依靠混沌密码[14-16]和加权分数傅里叶变换（WFRFT, weighted fractional Fourier transform）[17-21]等方法。混沌序列因其随机性，在子载波扰动、随机相位信号生成和预编码加密等方面具有广泛应用。然而，随着混沌密码分析技术的发展，部分数字混沌面临相空间重构、深度学习等攻击威胁。因此，设计随机性更强的混沌序列成为当前混沌密码研究的重点。布朗运动是一种自然界的随机现象，文献[12]将其与混沌密码相结合，通过混沌控制布朗运动的变化参数，生成更具随机性的序列，并应用于星座加密中。

WFRFT 作为一种新型信号处理手段，通过调整变换阶数扰乱信号分布规律，因此，在星座置乱加密中得到了广泛应用。文献[17]设计了一种二维多项加权分数傅里叶变换（M-WFRFT, multi-term WFRFT）安全通信方法，行、列信号均经过 M-WFRFT 处理，并利用 M-WFRFT 之间的等效转换关系，收发双方使用不同项数以迷惑潜在窃听者，有效提高了方向调制的安全性。文献[18]提出基于 WFRFT 的物理层认证方法，通过 WFRFT 改变认证信号的星座特征，实现认证标签信号的伪装与隐藏。在物理层安全方面，WFRFT 不仅单独发挥着重要作用，还与星座加密[19]、人工噪声[20]、波束成形[21]等结合，能够进一步增强通信系统的安全性和隐蔽性，广泛应用于复合调制信号的设计。然而，WFRFT 信号形式受变换阶数的控制，已有研究表明，利用循环相关法[21]、高阶累积量[22]等方法，可在未知条件下准确识别出 WFRFT 的变换阶数，对其安全性带来了一定威胁。为此，文献[23]消除了 WFRFT 理论公式推导的严格约束条件，提出扩展加权分数傅里叶变换（EWFRFT, extended WFRFT），该方法拥有 4 个相互独立的因子控制信号形式变化，有助于进一步提高星座加密的安全性。本文的主要工作如下。

1) 提出星座点沿着任意矢量方向缩放的加密技术。发送端通过运用三维变形中的缩放公式生成随机缩放矩阵，对每个星座点在其判决区域内进行移动，完成星座加密。该技术中每个星座符号均由 4 个相互独立的因素控制缩放加密，进一步提升三维星座加密的灵活性与充分性。

2) 结合布朗运动的随机不可预测性，利用经典 Hénon 和 Logistic 映射设计了混沌三维布朗运动序列，并用该序列控制缩放操作及 EWFRFT 的变换参数。仿真结果表明，该序列的运动轨迹复杂，相比原混沌序列，谱熵值更高，随机性更强。

3) 提出一种三维星座缩放加密的 EWFRFT 安全通信方法，加密后的星座点随机而杂乱地分布，密钥空间庞大且高度敏感，能够有效对抗统计、穷举、已知明文和选择明文等攻击，实现无线通信信号的安全传输。

1　星座缩放加密

为了实现星座缩放加密技术，通过分析星座调制和解调的基本原理，并借鉴三维空间中物体的缩放变形，来引入星座缩放加密的概念。

1.1　任意矢量方向缩放的数学表示

缩放是指对一个平面或空间中的对象乘以一个因子 k，使之发生拉伸或挤压的操作。其中 k 为缩放因子，控制对象的变化效果。如果 $|k|<1$，则对象在某个方向会变得更短；如果 $|k|>1$，则对象在

某个方向会变得更长。如果$k<0$，则获得反射的结果；如果对象为平面或空间中的一个点，则当$k>1$时，扩展后仍为一个点，相对于该点原始的位置向上或向外移动；当$0<k<1$时，缩短后仍为一个点，相对于该点原始的位置向下或向内移动；当$k=1$时，该点不会发生移动。沿任意方向矢量缩放如图1所示。其中，$\boldsymbol{v}_{//}$和$\boldsymbol{v}_{//}^{*}$表示与单位矢量$\boldsymbol{n}$平行，$\boldsymbol{v}_{\perp}$和$\boldsymbol{v}_{\perp}^{*}$表示与单位矢量$\boldsymbol{n}$垂直。

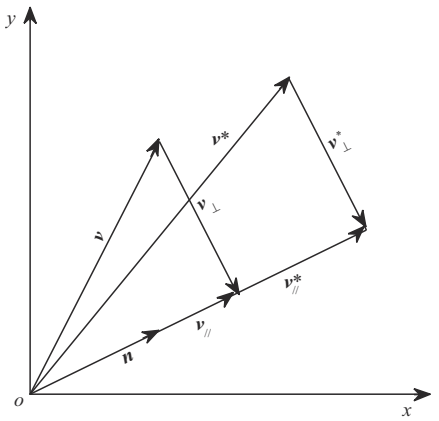


图1　沿任意方向矢量缩放

在二维平面中，向量$\boldsymbol{v}$沿着与单位矢量$\boldsymbol{n}$平行的方向缩放k，得到向量$\boldsymbol{v}^{*}$，可以通过缩放矩阵$\boldsymbol{S}(\boldsymbol{n},k)$表示

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

$$\boldsymbol{v}^{*}=\boldsymbol{v}\cdot\boldsymbol{S}(\boldsymbol{n},k) \tag{2}$$

其中，k是应用于与$\boldsymbol{n}$垂直且通过原点的线的缩放因子；n_x、n_y分别为单位矢量$\boldsymbol{n}$的x、y轴坐标。

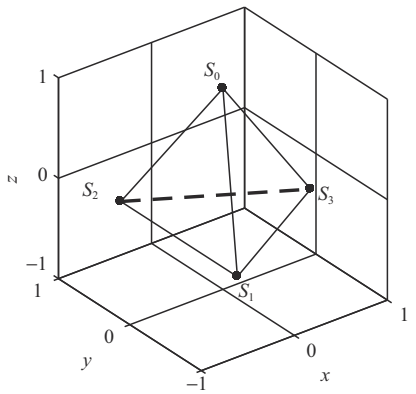
在三维空间中，可以生成一个三维矩阵$\boldsymbol{S}(\boldsymbol{n}',k')$，该矩阵将在由单位矢量$\boldsymbol{n}'$指定的任意方向上按因子$k'$缩放

$$\boldsymbol{S}(\boldsymbol{n}',k')=\begin{bmatrix}1+(k'-1)n_x^2 & (k'-1)n_xn_y & (k'-1)n_xn_z\\ (k'-1)n_xn_y & 1+(k'-1)n_y^2 & (k'-1)n_yn_z\\ (k'-1)n_xn_z & (k'-1)n_yn_z & 1+(k'-1)n_z^2\end{bmatrix} \tag{3}$$

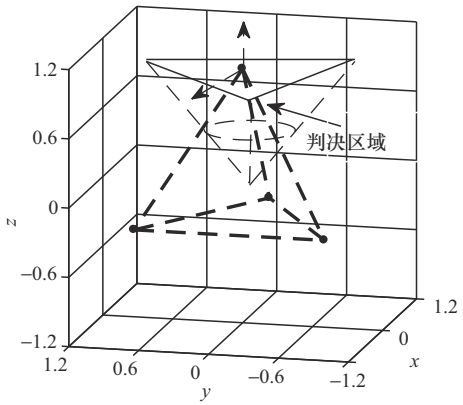
其中，n_x、n_y、n_z分别为单位矢量$\boldsymbol{n}'$的x、y、z轴坐标。

1.2　三维星座调制

三维星座调制在三维空间内设计星座点分布，将传输信息映射到星座点，并利用信号的幅度、相位及发射天线序号等特征进行联合调制，从而实现信号的高效传输。图2(a)展示了4个星座点的三维调制，星座点S_0、S_1、S_2、S_3构成了一个正四面体，坐标分别为$S_0=(0,0,1)$、$S_1=\left(-\frac{\sqrt{2}}{3},-\frac{2}{\sqrt{6}},-\frac{1}{3}\right)$、$S_2=\left(-\frac{\sqrt{2}}{3},\frac{2}{\sqrt{6}},-\frac{1}{3}\right)$和$S_3=\left(\frac{2\sqrt{2}}{3},0,-\frac{1}{3}\right)$。



(a) 星座映射关系



(b) 星座点S_0的判决区域

图2　4-ray三维调制星座图

在发送端，每2 bit信息按照$00\rightleftharpoons S_0$、$01\rightleftharpoons S_1$、$10\rightleftharpoons S_2$、$11\rightleftharpoons S_3$的对应关系映射到一个星座点。然而，由于信号在空间传播过程中受噪声干扰，收到的信号无法直接映射到原始星座点上，解调时需要采取最小距离判决方法，将接收的信号映射到与原始星座点欧氏距离最近的点上，即每个星座点都有各自的判决区域，只要信号落到星座点的判决区域，就会根据该星座点的映射关系恢复原始信息。图2(b)为星座点S_0的判决区域，如果收到的信号落到此区域，则信号将被解调为00。

基于解调的判决原理，参照三维空间中物体缩放变形，本文提出星座缩放加密技术。在发送端，信息经过三维映射后，对每个星座点使用共享的密钥，按照特定的映射规则在其判决区域内进行扩展或缩小等操作；在接收端，密钥和映射规则与发送端相同，能够恢复移动后的星座点，并完成信号的解调。这种加密方式在不增加通信误码率的前提下，对传输信号进行加密保护，有助于提高信号的抗干扰与抗截获能力。

1.3　EWFRFT

WFRFT定义为

$$\mathcal{F}_{\omega}^{a}[f(x)]=\omega_0(\alpha)f(x)+\omega_1(\alpha)F(x)+\omega_2(\alpha)f(-x)+\omega_3(\alpha)F(-x) \tag{4}$$

其中，α为变换阶数，$\alpha\in[0,4)$；$F(x)$是$f(x)$的傅里叶变换；$\omega_l(\alpha)$为加权系数，表示为

$$\omega_l(\alpha)=\frac{1}{4}\exp\left[-\frac{2\pi\mathrm{j}}{4}(\alpha-l)q\right],l=0,1,\cdots,3 \tag{5}$$

其中，j为虚数单位。

WFRFT具有连续性、边界性和阶数可加性3个基本性质，变换阶数α主要决定信号形式。文献[23]提出EWFRFT，突破了变换阶数对WFRFT的约束，具体定义为

$$\mathcal{F}^{+}[f(x)]=w_0(\boldsymbol{\theta})f(x)+w_1(\boldsymbol{\theta})F(x)+w_2(\boldsymbol{\theta})f(-x)+w_3(\boldsymbol{\theta})F(-x) \tag{6}$$

其中，$\boldsymbol{\theta}=[\theta_0,\theta_1,\theta_2,\theta_3]$为变换参数，$\theta_p\in[0,2\pi)$，$p=0,1,\cdots,3$。$w_n(\boldsymbol{\theta})$为加权系数，表示为

$$w_n(\boldsymbol{\theta})=\frac{1}{4}\sum_{p=0}^{3}\exp\left[\left(\theta_p-\frac{2\pi}{4}np\right)\mathrm{j}\right],n=0,1,\cdots,3 \tag{7}$$

EWFRFT主要由变换参数$\boldsymbol{\theta}$决定形式，同样具有连续性、边界性和参数可加性3个基本性质。离散信号$\boldsymbol{X}=[x_1,x_2,\cdots,x_m]$的EWFRFT定义为

$$\mathcal{F}^{+}[\boldsymbol{X}]=w_0(\boldsymbol{\theta})\boldsymbol{X}+w_1(\boldsymbol{\theta})\boldsymbol{X}_1+w_2(\boldsymbol{\theta})\boldsymbol{X}_2+w_3(\boldsymbol{\theta})\boldsymbol{X}_3 \tag{8}$$

其中，$\boldsymbol{X}_i$为$\boldsymbol{X}$的第i次离散傅里叶变换，$i=1,2,3$，加权系数$w_n(\theta_k)$的表达式同式(7)。

由于EWFRFT具有参数可加性，其可应用于通信系统。在发送端，信号经过EWFRFT处理，接收端只需要对参数进行取反操作，就能恢复原始信号，即$\mathcal{F}^{+}[\boldsymbol{X}]$的逆变换$\mathcal{F}^{-}[\boldsymbol{X}]$为

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

EWFRFT具备物理层加密的天然属性，通过调整不同的变换参数，EWFRFT对调制信号处理后呈现不同的星座图，提供了丰富的信号形式。与WFRFT相比，EWFRFT拥有4个相互独立的参数来控制信号的变化，这使得系统在面对参数扫描和调制识别攻击时，展现出更强的抵抗能力。

2　三维星座缩放加密的EWFRFT安全通信

本文提出一种三维星座缩放加密的EWFRFT安全通信方法，将经典Hénon和Logistic映射结合生成三维布朗运动，生成具有更好随机性的序列，进而控制缩放矩阵及EWFRFT的各项参数，具体通信系统结构如图3所示。在发送端，将实时发送的明文比特流进行等长分组，每组明文比特流通过串并转换映射到三维星座点，并对每个星座点实施二级加密。为不失一般性，本文仅介绍每组比特流的加密方法。首先，按照三维缩放公式构造的随机矩阵对星座点进行缩放加密，然后对I/Q变换后的星座符号进行EWFRFT加密，最后对加密后的分组信号添加循环前缀（CP, cyclic prefix）

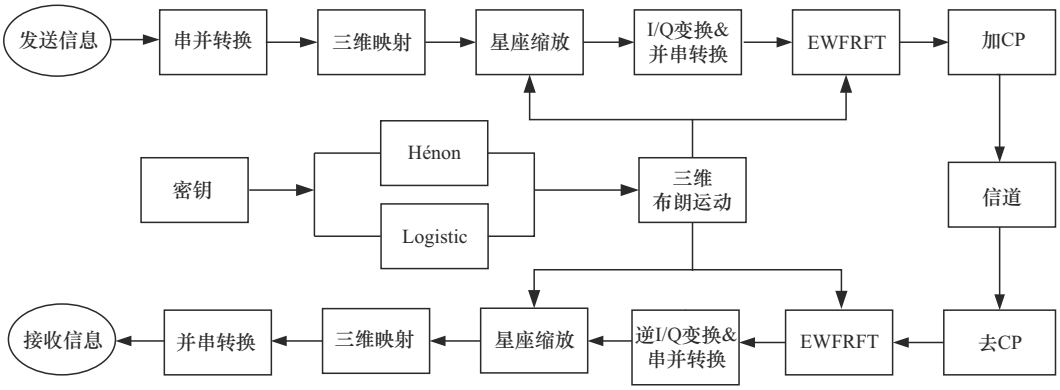


图3　三维星座缩放加密的EWFRFT通信系统结构

后，通过无线信道发送。在加密过程中，Hénon和Logistic映射的初值、控制参数及预迭代次数共同作为密钥，通过安全信道在合法通信双方之间预先共享。在接收端，合法接收方可利用共享密钥准确恢复原始信息，有效确保了通信的稳定性和安全性。

2.1　混沌三维布朗运动

布朗运动作为自然界的普遍现象，其运动轨迹具有无规则性和不可预测性。通过运用混沌序列来控制布朗运动的参数，不仅能进一步扰乱混沌序列的分布，还能显著提升序列的随机性。在三维空间中，一个点的布朗运动用数学表达式描述为

$$\begin{cases} \mathrm{dx} = \tau \sin\alpha \cos\beta \\ \mathrm{dy} = \tau \sin\alpha \sin\beta \\ \mathrm{dz} = \tau \cos\alpha \end{cases} \tag{10}$$

其中，$\tau \in [0,+\infty)$为运动步长，α和β表示运动的方向。

本文选用经典Hénon和Logistic映射设计混沌三维布朗运动序列，其映射表达式分别为

$$\begin{cases} x_{n+1} = 1 - ax_n^2 + y_n \\ y_{n+1} = bx_n \end{cases} \tag{11}$$

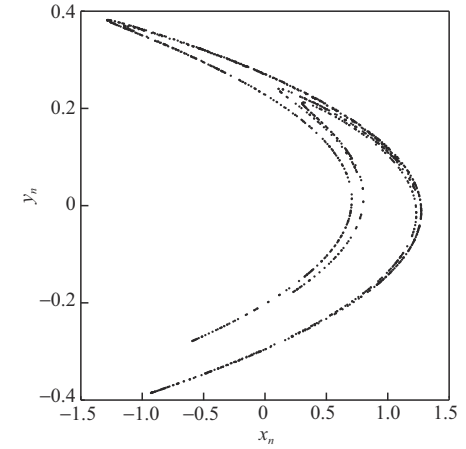
$$x'_{n+1} = cx'_n(1 - x'_n) \tag{12}$$

在式(11)中，当$1.07 \leqslant a \leqslant 1.4, b = 0.3$时，Hénon映射处于混沌状态；在式(12)中，当$3.57 \leqslant c \leqslant 4$时，Logistic映射处于混沌状态。设Hénon映射的初值为(x_0,y_0)，迭代m_1次后生成长度为L的混沌序列(x_n,y_n)，Logistic映射的初值为x'_0，迭代m_2次生成长度为L的混沌序列x'_n，本文构造的混沌三维布朗运动表达式为

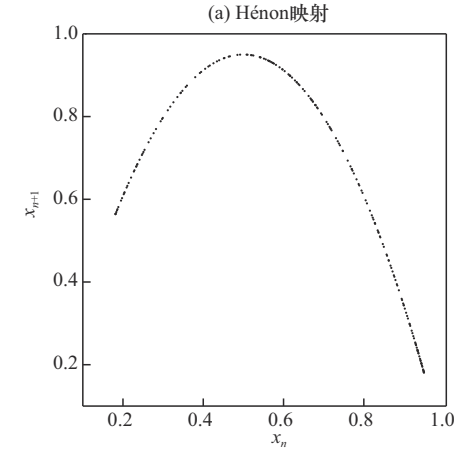
$$\begin{cases} \mathrm{dx}_n = \left| \dfrac{x_n}{\mathrm{mean}(x_n)} \right| \sin(y_n \times 2\pi) \cos(x'_n \times 2\pi) \\ \mathrm{dy}_n = \left| \dfrac{x_n}{\mathrm{mean}(x_n)} \right| \sin(y_n \times 2\pi) \sin(x'_n \times 2\pi) \\ \mathrm{dz}_n = \left| \dfrac{x_n}{\mathrm{mean}(x_n)} \right| \sin\left(\dfrac{y_n}{x'_n} \times \pi \right) \end{cases} \tag{13}$$

其中，$\mathrm{mean}(x_n)$为序列x_n的平均值。

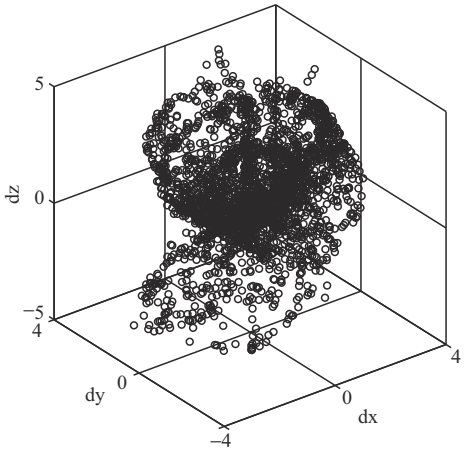
在对混沌三维布朗运动进行2 000次迭代后，观察其运动轨迹，并与Hénon和Logistic映射的奇异吸引子进行对比，如图4所示，混沌三维布朗运动序列的随机性和杂乱性较突出。本文通过谱熵（SE, spectral entropy）进一步量化这种随机性，SE能够反映混沌系统结构的复杂度。对比原始混沌序列与其三维布朗运动序列的谱熵值，如表1所示，混沌三维布朗运动序列的谱熵值相对较高，充分说明其随机性更强，在加密操作中具有巨大的应用潜力。



(a) Hénon映射



(b) Logistic映射



(c) 混沌三维布朗运动迭代2 000次的运动轨迹

图4　混沌三维布朗运动随机性对比

表 1　原始混沌序列与三维布朗运动序列谱熵对比

序列	SE
x_n	0.914 6
y_n	0.904 2
x_n'	0.905 7
dx_n	0.938 9
dy_n	0.943 9
dz_n	0.929 5

2.2　加密方法

发送端将明文比特信息按照 4-ray 三维星座调制进行映射，假设映射后的星座点为 N 个，第 i 个星座点 M_i 的坐标为 (x_i,y_i,z_i)，则明文信号可表示为

$$\boldsymbol{M}=\begin{bmatrix} x_1 & y_1 & z_1 \\ x_2 & y_2 & z_2 \\ \vdots & \vdots & \vdots \\ x_N & y_N & z_N \end{bmatrix} \tag{14}$$

本文运用 2 组不同的初值和控制参数，分别依据式(11)～式(13)预迭代后，生成长度为 N 的混沌三维布朗运动序列，设第一组混沌三维布朗运动序列为 $\mathrm{d}\boldsymbol{x}$、$\mathrm{d}\boldsymbol{y}$、$\mathrm{d}\boldsymbol{z}$，第二组为 $\mathrm{d}\boldsymbol{x}'$、$\mathrm{d}\boldsymbol{y}'$、$\mathrm{d}\boldsymbol{z}'$，将 $\mathrm{d}\boldsymbol{x}$、$\mathrm{d}\boldsymbol{y}$、$\mathrm{d}\boldsymbol{z}$ 作为缩放矩阵的方向矢量 $\boldsymbol{n}$ 的 x、y、z 轴坐标。为保证缩放加密的星座点落在各自的判决区域，从 $\mathrm{d}\boldsymbol{x}'$、$\mathrm{d}\boldsymbol{y}'$、$\mathrm{d}\boldsymbol{z}'$ 中筛选出 N 个取值在 $[0.8,1.6]$ 范围内的新序列作为缩放因子 $\boldsymbol{k}$，并依据式(3)生成 N 个随机缩放矩阵，其中，第 i 个缩放矩阵为 $\boldsymbol{S}_i(\boldsymbol{n}_i,k_i)$。计算缩放矩阵时，需要对方向矢量进行单位化处理。

依据生成的随机缩放矩阵，对每个明文信号星座点进行缩放加密，表示为

$$M_i'=M_i\boldsymbol{S}_i(\boldsymbol{n}_i,k_i) \tag{15}$$

其中，M_i' 为缩放加密后的第 i 个星座点。缩放加密后的星座点 $\boldsymbol{M}'$ 为

$$\boldsymbol{M}'=\begin{bmatrix} x_1' & y_1' & z_1' \\ x_2' & y_2' & z_2' \\ \vdots & \vdots & \vdots \\ x_N' & y_N' & z_N' \end{bmatrix} \tag{16}$$

缩放加密后的星座点按照式(17)进行 I/Q 及并串转换，得到 $\boldsymbol{M}''$ 为

$$\boldsymbol{M}''=\begin{bmatrix} x_1'+\mathrm{j}y_1' \\ z_1'+\mathrm{j}x_2' \\ y_2'+\mathrm{j}z_2' \\ \vdots \\ z_{N-1}'+\mathrm{j}x_N' \\ y_N'+\mathrm{j}z_N' \end{bmatrix}^{\mathrm{T}} \tag{17}$$

其中，$[\cdot]^{\mathrm{T}}$ 表示矩阵的转置。

对信号 $\boldsymbol{M}''$ 进行分组，每部分进行 EWFRFT 加密。为进一步提高 EWFRFT 的参数抗扫描特性，将生成的序列 $\mathrm{d}\boldsymbol{z}'$ 乘以 π 后作为 EWFRFT 的控制参数 $\boldsymbol{\theta}$，则加密后的信号 $\boldsymbol{M}'''$ 为

$$\boldsymbol{M}'''=\mathrm{EWFRFT}\left\{\boldsymbol{M}'',(\theta_1,\theta_2,\theta_3,\theta_4)\right\} \tag{18}$$

2.3　解密方法

合法通信双方预先通过安全通道共享密钥，接收端按照与发送端相同的方式生成两组混沌三维布朗运动序列，并筛选出缩放因子，构造缩放矩阵以及选取 EWFRFT 的控制参数。

对收到的信号 $\boldsymbol{R}$ 进行分组，每部分进行 EWFRFT 解密，解密后的信号 $\boldsymbol{R}'$ 为

$$\boldsymbol{R}'=\mathrm{EWFRFT}\left\{\boldsymbol{R},(-\theta_1,-\theta_2,-\theta_3,-\theta_4)\right\} \tag{19}$$

分离信号 $\boldsymbol{R}'$ 的实部和虚部，并进行如式(16)所示的串并转换，得到三维星座点，并对其进行缩放解密，得到 R_i'' 为

$$R_i''=R_i'(\boldsymbol{S}_i(\boldsymbol{n}_i,k_i))^{-1} \tag{20}$$

其中，R_i' 为第 i 个待缩放解密的星座点；R_i'' 为第 i 个缩放解密后的星座点；$[\cdot]^{-1}$ 表示矩阵的逆。

计算每个解密出的星座点 R_i'' 与原始星座图中 4 个星座点之间的欧氏距离，并将 R_i'' 判决为与原始星座点欧氏距离最小的星座点。然后，根据星座点与传输信息之间的映射关系，恢复最终的接收信息。

3　性能分析及仿真实验

在加密方法的设计中，确保方法的安全性与有效性至关重要。本节从星座加密特性、抗统计攻击、抗穷举攻击、误比特率等方面对本文方法进行仿真分析，评估其性能。仿真实验在以下平台完成，CPU 为 Intel Core i3-5005U 4 GB，GPU 为 NVIDIA GeForce 920A 4 GB，操作系统为 Windows 10 家庭版，仿真软件为 MATLAB R2016。仿真参数如表 2 所示。

表2 仿真参数

参数	取值
信道类别	AWGN
Hénon映射初值(x_0,y_0)	(0.5,0.5)
Hénon映射控制参数(a,b)	(1.4,0.3)
Hénon映射预迭代次数m_1	100
Logistic映射初值x_0'	0.3
Logistic映射控制参数c	3.96
Logistic映射预迭代次数m_2	100

3.1 三维星座缩放加密的完全保密性

信息论是研究密码算法保密性的重要方法之一。根据香农保密理论，当一个密码算法的明文与密文相互独立时，该算法是完全保密的，即对于明文空间$\boldsymbol{M}$中的任意明文g以及密文空间$\boldsymbol{C}$中的任意密文h，如果$p(m=g)\neq 0$，则有

$$p(c=h\,|\,m=g)=p(c=h) \tag{21}$$

其中，$p(m=g)$表示明文g在明文空间$\boldsymbol{M}$中的概率；$p(c=h\,|\,m=g)$表示明文g加密为密文h的概率；$p(c=h)$表示密文h在密文空间$\boldsymbol{C}$中的概率。

本文所提三维星座缩放加密的明文空间$\boldsymbol{M}$由三维映射符号组成，密文空间$\boldsymbol{C}$由缩放加密后的三维映射符号组成，密钥空间$\boldsymbol{K}$由混沌序列控制缩放参数生成的缩放矩阵组成。根据式(15)所示的缩放加密算法，可以得到定理1。

定理1 三维星座缩放加密是完全保密的。

证明 设密钥$\boldsymbol{S}\in\boldsymbol{K}$，明文调制星座符号$g\in\boldsymbol{M}$且密文调制星座符号$h=g\boldsymbol{S}$。

根据全概率公式，即事件$B_1,B_2,\cdots,B_n$是样本空间Ω的一个完备事件组，且$p(B_i)>0(i=1,2,\cdots,n)$，对于任意一个事件A，有$p(A)=\sum_{i=1}^{n}p(B_i)p(A\,|\,B_i)$。那么本文所提加密方法中有

$$p(c=h\,|\,m=g)=\sum_{\boldsymbol{D}\in\boldsymbol{K}}p(k=\boldsymbol{D})\,p(c=h\,|\,m=g,k=\boldsymbol{D}) \tag{22}$$

由于三维星座缩放加密是双射，证明过程见附录1，使用密钥$\boldsymbol{D}$只能将明文星座符号g唯一地加密成密文h，且将明文星座符号g加密成密文h的密钥$\boldsymbol{D}$也是唯一的，只能为$\boldsymbol{S}$，即

$$p(c=h\,|\,m=g,k=\boldsymbol{D})=1 \tag{23}$$

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

$$p(k=\boldsymbol{S})=\frac{1}{|\boldsymbol{K}|} \tag{24}$$

其中，$|\boldsymbol{K}|$为密钥空间$\boldsymbol{K}$的元素数量。$p(c=h\,|\,m=g)$表示为

$$\begin{aligned}&p(c=h\,|\,m=g)=\\&\sum_{\boldsymbol{D}\in\boldsymbol{K}}p(k=\boldsymbol{D})\,p(c=h\,|\,m=g,k=\boldsymbol{D})=\\&p(k=\boldsymbol{S})=\frac{1}{|\boldsymbol{K}|}\end{aligned} \tag{25}$$

由全概率公式可得

$$\begin{aligned}&p(c=h)=\\&\sum_{g\in\boldsymbol{M}}p(m=g)\,p(c=h\,|\,m=g)=\\&\sum_{g\in\boldsymbol{M}}p(m=g)\,p(k=\boldsymbol{S})=\\&\frac{1}{|\boldsymbol{K}|}\sum_{g\in\boldsymbol{M}}p(m=g)=\frac{1}{|\boldsymbol{K}|}\end{aligned} \tag{26}$$

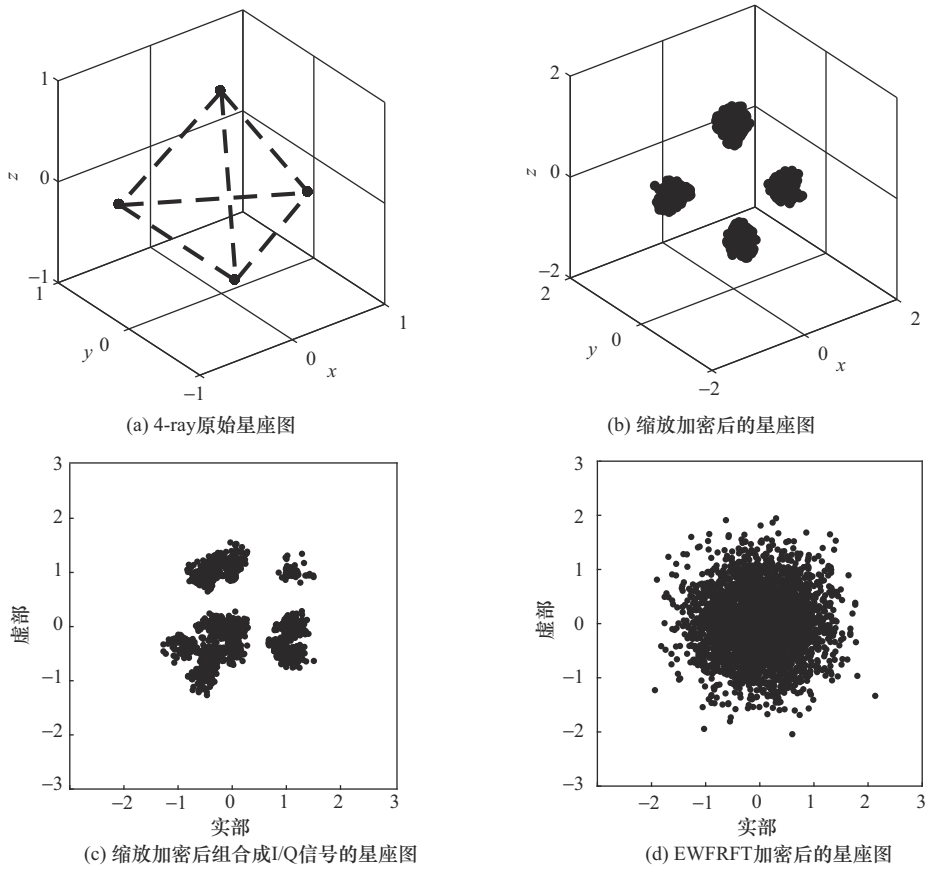
因此，$p(c=h\,|\,m=g)=p(c=h)$，根据香农保密理论可知，三维星座缩放加密是完全保密的。

3.2 星座加密特性分析

本文方法对三维星座实施两重加密，加密前后的4-ray星座图如图5所示。从图5可以看出，原本规整的星座点经过缩放加密后，在其周围散开，形成类似噪声的干扰，这给非法窃听者带来一定的迷惑，即使按照对抗人工噪声的方法从中分离出有用信号，也仅是部分加密后的信息，在密钥未知的情况下无法得到任何有用信息，从而为信息的安全传输提供了较好的保护。然而，缩放加密的星座图无论是三维星座还是组合的I/Q状态，仍然保留了原始星座点的聚集分布规律，存在调制样式信息泄露的风险。EWFRFT加密技术弥补了这一缺陷，经过其处理后，星座点变得随机而无序，彻底消除了任何分布规律。本文方法能够有效抵御调制信号的检测与识别，显著提升通信系统的安全性。

3.3 抗统计攻击分析

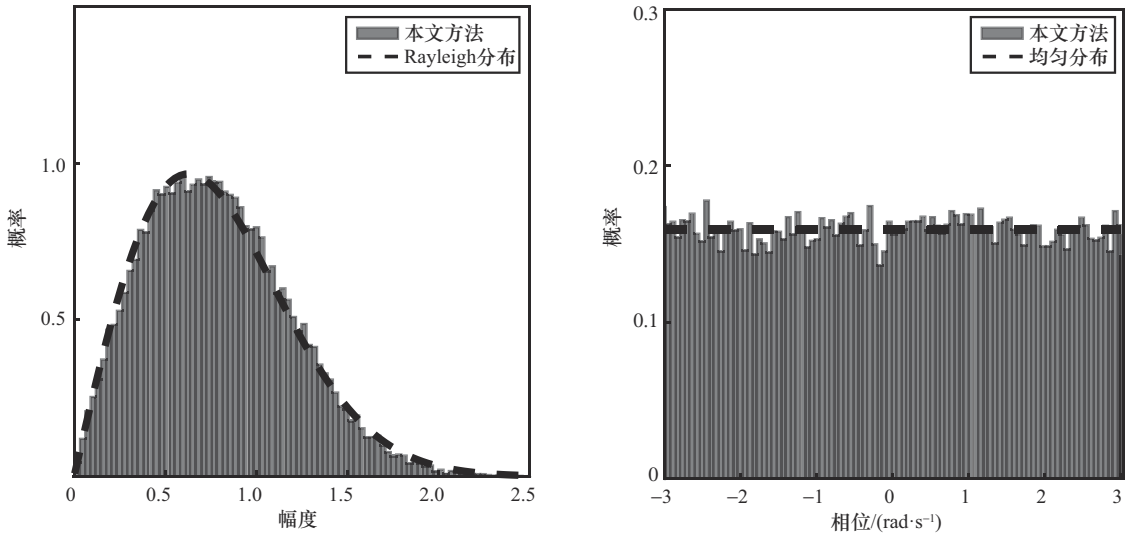
当前调制识别技术在面对高斯或类高斯信号时面临巨大的挑战。为了深入探究本文方法的有效性，对加密后信号进行统计分析，如图6所示。其中，2条加粗虚线分别为Rayleigh分布和概率密度为$\frac{1}{2\pi}$的均匀分布。其中，Rayleigh分布的均值和方差分别与加



(a) 4-ray原始星座图　(b) 缩放加密后的星座图

(c) 缩放加密后组合成I/Q信号的星座图　(d) EWFRFT加密后的星座图

图5　加密前后的4-ray星座图



(a) 加密信号的幅度分布　(b) 加密信号的相位分布

图6　加密信号的幅度和相位分布

密调制信号复包络幅度的均值和方差相等。

从图6可以看出，本文方法对三维星座进行加密处理后，信号的幅度呈现出接近Rayleigh分布的特点，而相位则与概率密度为$\frac{1}{2\pi}$的均匀分布基本吻合。这种特性使得依赖特征参数的统计攻击难以发挥作用，从而极大地降低了调制识别的准确性。

运用加密图像的信息熵定量分析本文方法加密信息的统计特性，计算表达式为

$$H(\boldsymbol{G}) = \sum_{i=0}^{2^N-1} p(\boldsymbol{G}_i) \mathrm{lb} \frac{1}{p(\boldsymbol{G}_i)} \tag{27}$$

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3幅大小均为256像素×256像素的Cammera、Peppers和Baboon灰度图像进行加密处理后，计算加密图像的信息熵，并与文献[9]和文献[19]方法进行对比，如表3所示。对比结果表明，本文方法对3幅图像加密后的信息熵接近理想值8，而同一幅加密图像的信息熵显著优于同领域的调制加密方法，表明本文方法加密后的信息分布更随机。

表3 加密图像的信息熵

方法	Cammera	Peppers	Baboon
本文方法	7.976 0	7.990 8	7.992 8
文献[9]方法	7.878 5	7.953 8	7.954 9
文献[19]方法	7.908 3	7.982 3	7.949 3

综上所述，本文方法不仅能使信号成功对抗基于特征参数的调制识别，还确保了加密信息呈现优异的随机性分布特性。

3.4 抗穷举攻击分析

密钥与整个通信系统的安全性及加密方法的有效性直接相关。随着计算能力的提升，一个出色的加密方法不仅要拥有足够大的密钥空间以抵御暴力破解，还需要对密钥的微小变动极其敏感。针对本文方法进行分析，其密钥系统由混沌的初值及控制参数共同构成，具体包括Hénon映射的初值(x_0,y_0)、控制参数a,b、Logistic映射初值x_0'和控制参数c，取值范围分别为$(-1 < x_0 < 1, -1 < y_0 < 1)$、$1.07 \leqslant a \leqslant 1.4, b = 0.3$、$0 < x_0' < 1$和$3.57 \leqslant c \leqslant 4$。本文采用控制变量法逐一分析该加密方法密钥的敏感性，在仿真实验中，每次仅对一个密钥发生微小变动，其余保持不变。然后对加密后的信息进行解密，得到解密信息的误比特率曲线，如图7所示。从图7可以看出，使用正确密钥对加密信息进行解密时，误比特率随着信噪比的增加而快速下降，说明本文方法的有效性。而使用错误密钥进行解密时，即使x_0、y_0、a、b、c中仅有一个参数发生10^{-15}变动，密钥x_0'发生10^{-16}变动，解密后的信息误比特率仍然保持在0.5左右，说明本文方法即使发生微小的变化，也不会造成任何有用信息的泄露。因此，在不考虑混沌预迭代次数和密钥取值步长的情况下，本文方法的密钥空间为$10^{15} \times 10^{15} \times 10^{15} \times 10^{15} \times 10^{16} \times 10^{15} = 10^{91}$。假设使用计算速度为每秒$3.38 \times 10^{17}$次双精度浮点运算的超级计算机尝试遍历密钥取值进行解密，那么获取加密序列的正确密钥至少需要9.38×10^{65}年。此外，文献[15]和文献[16]中提到的密钥空间分别为4×10^{30}和4.3×10^{29}，远小于本文方法的密钥空间。因此，本文方法的密钥空间能够有效抵御穷举攻击。

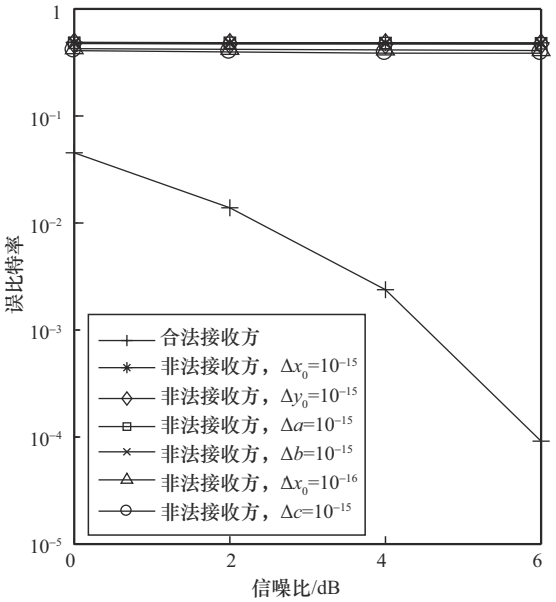
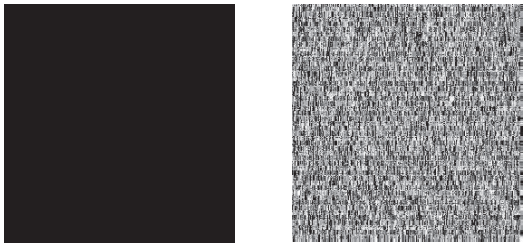


图7 密钥敏感性分析

3.5 抗已知明文和选择明文攻击分析

由于全黑或全白的图像能够令混淆效果失效，攻击者往往会选取此类特殊图像作为明文，用来分析、破译密码算法。为了应对这一挑战，本文方法先对三维映射符号进行缩放加密，再对组合的I/Q信号进行EWFRFT处理，主要目的是破坏传输信号的分布规律，保护通信的调制方式。同时，该方法能够对原始信息进行置乱和扩散，从而具备一定的应对已知明文和选择明文攻击的能力。运用本文方法对全黑图像进行加密，结果如图8所示。由图8可以看出，经过本文方法加密后的原始图像信息已经被有效隐藏。由此可见，本文方法可以有效抵御已知明文和选择明文攻击，保证通信的安全性。



(a) 原始全黑图像　　(b) 加密图像

图8　全黑图像的加密效果

3.6　误比特率分析

信号在空间传播过程中通常会受到噪声的干扰，这可能导致传输错误信息。为了评估本文方法对误比特率的影响，对比该方法对4-ray三维星座加密与QPSK理论值的误比特率，结果如图9所示。从图9可以明显看出，本文方法具有更低的误比特率。这是由于三维星座图相较于二维星座图，具有更大的最小欧氏距离，使得在发射能量相同的条件下，接收端的误比特率得以有效降低。此外，仿真结果进一步验证了本文提出的在判决区域内对星座点进行缩放加密的技术。在缩放因子取值范围$[0.8,1.6]$内，没有造成误比特率损耗，能够实现信息的准确、可靠传输，证明了该方法的有效性。同时，实验结果表明，本文给出的缩放因子取值范围还可以进一步拓宽，在保证加密效果的同时，不会带来额外的误码率。

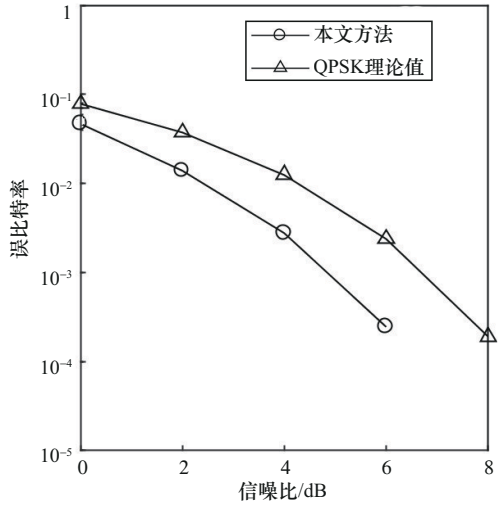


图9　误比特率分析

4　结束语

针对无线通信信号易遭截获分析、干扰破坏等安全问题，本文将混沌加密与EWFRFT相结合，提出一种三维星座缩放加密的EWFRFT安全通信方法。不同于比特层面加密，本文所提的三维星座缩放加密是在密钥的作用下，对三维调制后的星座符号进行可逆的数学变换。具体来说，通过Hénon和Logistic映射控制三维布朗运动的参数，生成具有更好随机性的序列，并将其作为缩放操作的方向矢量与缩放因子，进一步构造随机缩放矩阵，对每个三维星座点进行缩放加密。该密码方法属于“一符号一密钥”体制，具有理论上的完全保密性。随后，对缩放加密和组合后的I/Q信号进行变参数EWFRFT处理。仿真结果表明，该加密方法能够有效消除原始基带调制信号的分布规律、对抗信号的统计攻击及密钥的穷举攻击，显著提高了无线传输信号的抗检测识别能力。同时，仅对三维调制星座符号进行缩放加密，信号仍具有一定的分布规律。尽管通过EWFRFT处理能够消除这一缺陷，但仍无法完全排除单纯缩放加密可能存在的信息泄露问题。因此，在后续的工作中，将着重探索多种三维空间物体运动方式的有效结合，以构造更优良的星座置乱加密技术，从而进一步提升无线系统的安全性。

附录1　三维星座缩放加密是双射

证明　首先证明三维星座缩放加密是单射。

假设有2个不同的调制星座符号a和b，经过相同的缩放运算后得到相同的星座符号c，设缩放矩阵为$\boldsymbol{S}$，则

$$a\boldsymbol{S} = c \tag{28}$$

$$b\boldsymbol{S} = c \tag{29}$$

两式相减可得

$$(a - b)\boldsymbol{S} = 0 \tag{30}$$

由于缩放因子$k \neq 0$，因此缩放矩阵$\boldsymbol{S}$可逆，则有

$$a - b = 0 \tag{31}$$

即$a = b$，与假设矛盾。故三维星座缩放加密是单射。

然后，证明三维星座缩放加密是满射，即对于任意密文符号c，需要找到一个点a，经过缩放运算后得到c。

假设$a = c\boldsymbol{S}^{-1}$，则有

$$a\boldsymbol{S} = c\boldsymbol{S}^{-1}\boldsymbol{S} = c \tag{32}$$

故三维星座缩放加密是满射。

综上所述，三维星座缩放加密既是单射又是满射，即三维星座缩放加密是双射。

证毕。

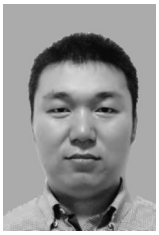
参考文献：

[1] WANG J, WANG X X, GAO R F, et al. Physical layer security for UAV communications: a comprehensive survey[J]. China Communications, 2022, 19(9): 77-115.

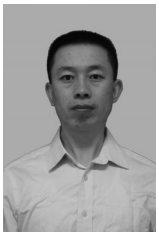
[2] HAJOMER A A E, YANG X L, HU W S. Secure OFDM transmission precoded by chaotic discrete hartley transform[J]. IEEE Photonics Jour-

nal, 2018, 10(2): 7901209.
[3] KHAN M A, ASIM M, JEOTI V, et al. On secure OFDM system: Chaos based constellation scrambling[C]//Proceedings of the 2007 International Conference on Intelligent and Advanced Systems. Piscataway: IEEE Press, 2007: 484-488.
[4] ZHONG J, YANG X L, HU W S. Performance-improved secure OFDM transmission using chaotic active constellation extension[J]. IEEE Photonics Technology Letters, 2017, 29(12): 991-994.
[5] YERRAPRAGADA A K, EISMAN T, KELLEY B. Physical layer security for beyond 5G: ultra secure low latency communications[J]. IEEE Open Journal of the Communications Society, 2021, 2: 2232-2242.
[6] 倪磊, 达新宇, 胡航, 等. 基于改进Logistic相位扰码的抗截获通信[J]. 华中科技大学学报(自然科学版), 2019, 47(6): 35-40.
NI L, DA X Y, HU H, et al. Research on anti-interception communication based on improved Logistic phase scrambling[J]. Journal of Huazhong University of Science and Technology (Natural Science Edition), 2019, 47(6): 35-40.
[7] 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.
[8] 岳敖, 李为, 马东堂, 等. 拉丁阵和幅相变换相结合的物理层加密传输算法[J]. 信号处理, 2016, 32(6): 660-668.
YUE A, LI W, MA D T, et al. A novel physical layer encryption algorithm combined Latin rectangle and phase-amplitude mask[J]. Journal of Signal Processing, 2016, 32(6): 660-668.
[9] 李小倩, 李为, 雷菁, 等. OFDM系统中基于三维星座旋转的物理层安全加密算法[J]. 电子学报, 2017, 45(12): 2873-2880.
LI X Q, LI W, LEI J, et al. A novel physical layer encryption algorithm based on three dimensional constellation rotation in OFDM system[J]. Acta Electronica Sinica, 2017, 45(12): 2873-2880.
[10] 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.
[11] 于浩洋, 孟庆微, 贠彦直, 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.
[12] 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.
[13] DUNN F, PARBERRY I. 3D math primer for graphics and game development[M]. Boca Raton: CRC Press, 2011.
[14] 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.
[15] ZHANG W, ZHANG C F, CHEN C, et al. Experimental demonstration of security-enhanced OFDMA-PON using chaotic constellation transformation and pilot-aided secure key agreement[J]. Journal of Lightwave Technology, 2017, 35(9): 1524-1530.
[16] ZHANG C F, ZHANG W, HE X J, et al. Physically secured optical OFDM-PON by employing chaotic pseudorandom RF subcarriers[J]. IEEE Photonics Journal, 2017, 9(5): 7204408.
[17] 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.
[18] FANG X J, SHA X J, ZHANG N, et al. Towards PHY-aided authentication via weighted fractional Fourier transform[C]//Proceedings of the 2016 IEEE 84th Vehicular Technology Conference (VTC-Fall). Piscataway: IEEE Press, 2016: 1-5.
[19] 王浩波, 达新宇, 倪磊, 等. 基于DL-MPWFRFT卫星混沌加密通信研究[J]. 测控技术, 2019, 38(9): 98-102.
WANG H B, DA X Y, NI L, et al. Research on satellite chaotic encryption communication based on DL-MPWFRFT[J]. Measurement & Control Technology, 2019, 38(9): 98-102.
[20] 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.
[21] 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.
[22] LIU F. A cross-hierarchical scanning method based SP-4-WFRFT for digital communication signals[J]. Mathematical Problems in Engineering, 2018(1): 6580146.
[23] 马聪. 基于WFRFT的扩展混合载波信号设计与性能分析[D]. 哈尔滨: 哈尔滨工业大学, 2019.
MA C. Design and performance analysis of extended hybrid carrier signals based on WFRFT[D]. Harbin: Harbin Institute of Technology, 2019.

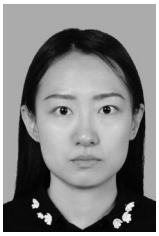
[作者简介]



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



贠彦直（1988– ），男，甘肃定西人，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。



王晗（1989– ），女，陕西西安人，博士，空军工程大学讲师，主要研究方向为通信信号处理、网络层协议。