引用本文:常馨宇,邓涛,张琳. 一种基于混沌加密的奇数阶正交变换辅助 MIMO 收发机设计[J]. 光通信技术,2025,49(2):57-63.

# 一种基于混沌加密的奇数阶正交变换辅助 MIMO 收发机设计

常馨宇[1],邓 涛[2],张 琳[1*]
(1.中山大学 网络空间安全学院,广东 深圳 518000;2.中山大学 电子与信息工程学院,广州 510006)

**摘要**:针对水下可见光多输入多输出(MIMO)通信系统天线配置自由度低和安全性不足的问题,设计一种基于混沌加密的奇数阶正交变换辅助的水下可见光MIMO收发机。首先,提出了奇数阶正交矩阵生成算法,提升了水下可见光通信系统的可拓展性。其次,使用双混沌加密算法对传输数据进行加密,提升了水下可见光通信系统的信息传输安全性。仿真结果表明,相较于基准方案,该方案具有更优的可靠性和安全性性能。

**关键词**:水下可见光通信; 多输入多输出; 正交变换; 混沌加密; 安全性
**中图分类号**:TN91　**文献标志码**:A　**文章编号**:1002-5561(2025)02-0057-07
DOI:10.13921/j.cnki.issn1002-5561.2025.02.011　开放科学(资源服务)标识码(OSID):

# Design of an odd order orthogonal transform assisted MIMO transceiver based on chaotic encryption

CHANG Xinyu[1], DENG Tao[2], ZHANG Lin[1*]
(1. School of Cyber Science and Technology, Sun Yat-sen University, Shenzhen Guangdong 518000, China;
2. School of Electronics and Information Technology, Sun Yat-sen University, Guangzhou 510006, China)

**Abstract**: Aiming at the issues of low antenna configuration freedom and insufficient security in underwater visible light multiple-input multiple-output(MIMO) communication systems, a design for an underwater visible light MIMO transceiver assisted by odd-order orthogonal transformation based on chaotic encryption is proposed. Firstly, an odd-order orthogonal matrix generation algorithm is introduced to enhance the scalability of underwater visible light communication systems. Secondly, a dual chaotic encryption algorithm is employed to encrypt the transmitted data, improving the information transmission security of underwater visible light communication systems. Simulation results indicate that compared to baseline schemes, this approach offers superior reliability and security performance.

**Key words**: underwater visible light communication, multiple input multiple output, orthogonal transform, chaotic encryption, security

## 0 引言

近年来,水下可见光通信(UVLC)因其丰富的频谱资源、强大的抗电磁干扰能力以及高速的数据传输率受到了广泛关注[1-2]。然而,在水下通信环境中,路径损耗、信道衰落和湍流闪烁效应会导致传输光信号的幅度和相位失真,从而降低 UVLC 系统的传输可靠性。为此,研究人员将多输入多输出(MIMO)技术引入 UVLC 系统中,通过利用额外的空间分集增益来对抗信道衰落效应。

在现有研究中,基于重复编码(RC)、空间复用(SMP)和空间调制(SM)的 MIMO UVLC 系统[3]被广泛探讨并取得了一定成果。此外,极化编码[4]和准相干 MIMO[5]传输方案的应用也在一定程度上抑制了湍流闪烁效应。还有学者提出了基于正交频分复用(OFDM)的多用户预编码 VLC 系统[6],以及结合全空分多址(SDMA)和准正交多址(QOMA)的 MIMO 传输方案[7],提升了系统的误码率性能和可靠性。文献[8]提出了一种正交变换

**收稿日期**:2024-06-16。

**作者简介**:常馨宇(2003—),男,辽宁锦州人,中山大学网络空间安全学院本科生,主要研究方向是通信安全、对抗攻击、人工智能安全等,曾担任中山大学大学生创新训练国家级项目“AI 安全-物理攻击与防御方法”的组长,已公开的专利 1 项,发表中文核心期刊文章 1 篇。
*** 通信作者**:张琳(1976—),女,博士,教授,硕士生导师,主要研究方向为人工智能、数据分析与特征提取、智能通信等新一代无线通信、网络和通信安全。

(OT)辅助的 MIMO 传输方案。然而,该方案限制了发射和接收孔径数量为二的整数次幂,这削弱了天线阵列的方向性和波束赋形能力,降低了系统的可扩展性和适应性。目前,许多现有方案主要关注系统的可靠性,而忽视了数据传输过程中可能产生的信息泄露问题,缺乏足够的数据机密性保护措施,导致整体安全性不足。因此,本文提出一种基于混沌加密的奇数阶 OT 辅助 MIMO 收发机设计方案。

## 1 系统模型

### 1.1 发射机结构

根据提出的混沌加密与奇数阶 OT 辅助的MIMO 收发机设计思路, 本文首先设计一种多用户 UVLC MIMO 通信系统发射机,其结构如图 1 所示。该结构主要分为双混沌数据加密模块、OT 模块和预编码模块三部分,能够有效保障数据传输的可靠性和安全性。在 MIMO 的 VLC 系统中,一个基站(例如海洋中的一艘船)可以通过发射机同时向多个用户(如自主水下航行器或潜艇)传输数据。本设计中的发射机拥有 $N_t$ 个发射孔,用于向 $K$ 个用户发送数据,而第 $j$ 个用户使用 $N_{r,j}$ 个孔径的接收器接收数据。因此,所有用户接收孔的数量为 $N_r=\sum_{j=1}^{j=K}N_{r,j}$。

#### 1.1.1 双混沌数据加密模块

首先,在发射端,用户比特流数据 $b_0,b_1,\cdots,b_n$ 经过双混沌数据加密模块进行加密,然后得到加密比特流数据 $b_0',b_1',\cdots,b_n'$。本文采用基于双混沌系统的数字混沌加密算法对用户数据比特进行加密。双混沌数据加密和解密算法流程图如图 2 所示。在加密过程中,本文使用了 Cat 映射和 Logistic 映射。

Cat 映射是一个二维可逆混沌映射,其表达式为

$$\begin{bmatrix}x_{n+1}\\y_{n+1}\end{bmatrix}=\begin{bmatrix}1 & a\\ b & ab+1\end{bmatrix}\begin{bmatrix}x_n\\y_n\end{bmatrix}\bmod 1 \tag{1}$$

其中,$a$、$b$ 为控制参数,$x_n$、$y_n$ 为第 $n$ 次映射迭代的中间结果,$x_{n+1}$、$y_{n+1}$ 为第 $n+1$ 次映射迭代的中间结果,mod1 表示只取小数部分。

Logistic 映射是一种自包含的一维离散动力系统,它通过非线性的迭代函数产生混沌信号,其表达式为

$$x_{n+1}=(\beta+1)\left(1+\frac{1}{\beta}\right)^{\beta}x_n(1-x_n)^{\beta} \tag{2}$$

其中, 初始值 $x_0\in(0,1)$;$\beta$ 为控制参数, 取值范围为 1~4。

发射机首先对二进制明文序列流按照位数 $M$ 进行分割,进而对长度 $M$ 的二进制比特流数据 $m$ 进行循环移位加密,此过程可以表示为

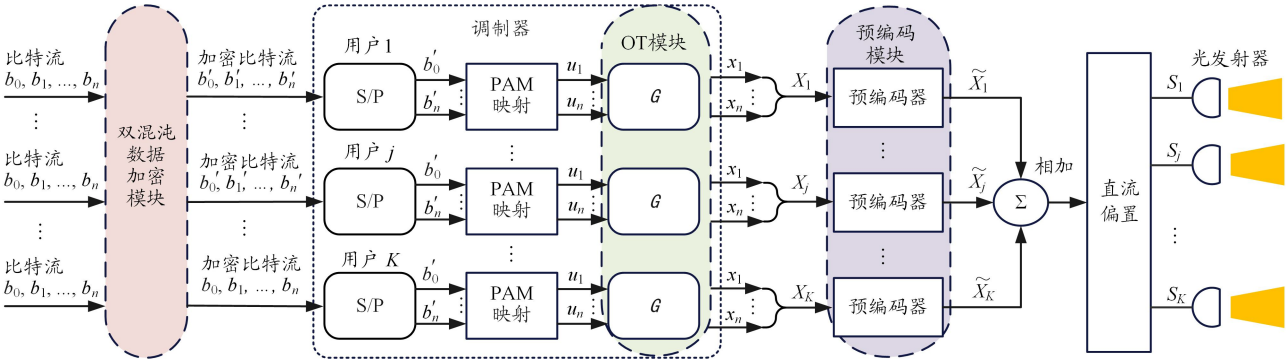


图 1 多用户 UVLC MIMO 通信系统的发射机结构

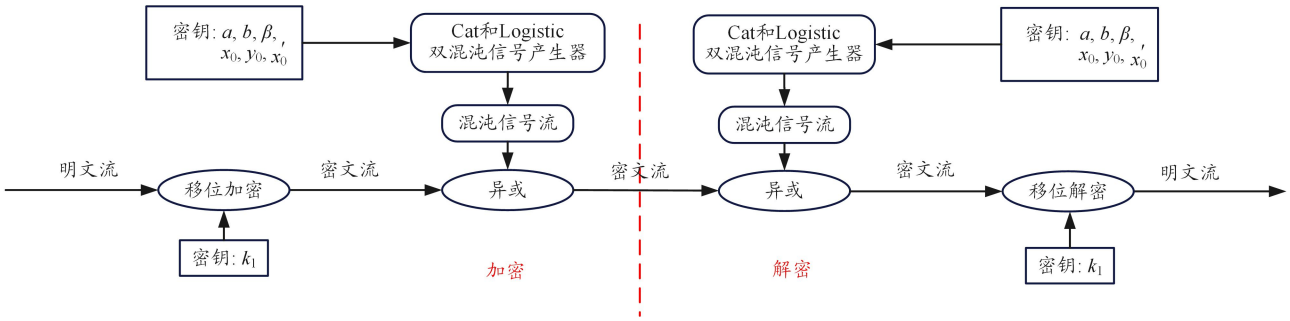


图 2 双混沌数据加密和解密算法流程图

$$c_1 \equiv (m+2k_1) \bmod (2^M) \tag{3}$$

其中,$c_1$为密文流,$k_1$为密钥。

发射机对完成初步加密后的密文流 $c_1$进行双混沌数据加密。双混沌数据加密算法中所使用的密钥包括混沌初始值 $x_0$、$y_0$、$x_0'$和控制参数 $a$、$b$、$\beta$。双混沌数据加密算法具体步骤如下:

步骤 1:选择参数 $a$、$b$和 $\beta$,并将 $x_0$、$y_0$和 $x_0'$作为 Cat 映射和 Logistic 映射的初始值,最终将上述参数和初始值组合作为加密密钥。

步骤 2:迭代 200 次得到 $x_n$、$y_n$、$x_0'$。

步骤 3:计算 $x_n \times y_n \times x_0' \times 100$,并取乘积小数点后的第 3、5、7、9、11、13 位组成一个六位十进制数。这个数对 $2^M$取模可以得到一个 $M$ 位的密钥流。在密钥流和移位加密得到的密文之间进行异或运算,得到最终的密文。

步骤 4:再迭代 5 次得到 $x_{n+1}$、$y_{n+1}$、$x_0'+1$。

重复步骤 3 和步骤 4,直到移位加密的所有初始密文都被进一步加密。

### 1.1.2 OT模块

双混沌数据加密后的用户数据比特经过串行/并行(S/P)转换后,被调制成脉冲幅度调制(PAM)符号,表示为 $u_1, u_2, \cdots, u_p, u_p \in \mathrm{U}$,U 表示 $M$-PAM 星座图,再由所提出的 OT 得到要传输给用户 $j$ 的调制信号 $X_j$,对 $X_j$进行预编码运算后,得到信号 $\tilde{X}_j$。

PAM 符号向量 $\boldsymbol{u}$ 由 $p \times p$ 维的正交矩阵 $\boldsymbol{G}$ 变换,如式(4)所示。

$$\boldsymbol{X}=\boldsymbol{G}\boldsymbol{u} \tag{4}$$

其中,$\boldsymbol{u}=[u_1, u_2, \cdots, u_p]^{\mathrm{T}}$,$p=N_{\mathrm{t}}-\tilde{L}_j$,$\tilde{L}_j$为信道矩阵的秩,$\boldsymbol{X}$是完成 OT 的符号向量。当 $p=3$ 时,正交矩阵的形式为

$$\boldsymbol{G}_{3\times3}(a,b,c,d)=\begin{bmatrix} ad & -b & ac \\ bd & a & bc \\ -c & 0 & d \end{bmatrix} \tag{5}$$

其中,$a$、$b$、$c$、$d$是取值范围为[-1,1]的实数。为了确保发射功率保持恒定,系统将对 $a$、$b$、$c$、$d$进行归一化,使得$\sqrt{a^2+b^2}=1$且$\sqrt{c^2+d^2}=1$。因此,本文使用暴力搜索方法来求取 $a$、$b$、$c$、$d$的最优值时,算法只需计算 $a$ 和 $c$ 的值即可。$a$、$c$的搜索算法如算法 1 所示。

**算法 1** $a$、$c$的搜索算法

**输入**:信道奇异值矩阵 $\Lambda$

**输出**:$a, c$

1)初始化 $g_0=0$; $a_0=1$; $c_0=-1$;
2)for $\dot{a}$ =[-1,1] 执行
3) 计算 $\dot{b}=\sqrt{1-\dot{a}^2}$;
4) for $\dot{c}$ =[-1,1] 执行
5) 计算 $\dot{d}=\sqrt{1-\dot{c}^2}$;
6) $d_0=\infty$;
7) for $i$=1 to $M^{p-1}$ 执行
8) $t_0=\infty$;
9) for $j$=$i$+1 to $M^p$执行
10) 计算 $\boldsymbol{G}_{p\times p}=\boldsymbol{G}_{3\times3}(\dot{a},\dot{b},\dot{c},\dot{d})$;//$\dot{a}$, $\dot{b}$, $\dot{c}$, $\dot{d}$是迭代过程中对应最终结果 $a$、$b$、$c$、$d$的中间变量
11) 计算 $t_1=\| \Lambda \boldsymbol{G}(\dot{u}^i-\dot{u}^i) \|_F^2$;
12) if $t_1 \leqslant t_0$ then
13) $t_0=t_1$;//$t_0$ 是记录最小临时值的变量(初始为无穷大以便更新)
14) end
15) end
16) if $t_0 \leqslant d_0$ then
17) $d_0=t_0$;
18) end
19) end
20) if $d_0 \geqslant g_0$ then
21) $a_0=\dot{a}$; $c_0=\dot{c}$; $g_0=d_0$;
22) end
23) end
24)end
25)返回 $a=a_0$; $c=c_0$

### 1.1.3 预编码模块

经 OT 后的用户数据进行预编码以抑制多用户干扰(MUI),此过程可以表示为

$$\tilde{X}_j=\boldsymbol{P}_j X_j \tag{6}$$

其中,$\boldsymbol{P}_j$为预编码矩阵。不失一般性,本文假设发射机能够获得完美的信道状态信息(CSI)估计,且第 $j$ 个用户信号所经历的信道矩阵为 $\boldsymbol{H}_j$,互补信道矩阵$\tilde{\boldsymbol{H}}_j=[\boldsymbol{H}_1^{\mathrm{T}}, \cdots, \boldsymbol{H}_{j-1}^{\mathrm{T}}, \boldsymbol{H}_j^{\mathrm{T}}, \cdots, \boldsymbol{H}_K^{\mathrm{T}}]^{\mathrm{T}}$。

在预编码模块中,发射机首先对信道矩阵$\overline{\boldsymbol{H}}_j$和互补信道矩阵$\tilde{\boldsymbol{H}}_j$进行奇异值分解(SVD),此过程可表示为

$$\overline{\boldsymbol{H}}_j=\boldsymbol{H}_j\widetilde{\boldsymbol{V}}_j^{(0)}=\boldsymbol{U}_j\boldsymbol{\Lambda}_j\boldsymbol{V}_j^{\mathrm{T}} \tag{7}$$

$$\widetilde{\boldsymbol{H}}_j=\widetilde{\boldsymbol{U}}_j\widetilde{\boldsymbol{\Lambda}}_j\left[\widetilde{\boldsymbol{V}}_j^{(1)}\middle|\widetilde{\boldsymbol{V}}_j^{(0)}\right]^{\mathrm{T}} \tag{8}$$

其中,$\overline{\boldsymbol{H}}_j$的尺寸为 $N_{\mathrm{r},j}(N_{\mathrm{t}}-\tilde{L}_j)$;正交矩阵$\widetilde{\boldsymbol{U}}_j$、$\boldsymbol{U}_j$、$\boldsymbol{V}_j$的尺寸分别为$(N_{\mathrm{r}}-N_{\mathrm{r},j})(N_{\mathrm{r}}-N_{\mathrm{r},j})$、$N_{\mathrm{r},j}N_{\mathrm{r},j}$和$\left(N_{\mathrm{t}}\tilde{L}_j\right)\left(N_{\mathrm{t}}\tilde{L}_j\right)$;$\widetilde{\boldsymbol{V}}_j^{(0)}$是构成$\widetilde{\boldsymbol{H}}_j$零空间的一组基,使得$\widetilde{\boldsymbol{H}}_j\times\widetilde{\boldsymbol{V}}_j^{(0)}=0$;$\widetilde{\boldsymbol{\Lambda}}_j$和$\boldsymbol{\Lambda}_j$分别为$\widetilde{\boldsymbol{H}}_j$和$\overline{\boldsymbol{H}}_j$进行 SVD 后得到的对角矩阵,$\boldsymbol{U}_j$、$\boldsymbol{V}_j$是$\overline{\boldsymbol{H}}_j$进行 SVD 后得到的正交矩阵。

基于$\widetilde{\boldsymbol{V}}_j^{(0)}$和$\boldsymbol{V}_j$可计算得到的预编码矩阵$\boldsymbol{P}_j$为

$$\boldsymbol{P}_j=\widetilde{\boldsymbol{V}}_j^{(0)}\boldsymbol{V}_j \tag{9}$$

然后,发射机将经预编码后的 $K$ 个用户的数据信号进行叠加,并添加直流偏置 $d_{\mathrm{c}}$,以确保传输信号非负,所得到的发射信号可表示为

$$\boldsymbol{S}=\sum_{j=1}^{K}=(\widetilde{\boldsymbol{X}}_j)+d_{\mathrm{c}}=\sum_{j=1}^{K}(\boldsymbol{P}_j\boldsymbol{X}_j)+d_{\mathrm{c}}=[S_1,S_2,\cdots,S_{N_{\mathrm{t}}}]^{\mathrm{T}} \tag{10}$$

最后,发射信号 $\boldsymbol{S}$通过 $N_{\mathrm{t}}$ 个发射孔径进入信道进行传输。

### 1.2 水下可见光信道模型

水下可见光信道的信道系数 $h$ 可建模为路径损耗和衰落的组合[9-10],其表达式为

$$h=h_{\mathrm{l}}h_{\mathrm{t}} \tag{11}$$

其中,$h_{\mathrm{l}}$为路径损耗系数,$h_{\mathrm{t}}$为湍流效应引起的信道衰落系数。

由于水下环境中,可见光信号的路径损耗会受到吸收和散射效应的影响,难以用明确的数学模型进行描述,故本文采用蒙特卡罗(MC)方法[11]对 $h_{\mathrm{l}}$进行仿真。

信道衰落系数 $h_{\mathrm{t}}$与水下环境中存在的湍流效应有关,湍流效应会导致光强的波动,波动强度可通过对数强度方差[10,12]进行建模,其表达式为

$$\sigma_{\ln I}^2=8\pi^2k^2\int_0^L\int_0^\infty\kappa\Phi_n(\kappa)\times\left\{1-\cos\left[\frac{\kappa^2z}{k}(1-(1-\Theta)z)\right]\right\}\mathrm{d}\kappa\mathrm{d}z \tag{12}$$

其中,$\Theta$=0 和 1 分别代表球面波和平面波。$k$ 为波数,$\kappa$ 和 $\Phi_n(\kappa)$分别为湍流波动的标量空间频率和功率谱,$I$ 为接收信号强度,$L$ 为传播距离,$z$ 为距离光源的距离。当传输光信号为平面波时,对数强度方差 $\sigma_{\ln I}^2$可以简化为 Rytov 方差 $\sigma_R^2$[12-13],其表达式为

$$\sigma_{\ln I}^2=\sigma_R^2=1.23C_n^2k^{\frac{7}{6}}L^{\frac{11}{6}} \tag{13}$$

其中,$C_n^2$为折射率结构参数,取值范围为 $10^{-17}$~$10^{-12}$,折射率结构参数取值的变化可以控制湍流效应的强度。闪烁指数 $\sigma_I^2$可以用 $\sigma_I^2=\frac{\mathrm{E}[I^2]-\mathrm{E}^2[I]}{\mathrm{E}^2[I]}$来估计,$\mathrm{E}[\cdot]$表示求期望(平均值)。基于弱涨落理论,$\sigma_I^2=\exp\left(\sigma_{\ln I}^2\right)-1\backsimeq\sigma_{\ln I}^2$[12]。在弱湍流情况下,即当 $\sigma_I^2<1$ 时,衰落信道系数 $h_{\mathrm{t}}$ 服从对数正态分布[10,14];在中等或强湍流条件下,$h_{\mathrm{t}}$ 服从伽马-伽马分布[9,15]。

### 1.3 接收机结构

系统接收机结构如图 3 所示。第 $j$ 个用户的接收信号量 $y_j$可表示为

$$y_j=\boldsymbol{H}_j s+n_j \tag{14}$$

其中,$n_j$为加性高斯白噪声(AWGN)向量,其均值为 0,方差 $\sigma_n^2=\sigma_{\mathrm{b}}^2+\sigma_{\mathrm{d}}^2+\sigma_{\mathrm{th}}^2$,其中,$\sigma_{\mathrm{b}}^2$、$\sigma_{\mathrm{d}}^2$、$\sigma_{\mathrm{th}}^2$分别表示背景噪声、暗电流噪声和热噪声的方差[16]。接收信号 $y_j=[y_{j,1},y_{j,2},\cdots,y_{j,N_{\mathrm{r},j}}]^{\mathrm{T}}$通过 $N_{\mathrm{r},j}$个发射孔径接收。

在接收端,对用户接收到的信号首先去除直流偏置得到$\overline{R}_j$信号,其表达式为

$$\overline{R}_j=\boldsymbol{\Lambda}_j\mathrm{x}_j+\boldsymbol{U}_j^{\mathrm{T}}n_j=\boldsymbol{\Lambda}_j\boldsymbol{G}_ju_j+\boldsymbol{U}_j^{\mathrm{T}}n_j \tag{15}$$

由于 $\boldsymbol{\Lambda}_j$为对角矩阵,$\overline{R}_j$可以进一步表示为

$$\overline{R}_j=\begin{bmatrix}\overline{R}_1\\\vdots\\\overline{R}_{N_{\mathrm{r},j}}\end{bmatrix}=\begin{bmatrix}\lambda_1x_1\\\vdots\\\lambda_{N_{\mathrm{r},j}}x_{N_{\mathrm{r},j}}\end{bmatrix}+\begin{bmatrix}\tilde{n}_1\\\vdots\\\tilde{n}_{N_{\mathrm{r},j}}\end{bmatrix} \tag{16}$$

其中,$\tilde{n}_i$为经逆 OT 后的噪声向量,$\lambda_i$为对角矩阵 $\boldsymbol{\Lambda}_j$的第 $i$ 个对角线元素。

最后,系统进行最大似然(ML)检测,从$\overline{R}_j$中恢复

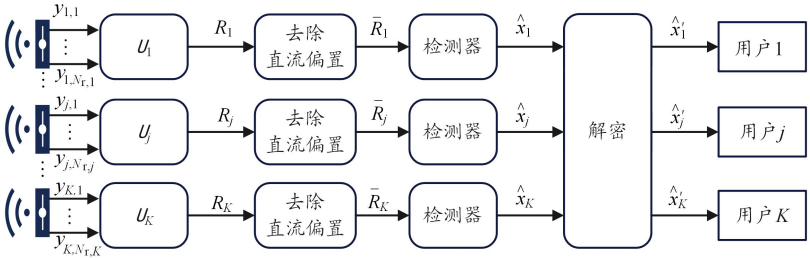


图 3 系统接收机结构图

加密信号 $x_j$,此过程可以表示为

$$\hat{x}_j=\underset{x_j}{\operatorname{argmax}}\ p(R_j\mid x_j,\Lambda_j)=\underset{x_j}{\arg\max}\ \|\bar{R}_j-\Lambda_j x_j\|_F^2 \quad (17)$$

其中,$\|\cdot\|_F$表示 Frobenius 范数,$\hat{x}_j$表示 $x_j$的估计值。然后,系统将对$\hat{x}_j$进行解密,解密过程与加密步骤相反。解密步骤如下:先将混沌加密过程中步骤 3 产生的 $M$ 位的密钥流与密文流异或,得到初步的密文流 $c_1$;再进行移位解密,移位解密过程可以表示为

$$m\equiv(c_1-2k_1)\bmod(2^M) \quad (18)$$

由此,恢复得到用户的二进制比特流数据 $m$。

## 2 数值仿真结果

本文对所提出的方案在安全性方面的性能进行分析,并基于 UVLC 信道环境,通过仿真研究验证该方案的有效性。同时,还将所提方案与现有方案对比分析,以全面评估其性能优势。

### 2.1 仿真参数设置

系统的仿真参数设置主要参考文献[8],具体如表 1 所示。该系统配置了 6 个发射孔径和 2 个用户,每个用户的接收孔径数量为 3,正交矩阵尺寸设定为 3×3。此外,接收孔径直径被设置为 5 cm[14],与链路的相干长度相匹配,因此无需进行孔径平均处理。本文假设相邻孔径之间的距离大于横向相干长度(或相干半径),因此不同发射和接收孔径之间的信道是统计独立的。参考文献[17],将发射机的发散半角设为 0.5°,以确保覆盖要求得到满足。

为了确保比较的公平性,将不同方案的频谱效率 $\zeta$ 保持一致,均为 6 b·s$^{-1}$·Hz$^{-1}$。为满足这一要求,本文方案和 SMP 方案的调制方式均采用 4PAM,RC 方案采用 64PAM[3-4]。

表 1 系统参数设置

| 参数 | 值 |
|---|---|
| 光源 | 激光 |
| 波束宽度/mm | 3 |
| 束波长 $\lambda_0$/mm | 532 |
| 光到电的转换效率 $\eta$ | 1 |
| 接收机 FOV 半角 $\Psi(1/2)$/(°) | 45 |
| 接收机孔径 $D$/m | 0.05 |
| 发射机发散半角 $\Phi(1/2)$/(°) | 0.5 |
| 接收器间隔距离 $s_r$/m | 0.25 |
| 发射机间隔距离 $s_t$/m | 0.25 |

### 2.2 安全性能分析

#### 2.2.1 密钥分析

首先,在本文提出的双混沌数据加密算法中,选择了 2 个内部控制参数和 3 个初始状态作为密钥。其中,3 个混沌系统的初始值 $x_0$、$y_0$、$x_0'$可以在全体实数域内自由选取,这提供了极其庞大的密钥空间。其次,即便攻击者知晓加密算法使用了 Cat 映射和 Logistic 映射,并试图绕过直接的穷举密钥攻击而通过推算 3 个内部控制参数($a$ 和 $b$)的方式进行破解,此方法亦难以实现。

为了测试系统的密钥敏感性,本文进行以下实验。首先,保持 Cat 映射和 Logistic 映射的迭代初始值 $x_0$、$x_0'$不变,仅将 $y_0$ 增加 $10^{-15}$,然后观察 2 个加密后的 6 位二进制消息的归一化占比分布结果。接着,保持 $x_0$、$y_0$ 不变,而将 $x_0'$增加 $10^{-15}$,并记录 2 个加密后的六位二进制消息的归一化占比分布结果。实验结果显示,不论是改变 $x_0'$还是 $y_0$,即使只改变了极小的一个值,所得到的加密消息之间也表现出显著差异。这表明此加密算法对密钥具有高度敏感性,任何对密钥的微小更改都会导致完全不同的加密结果。因此,暴力破解攻击的效率会显著降低。

#### 2.2.2 合法用户和窃听者误符号率(SER)性能分析

合法用户和窃听者的 SER 性能对比如图 4 所示。可以看出,两者在接收加密信号时的 SER 表现出显著差异。鉴于合法用户持有正确的解密密钥并熟悉相应的加解密算法,他们能够高效地从加密信号中恢复原始信息,并成功进行信息解调。因此,其 SER 较低,这表明数据传输具有较高的准确性。相比之下,尽管窃听者能够接收到信号,但由于缺乏必要的密钥信息和相应的解密算法,他们无法准确地解码原始信号。这

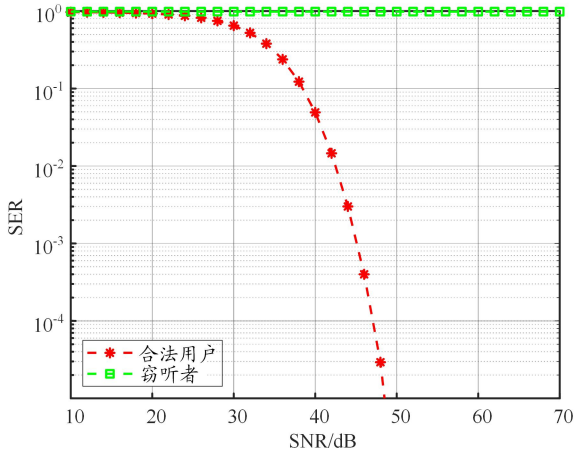


图 4 合法用户和窃听者之间的 SER 性能比较

导致了窃听者的 SER 偏高,意味着接收数据中存在显著的误码率,从而无法有效地获取或理解实际传输的信息内容。

### 2.3 方案对比分析

#### 2.3.1 加密方案比较

1)统计学分析对比:加密算法的统计学特性可以通过对比加密前后的柱形图进行分析。实验结果显示,移位加密和异或加密的加密方案可以很容易地根据消息的统计学规律由密文推测出明文。与移位加密和异或加密的方案相比,本文提出的混沌加密方案在加密前后的统计学特性表现出显著变化。这种变化有效地隐藏了明文的统计学特性,使得攻击者难以推断出数据的模式和结构,从而增强了抵抗频率分析的能力,并提高了整体的抗攻击性能。

2)敏感性分析对比:本文采用了一种在图像加密领域常用的指标——归一化平均变化强度 (UACI)来评估这种密钥敏感性。对于一个理想的加密算法来说,UACI 的理想值约为 33.463 5%。本文对移位加密、异或加密与本文混沌加密方案之间的 UACI 值进行了对比分析。对每种加密方法进行了 100 次 UACI 计算,并统计了这些结果的平均值。在进行的 100 次试验中,移位加密的 UACI(统一平均变化强度)值波动范围在 39.5%~41.5%之间,平均值达到了 40.405 1%。这一结果与理想值相比存在较大差距。异或加密的 UACI 值在这 100 次测试中的范围是 6.2%~6.35%,平均值为 6.250 1%,与理想值相差甚远。而本文混沌加密方案的 UACI 值在 32%~34.5%内变动, 平均值为 33.305 4%,非常接近理想的 33.463 5%值。

由此可知,本文混沌加密算法对密钥具有高度敏感性。

#### 2.3.2 安全容量的比较

为了定量评价安全性能,本文对不同方案的安全容量进行了比较,如图 5 所示。可以看出,当其它参数相同时, 本文方案的安全容量始终远高于 RC 方案和 SMP 方案。

#### 2.3.3 可靠性比较

在仿真实验中, 信号通过 20 m 的清水介质进行传输。实验设定水体环境为弱湍流区,使用对数正态分布模型模拟湍流效应,其参数 $\sigma_l^2$ 设为 0.05。在水下弱湍流信道环境下, 不同方案的 SER 对比如图 6 所示。可以看出,当 SER 为 $10^{-5}$ 时,本文方案相较于 RC 方案表现出大约 10 dB 的 SNR 性能优势; 而在 SER 达到 $5\times10^{-2}$ 时,本文方案相对于 SMP 方案的优势扩大至约 20 dB,并随着 SER 的下降两者的差距增大。

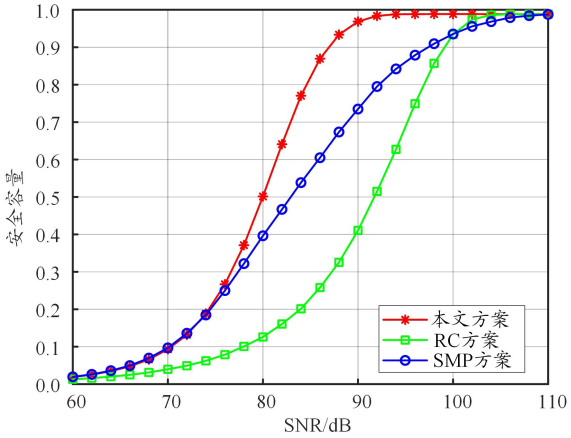


图 5 安全容量的比较

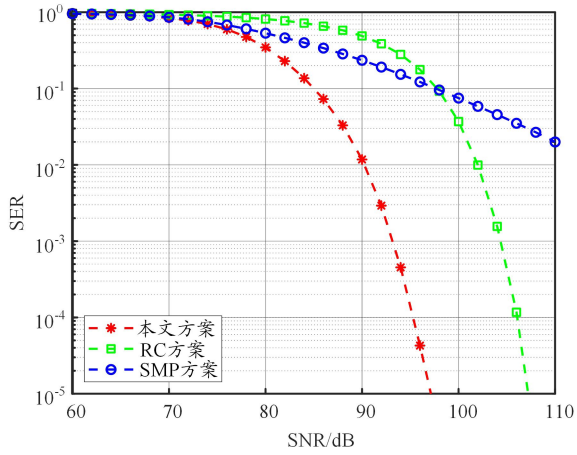


图 6 在水下弱湍流信道环境下,不同调制方案的性能比较

在中等湍流信道环境($\sigma_l^2$ = 1.23)下,采用 γ–γ 模型来模拟湍流效应,得到不同方案时的 SER 对比情况如图 7 所示。可以看出,本文方案在 SER 为 $10^{-3}$ 时的 SNR 性能优于 RC 方案约 11 dB;在 SER 为 $5\times10^{-2}$ 时,本文方案的 SNR 性能优于 SMP 方案约 20 dB,并随着 SER 的下降,两者的差距增大。

在强湍流条件($\sigma_l^2$ = 1.85)下,采用 γ–γ 模型进行分析,如图 8 所示。可以看出,本文方案在 SER 为 $10^{-5}$ 时的 SNR 性能优于 RC 方案约 9 dB; 在 SER 为 $10^{-2}$ 时,本文方案的 SNR 性能优于 SMP 方案约 25 dB。

由上述分析可知, 不论是在何种湍流条件下,本文方案相比于 RC、SMP 方案均能实现更低的 SER,从而提升通信质量。

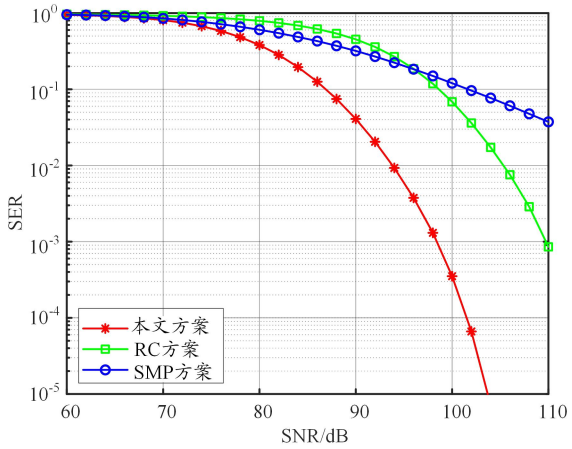


图 7 在水下中等湍流信道环境下,不同调制方案的性能比较

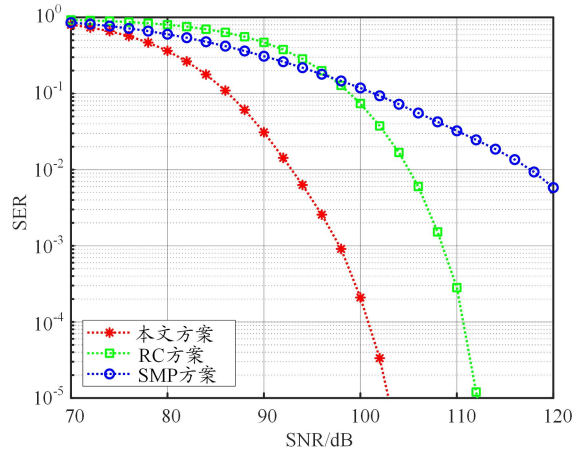


图 8 在水下强湍流信道环境下,不同调制方案的性能比较

## 3 结束语

针对水下可见光 MIMO 通信系统中天线配置自由度受限和物理层安全性薄弱 的双重挑战,本文提出了一种奇数阶 OT 辅助的 MIMO 收发机架构, 其核心基于混沌加密机制。该方案融合了奇数阶正交矩阵生成算法与 Logistic-Cat 双混沌系统驱动的高维数字加密算法,实现了对用户数据的双链路加密。仿真结果表明,相较于基准方案,本文提出的方案在可靠性和安全性方面表现出更优性能。

由于伴随着计算复杂度的增加,本研究后续将聚焦于开发低复杂度近似算法,以在可接受精度损失范围内提升计算效率。

**参考文献:**

[1] HUANG N, WANG X, CHEN M. Transceiver design for MIMO VLC systems with integer-forcing receivers[J]. IEEE Journal on Selected Areas in Communications, 2017, 36(1): 66–77.

[2] KAUSHAL H, KADDOUM G. Underwater optical wireless communication[J]. IEEE Access, 2016, 4: 1518–1547.40-43

[3] FATH T, HAAS H. Performance comparison of MIMO techniques for optical wireless communications in indoor environments[J]. IEEE Transactions on Communications, 2012, 61(2): 733–742.

[4] LI X, SUN L, HUANG J, et al. Channel polarization scheme for ocean turbulence channels in underwater visible light communication[J]. Journal of Marine Science and Engineering, 2023, 11(2): 341–341.

[5] 张林,王大帅,张鹏,等. 水下无线光通信抗湍流调制技术[J]. 光通信技术,2024,48(6):11–15.

[6] CAI K, JIANG M. SM/SPPM aided multiuser precoded visible light communication systems[J]. IEEE Photonics Journal, 2016, 8(2): 1–9.

[7] RAJALAKSHMI R, POTHIRAJ S, MAHDAL M, et al. Adaptive fuzzy logic deep-learning equalizer for mitigating linear and nonlinear distortions in underwater visible light communication systems[J]. Sensors, 2023, 23(12): 5418–5418.

[8] HUANG G, ZHANG L, JIANG Y, et al. A general orthogonal transform aided MIMO design for reliable maritime visible light communications[J]. Journal of Lightwave Technology, 2020, 38(23): 6549–6560.

[9] 邓绍江,肖迪,涂凤华. 基于 Logistic 映射混沌加密算法的设计与实现[J]. 重庆大学学报(自然科学版),2004(4):61–63.

[10] LUONG D A, THANG T C, PHAM A T. Effect of avalanche photodiode and thermal noises on the performance of binary phase-shift keying-subcarrier-intensity modulation/free-space optical systems over turbulence channels[J]. IET Communications, 2013, 7(8): 738–744.

[11] JAMALI M V, SALEHI J A, AKHOUNDI F. Performance studies of underwater wireless optical communication systems with spatial diversity: MIMO scheme[J]. IEEE Transactions on Communications, 2016, 65(3): 1176–1192.

[12] GABRIEL C, KHALIGHI M A, BOURENNANE S, et al. Channel modeling for underwater optical communication[C]//IEEE. Proceedings of 2011 IEEE GLOBE-COM Workshops(GC Wkshps). New York: IEEE, 2011: 833–837.

[13] ANDREWS L C, PHILLIPS R L, HOPEN C Y. Laser beam scintillation with applications[M]. Washington: SPIE press, 2001.

[14] MISHRA A, PATI P S, GIRI R K. Performance analysis of SIM based FSO using various modulation techniques with APD receiver over turbulent channel[C]//IEEE. Proceedings of 2017 International Conference on Wireless Communications, Signal Processing and Networking(WiSPNET). New York: IEEE, 2017: 2730–2734.

[15] NAVIDPOUR S M, UYSAL M, KAVEHRAD M. BER performance of free-space optical transmission with spatial diversity[J]. IEEE Transactions on Wireless Communications, 2007, 6(8): 2813–2819.

[16] FU Y, DU Y. Performance of heterodyne differential phase-shift-keying underwater wireless optical communication systems in gamma-gamma-distributed turbulence[J]. Applied Optics, 2018, 57(9): 2057–2063.

[17] LIU W, XU Z, YANG L. SIMO detection schemes for underwater optical wireless communication under turbulence[J]. Photonics Research, 2015, 3(3): 48–53.

[18] OUBEI H M, DURAN J R, JANJUA B, et al. 4.8 Gbit/s 16-QAM-OFDM transmission based on compact 450-nm laser for underwater wireless optical communication[J]. Optics Express, 2015, 23(18): 23302–23309.