引用本文：杨立锐，郭心悦. 基于物理层加密的 OFDM 可见光通信系统安全传输方案[J]. 光通信技术，2023，47(1)：17–24.

基于物理层加密的 OFDM 可见光通信系统安全传输方案

杨立锐，郭心悦 *

（上海理工大学 医用光学技术与仪器教育部重点实验室，上海 200093）

摘要：针对可见光通信(VLC)链路的数据传输安全性不高的问题。在正交频分复用(OFDM)VLC 系统中，提出一种比特级、符号级和相位联合加密的三级物理层加密方案。首先，引入 Logistic 映射的混沌序列加密方法降低加密数据的相关性，提高加密数据的安全性和系统的传输性能；然后，提出基于 S 替换表的星座映射，根据不同的 S 替换表生成对应的星座映射关系，使得原始二进制比特数据和加密后生成的数字调制信号之间始终保持格雷映射的特性，保证格雷增益。仿真结果表明：相比现有的方案，提出的物理层加密方案不仅具有更高的安全性，还降低了 OFDM VLC 系统发送数据的峰均功率比，缓解了发光二极管(LED)发射端产生的非线性失真，提升了系统的误码率性能。

关键词：可见光通信；光正交频分复用；物理层安全；比特级加密；星座替换

中图分类号：TN929.1　**文献标志码**：A　**文章编号**：1002-5561(2023)01-0017-08

DOI：10.13921/j.cnki.issn1002–5561.2023.01.004　开放科学(资源服务)标识码(OSID)：

Secure transmission scheme of OFDM visible light communication system based on physical layer encryption

YANG Lirui, GUO Xinyue*

(Key Laboratory of Optical Technology and Instrument for Medicine,
Ministry of Education, University of Shanghai for Science and Technology, Shanghai 200093, China)

Abstract: Aiming at the problem of low data transmission security of visible light communication (VLC) link, the data transmission security problem of VLC link is becoming more and more prominent. In orthogonal frequency division multiplexing (OFDM) VLC system, a three-level physical layer encryption scheme with specific level, symbol level and phase joint encryption is proposed. Firstly, the chaotic sequence encryption method of Logistic mapping is introduced to reduce the correlation of encrypted data, improve the security of encrypted data and the transmission performance of the system. Then, the constellation mapping based on S replacement table is proposed, and the corresponding constellation mapping relationship is generated according to different S replacement tables, so that the characteristics of gray mapping are always maintained between the original binary bit data and the digital modulation signal generated after encryption, and the gray gain is guaranteed. The simulation results show that compared with the existing schemes, the proposed physical layer encryption scheme not only has higher security, but also reduces the pek-per-power ratio of the data sent by the OFDM VLC system, alleviates the nonlinear distortion generated by the light-emitting diode(LED) transmitter, and improves the bit error rate performance of the system.

Key words: visible light communication, optical orthogonal frequency division multiplexing, physical layer security, bit-level encryption, constellation replacement

0 引言

过去数十年，随着信息社会的发展，智能移动设备、智能家居被广泛使用，无线数据流量呈指型增长，传统的射频无线通信技术受频谱资源限制，逐渐不能满足人们日益增长的通信需求。在此背景下，可见光通信(VLC)作为一种新兴的无线通信技术受到了广泛关注[1–2]。与传统的射频通信相比，VLC 带宽较大且不受管制，不存在电磁辐射和电磁干扰等问题，并且具

收稿时期：2022–10–01。

基金项目：国家重点研发计划项目(2018YFB1801503)资助。

作者简介：杨立锐(1998—)，男，安徽六安人，硕士研究生，现就读于上海理工大学光电信息与计算机工程学院信息与通信工程专业，主要研究方向为可见光通信中的物理层加密技术。

*** 通信作者**：郭心悦(1981—)，女，博士，副教授，主要研究方向为无线通信技术。

有前端成本低、安全可靠等优点。

VLC 系统中，数据传输速率主要受限于发光二极管(LED)的调制带宽。目前，大功率的 LED 尚不能完全兼顾带宽和发光效率，LED 的频率响应随着频率增大而急剧衰减。正交频分复用(OFDM)调制技术不仅能有效克服频率选择性衰落，而且具有很高的频谱利用率，因而被广泛应用于 VLC 系统[3]，但其缺点是 OFDM 调制的峰均功率比(PAPR)较高。根据 LED 的伏-安特性曲线可知，线性驱动峰值电压范围非常有限，过高的 PAPR 很容易造成 LED 发射端的非线性失真，从而导致整个系统误码率性能下降[4]。同时，与其它无线通信技术一样，VLC 链路也面临着数据传输的安全问题。文献[5-6]提出的物理层加密技术是一种借助密钥在物理层实施加密的方法。与传统的加密方式相比，物理层加密技术可以与编码技术相结合，能同时提高物理层数据的传输性能和数据安全性；此外，物理层加密技术具有技术易实现、维护方便等优点，还可以与其它的无线通信技术相结合，如多天线技术、多载波通信技术等。目前，研究人员已经在 OFDM VLC 系统中提出一些物理层加密方案。文献[7]提出了一种带预均衡的信道确定子载波移动方案，该方案属于无密钥加密技术，即借助信道信息通过物理层的信号处理来提高系统的安全性。然而，这类加密方案需要在通信过程中估计窃听通道或物理定位窃听者，复杂度高、实现较困难。文献[8-9]提出了基于密钥的加密技术，利用循环前缀(CP)样本的极性从双极性实值 OFDM 样本创建动态密钥，通过在会话持续时间内与原始信号相乘来加密，增强了 OFDM VLC 的保密性。尽管系统支持对窃听者的高计算安全性，但容易受到已知明文攻击和选择明文攻击的影响。文献[10]提出了一种基于混沌序列的二级混合加密方法来提高传输图像数据的安全性和系统的传输性能，但增加了计算复杂度，且无法保证在各种攻击时的系统保密性。AL-MOLIKI Y M 等人[11]提出了基于轻量级信道独立 OFDM VLC 的加密方法，通过哈希函数和 CP 样本创建动态密钥进行不同类型的加密，可确保在面对各种攻击时的保密性，还能降低系统的 PAPR，但经过加密后，原始的二进制比特流数据和正交幅度调制(QAM)信号之间不满足格雷映射的关系，故系统的误码率(BER)性能会有所降低。

基于此，本文在 OFDM VLC 系统中提出一种比特级、符号级和相位联合加密的三级物理层加密方案。

1 系统原理

1.1 系统模型

基于物理层加密的 OFDM VLC 系统模型如图 1 所示。其中，ID_A 为发送者的身份，ID_B 为接收者的身份，他们之间的会话密钥为 SK。以 ID_A、ID_B、SK 作为哈希函数(SHA-512)的输入，产生混沌序列的初始值，再利用每帧变化的 CP 与哈希函数异或创建 3 个动态子密钥（K_i^1、K_i^2、K_i^3）来实现不同的加密方案。对 i 个 OFDM 符号生成的密钥 K_i^1 用于产生 S 替换表，实现对输入的下一帧原始像素点数据的替换；K_i^2 用于频域 OFDM 符号的相位加密；K_i^3 用于生成用于置换时域 OFDM 数据位置的 P 排列表。

在发送端，首先将输入的数据与混沌序列进行比特异或实现比特级的加扰，加扰后的数据通过 K_i^1 生成的 S 替换表进行符号级的替换，再根据 S 替换表生成的新的映射关系对替换后的符号进行 QAM，得到频域信号；在生成频域信号之前，插入导频序列用于接收端的信道估计。然后，通过 K_i^2 生成的流密码对频域信号进行相位加密、厄米特对称和快速傅里叶逆变换(IFFT)，生成实值的 OFDM 信号并添加 CP[4]。最后，通过密钥 K_i^3 产生的 P 排列表对发送信号时域排列，生成的时域信号经过数/模(D/A)转换后加载到 LED 两端，通过可见光进行发送。

在接收端，光电二极管(PD)将接收到的光功率转变为电信号，经过模/数(A/D)转换后变为数字信号。接收端的信号处理是发送端的逆过程，包括解密和解调两部分。其中，需先对密钥进行解密，然后用解密后的密钥恢复原始数据，最后利用发送端插入的导频序列进行频域上的信道估计，消除信道对信号产生的影响[12]。

1.2 加密原理

1.2.1 基于 Logistic 映射的比特级置乱

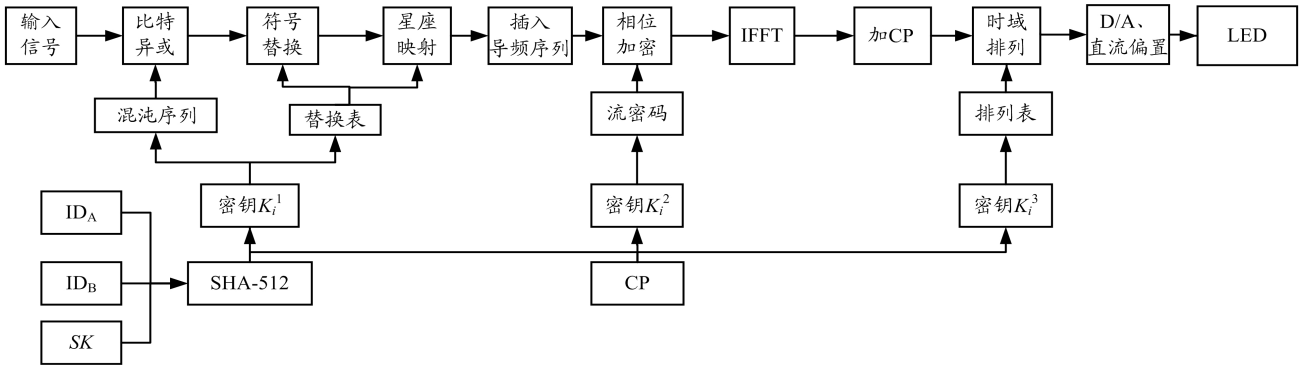
本文采用 Logistic 映射的混沌序列加密方法，将 Logistic 映射的混沌序列对输入的原始数据进行比特级别的置乱，使得信源数据均匀随机，既能提升数据安全性，还能改善系统的传输性能和提高系统的可靠性。比特级置乱过程如下：

首先，原始数据被转换为比特流，再被基于 Logistic 映射的混沌序列加扰。Logistic 映射定义为

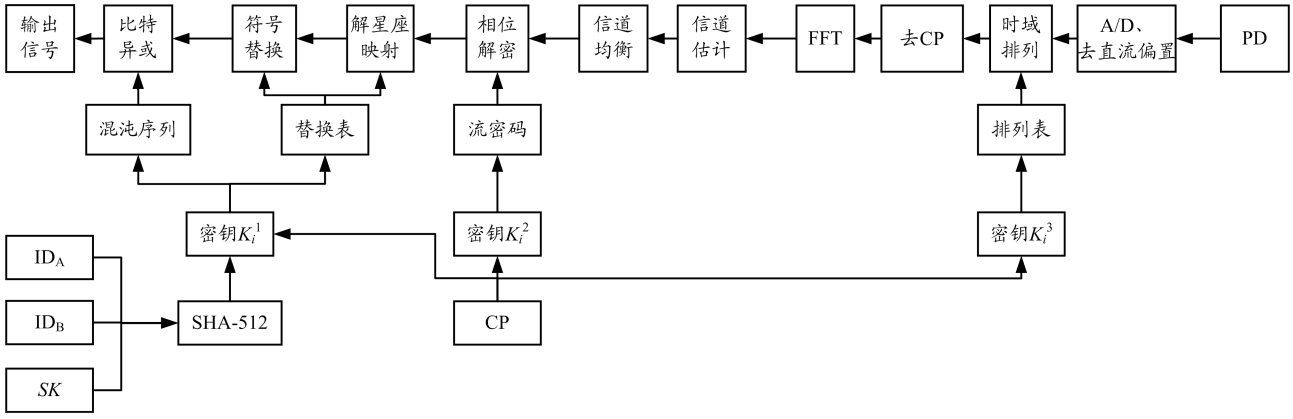
$$X_{i+1}=\alpha X_i(1-X_i) \tag{1}$$

其中，$X_i \subset (0,1)$；α 为控制参数，当 $3.569945627<\alpha\leqslant 4$，序列处于混沌状态。根据式(1)得到混沌加扰序列。

其次，通过逻辑混沌映射均匀化处理方案对逻辑



（a）发射端



（b）接收端

图 1　基于物理层加密的 OFDM VLC 系统框图

序列进行优化[13-14]，得到新的序列 Y_i 为

$$Y_i=(1/\pi)\cdot\sin^{-1}(X_i^2) \tag{2}$$

然后，为了生成混沌整数序列，进行如下操作：

$$X_i=\mathrm{mod}(\mathrm{F}(Y_i)\cdot 10^{15},M) \tag{3}$$

其中，F(·)运算符表示向下取整，mod(·)表示取余数，M 表示 QAM 阶数。

最后，利用得到的混沌加扰序列与原始传输数据 G 进行异或，得到逻辑加密后的数据 E_{data} 为

$$E_{\mathrm{data}}=X\oplus G \tag{4}$$

其中，$X=[X_1,X_2,\ldots,X_i]$。

1.2.2 基于 S 替换表的星座映射

本文提出基于 S 替换表生成 QAM 信号星座映射关系。根据加密方案，每个 OFDM 符号对应一个不同的 S 替换表，因此需要根据每一个 S 替换表的替换关系生成不同的星座映射关系，使得原始二进制比特数据和加密后生成的数字调制信号之间能始终保持格雷映射的特性，这样就能避免因加密导致的格雷增益损失。

采用产生的动态密钥 K_i^1 和密钥调度算法（KSA）随机生成 S 替换表后的符号 T_{j+1} 可以表示为

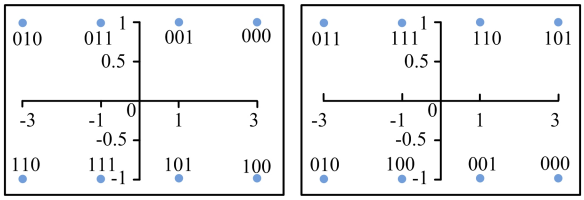
$$T_{j+1}=S_i X_{j+1} \tag{5}$$

其中，X_{j+1} 是经过 Logistic 映射置乱后的第 j+1 个数据，S_i 表示对第 i 个 OFDM 符号生成的 S 替换表。

以 8QAM 为例的一种可能的 S 替换表如表 1 所示。根据表 1 的替换关系提出的星座映射关系与文献[11]的星座映射关系（8QAM 星座映射图）对比情况如图 2 所示。可以看出，文献[11]方案在 QAM 前后是满足格雷映射的，即相邻星座点之间相差一个比特，但由于进行了替换操作，这种映射使得替换以后的数据跟映射后的数据不能保持格雷特性。同时，由于原始的二进制数据源需要先加密后再进行

表 1　一种可能的 S 替换表

输入数据 X_{j+1}	替换数据 T_{j+1}
000	101
001	110
010	011
011	111
100	000
101	001
110	010
111	100



（a）文献[11]方案　　（b）本文方案

图 2　不同方案的星座映射关系

QAM，因此该星座映射关系只能保证加密后的二进制比特数据与 QAM 信号满足格雷映射的关系，无法获得格雷增益。本文根据 S 替换表提出的星座映射关系中，虽然从图 2 反映的二进制比特和 QAM 信号的映射关系不满足格雷映射的特性，但是该星座图得到的 QAM 信号与 S 替换之前的二进制数据满足格雷映射的关系，因此系统可以获得格雷增益，避免了因加密导致的格雷增益损失，保证了传输的可靠性不受影响。

1.2.3 相位级加密

经过上述处理后，再进行相位加密和时域排列。利用 K_{i-1}^{2} 生成 a_{i-1}、b_{i-1}、c_{i-1} 这 3 种不同的伪随机序列，首先，当 c_{i-1} 的值为−1 时，交换 T_i 的实部和虚部后，分别乘以 a_{i-1} 和 b_{i-1}；当 c_{i-1} 的值为 1 时，对 T_i 不做任何处理。通过相位加密可以将同相频域 OFDM 异相，提高系统的 PAPR 性能。相位加密前后数据的关系如下：

$$Z_i=\begin{cases}T_i, c_{i-1}=1\\ \mathrm{Re}(T_i)\cdot a_{i-1}+\mathrm{j}\cdot\mathrm{Im}(T_i)\cdot b_{i-1}, c_{i-1}=-1\end{cases} \tag{6}$$

其中，T_i 是经过 QAM 以后的频域信号。为了生成实值 OFDM 信号，对相位加密后的信号 Z_i 进行厄米对称处理得到 $\overline{Z}_i$，并对 $\overline{Z}_i$ 进行厄米对称和 IFFT。IFFT 运算后，还需在 OFDM 信号前添加 CP，用于防止符号间干扰并且生成下一帧使用的动态密钥。

然后，在时域上重新排列序列得到发送信号 $\overline{r}_i$。时域排列是一种动态置换方法，在第 i 帧处利用 K_i^3 创建置换表，通过动态密钥更新每个输入帧的排列表。

最后，经过 D/A、叠加直流（DC）偏置后加载到 LED 两端，将可见光信号发送出去。在接收端得到的接收信号为

$$y_i(t)=h(t)\otimes\overline{r}_i(t)+n(t) \tag{7}$$

其中，$n(t)$ 为时域噪声向量，$h(t)$ 为可见光链路的信道增益。

1.3 解密过程

在接收端，进行与发射端相反的操作即可解密。发射端与接收端通过 Diffie-Hellman（D-H）密钥交换来实现秘密信息（$\mathrm{ID_A}$、$\mathrm{ID_B}$、SK）的共享。D-H 加密协议允许事先不了解的双方通过通信信道共同建立共享密钥，实现秘密信息的交换。对交换后的信息应用 SHA-512 与 CP 进行异或操作后即可得到每帧用来解密的密钥。将解密的密钥依据发送端的划分顺序，分为 K_i^1、K_i^2、K_i^3，用于后续通信：借助动态密钥 K_{i-1}^3 生成的排列表进行反向位置排列，在生成下一帧解密所需的密钥后，移除 CP，进行 OFDM 解调和频域均衡，并对 m_i 进行快速傅里叶变换（FFT），得到

$$V_i=Z_i+N_i \tag{8}$$

其中，m_i 表示在进行 FFT 之前的时域信号（去除 CP 后的信号），N_i 表示频域噪声。

再用 a_{i-1}、b_{i-1}、c_{i-1} 对信号 V_i 进行解密。根据式（6）、式（8）解密后的信号 $\overline{V}_i$ 为

$$\begin{aligned}\overline{V}_i&=\mathrm{Re}(V_i)\cdot a_{i-1}+\mathrm{j}\cdot\mathrm{Im}(V_i)\cdot b_{i-1}\\&=T_i+\mathrm{Re}(N_i)\cdot a_{i-1}+\mathrm{j}\cdot\mathrm{Im}(N_i)\cdot b_{i-1}\end{aligned} \tag{9}$$

利用 S 替换表的星座映射关系对 $\overline{V}_i$ 进行 QAM 解调，再进行反替换，得到

$$U_i=S_{i-1}^{-1}(E_i) \tag{10}$$

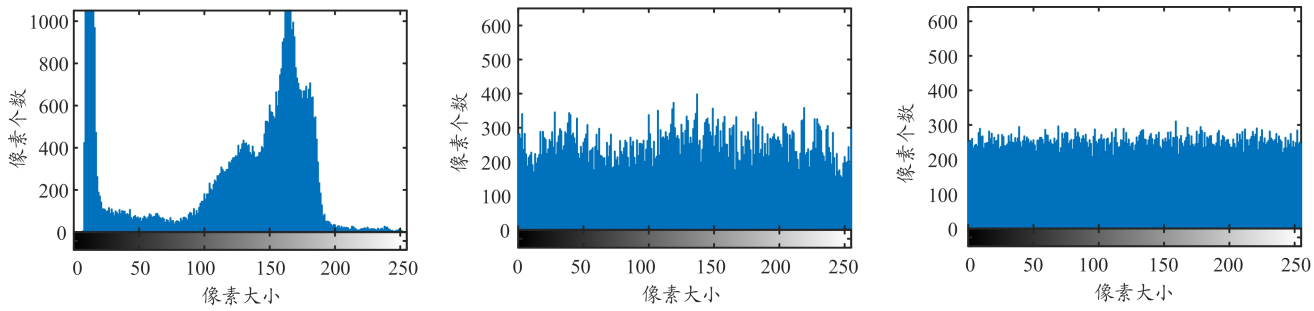
其中，E_i、U_i 分别为经过 QAM 解调后、替换后的数据，S_{i-1}^{-1} 表示第 i−1 帧的 S 反替换表。

将输出序列与混沌逻辑序列进行异或，最后恢复出原始比特数据流。

2 仿真结果与分析

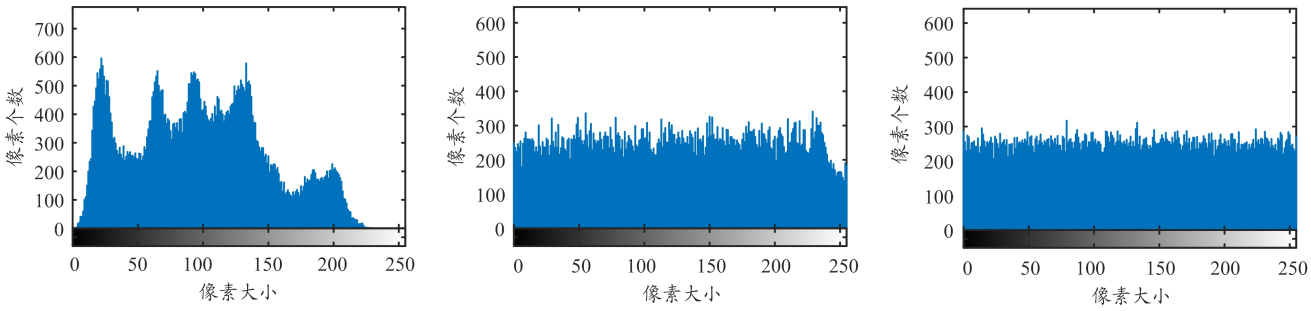
本文对基于物理层加密的 OFDM VLC 系统性能进行了仿真与评估，并与未进行加密和基于文献[11]方案加密的 OFDM VLC 系统的性能进行了对比。仿真实验的主要参数设置如下：OFDM 载波数为 512，CP 长度为 64，光电探测器的有效区域为 1 $\mathrm{cm^2}$，发送功率为 1 W，半功率角为 70°，接收端视场角（FOV）为 85°，数字调制方式为 16QAM 或者 256QAM。仿真中，根据文献[15]建立 VLC 信道模型，并分别选择随机数据源和尺寸为 256×256 像素的标准 Lena 图像、Cameraman 图像作为输入数据来评估系统的性能。

图 3 和图 4 为原始输入数据（Lena 图像和 Cameraman 图像）在 256QAM 下，经不同加密方案加密后的数据直方图。可以看出，相比文献[11]方案，本文方案的加密数据对应的直方图更接近均匀分布。这是因



(a) 原始图像直方图　(b) 文献[11]方案　(c) 本文方案

图 3 输入源为 Lena 图像时不同方案的直方图



(a) 原始图像直方图　(b) 文献[11]方案　(c) 本文方案

图 4 输入源为 Cameraman图像时不同方案的直方图

为该方案对输入图像数据进行了基于 Logistic 映射的比特级置乱,其数据的随机化程度更高,可以更有效地对抗统计攻击;同时,随机化的数据源对于系统传输性能也有很大的影响。

以 Cameraman 图像作为输入源, 在 256QAM 下,本文方案加密后子载波之间的相关性如图 5 所示。可以看出,各子载波间的相关性不显著,相关峰仅出现在相同的子载波符号间。因此,攻击者很难发现连续加密的 OFDM 符号之间的任何关系[16]。表 2 和表 3 分别为不同加密方案下输入数据为 Lena 图像和 Cameraman 图像相邻像素之间的相关系数情况。可以看出,本文方案能显著降低图像数据的相关性,优于文献[11]方案。因此,本文提出的加密方案安全性更高。

PAPR 是衡量发送信号易受 LED 发射非线性失真程度的重要指标,PAPR 越高、发送信号的非线性失真就会越严重。发送信号 PAPR 值的统计结果可以用互补累积分布函数(CCDF)表示,CCDF 曲线上的每一点表示大于该 PAPR 值的概率。在调制格式为 256QAM,输入数据为 Cameraman 图像和 Lena 图像时,3 种方案的发送信号对应 PAPR 值的 CCDF 曲线如图 6 所示。可以看出,与未加密方案相比,本文方案有效降低了系统的 PAPR。这是因为经过物理层加密技术后,根据直

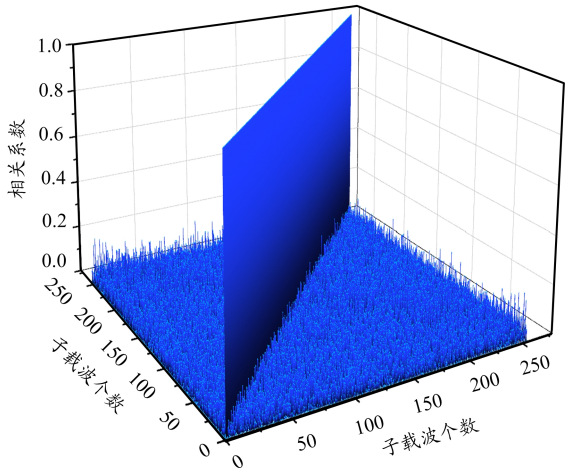


图 5 本文方案中加密后子载波间的相关性

表 2 Lena 图像相邻像素的相关系数

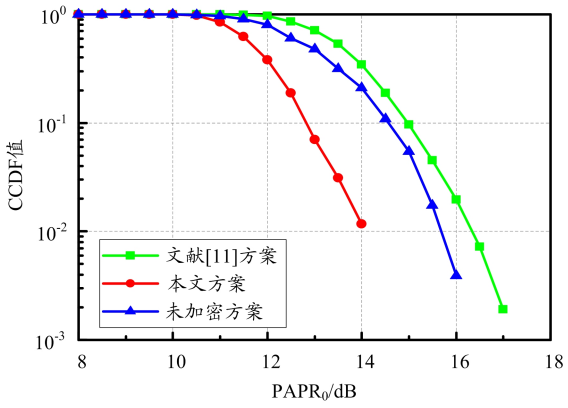
方案	水平相关系数	竖直相关系数	对角相关系数
原始图像	0.9602	0.9876	0.9276
文献[11]方案	0.0800	0.0090	0.0019
本文方案	0.0146	0.0020	0.0040

表 3 Cameraman 图像相邻像素的相关系数

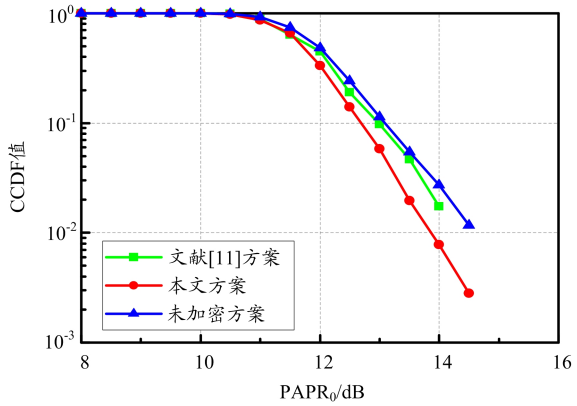
方案	水平相关系数	竖直相关系数	对角相关系数
原始图像	0.9703	0.8771	0.9130
文献[11]方案	0.0427	0.0097	1.9266e−4
本文方案	0.0059	5.2451e−4	−8.3233e−4

方图和相关性结果可知，前后数据间的相关性大大降低，使得OFDM 各子载波上的频域信号同相或接近同相的概率减小，进而降低 OFDM 信号的 PAPR。与文献[11]方案相比，本文方案由于引入基于 Logistic 映射的比特级置乱，因此发送数据的相关性和 PAPR 进一步降低。

本文使用随机数据源和图像数据源评估物理层加密技术对系统 BER 性能的影响。本文评估系统BER 性能时，不考虑发送端产生的非线性失真的影响，即假设 LED 工作在线性工作区域。输入为随机数据源时，在 2 种不同调制方式下（16QAM 和 256QAM）的 3 种



（a）Cameraman 图像

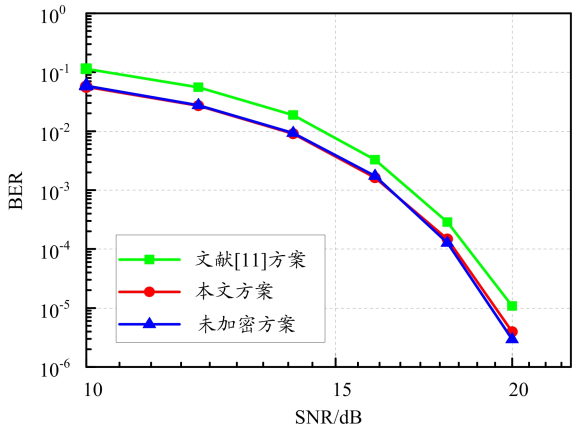


（b）Lena 图像

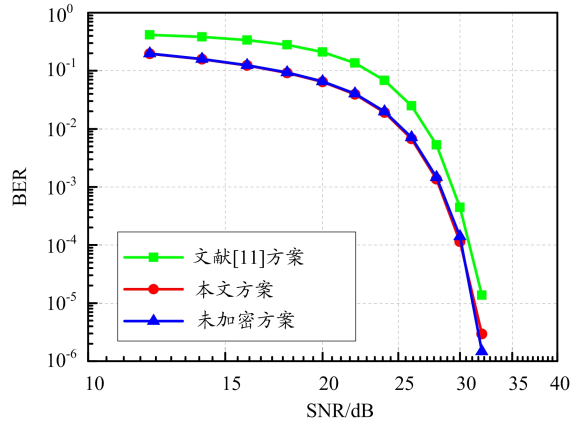
图 6 不同方案 PAPR 的 CCDF 曲线

OFDM VLC 系统的 BER 性能结果如图 7 所示（以未加密 OFDM VLC 系统的 BER 性能作为比较基准）。可以看出，本文方案的OFDM VLC 系统的 BER 曲线与未加密系统的曲线几乎重合，说明对于输入为随机数据源的情况，本文提出的物理层加密算法不会影响系统的 BER 性能。然而，文献[11]方案系统的 BER 明显升高，说明文献[11]所提出的物理层加密算法对系统 BER 性能产生了影响。这是因为该方案中原始的二进制比特流数据和经过加密、调制后产生的 QAM 信号之间不满足格雷映射关系，不能获得格雷增益，故而 BER 性能下降，尤其是在低信噪比条件下，BER 性能下降更为明显。

输入数据为 Cameraman 图像和 Lena 图像时，2 种不同调制方式下（16QAM 和 256QAM）3 种方案系统的 BER 性能如图 8 所示。可以看出，当输入为图像源时，本文提出的物理层加密算法的误码率性能优于未加密

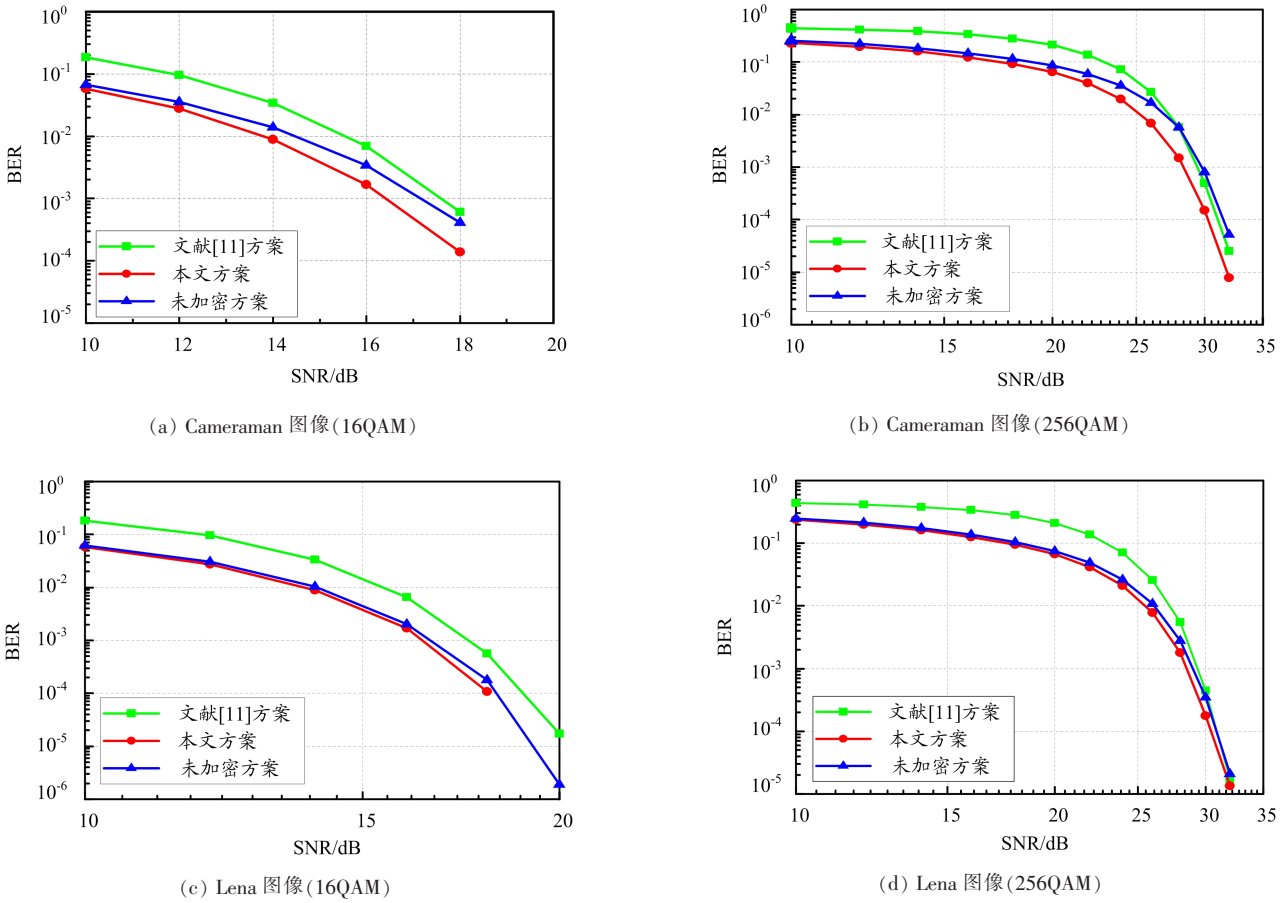


（a）16QAM



（b）256QAM

图 7 输入为随机数据源时，
不同加密方案 OFDM VLC 系统 BER 性能对比



(a) Cameraman 图像(16QAM)　(b) Cameraman 图像(256QAM)

(c) Lena 图像(16QAM)　(d) Lena 图像(256QAM)

图 8　输入为图像时,不同加密方案 OFDM VLC 系统 BER 性能对比

方案和文献[11]方案,这因为该方案使用了逻辑加密和星座替换;且对于相关性较高的图像信源而言,物理层加密技术所采用的比特级加密、符号替换、相位加扰等加密操作能减小传输数据的相关性,使得信源分布更为随机,因此具有更好的 BER 性能。文献[11]方案虽然也具有上述优点,但是其损失了格雷增益,BER 性能受到了很大影响。而本文方案通过引入基于星座替换的符号加扰,满足了原始的二进制比特流数据和加密后调制产生的 QAM 信号之间的格雷映射关系,从而保证了格雷增益。

最后,为了更直观地显示本文提出物理层加密方案的 BER 性能,以 Cameraman 图像为输入源,文献[11]方案和本文方案在不同信噪比下恢复的图像对比情况如图 9 所示。显然,在相同信噪比的情况下,相比文献[11]方案,本文方案的 OFDM VLC 系统恢复的图像噪点少,图像质量更好。

(a) *SNR*=8 dB,文献[11]方案　(b) *SNR*=14 dB ,文献[11]方案　(c) *SNR*=20 dB,,文献[11]方案

(d) *SNR*=8 dB，本文方案　(e) *SNR*=14 dB，本文方案　(f) *SNR*=20 dB，本文方案

图 9　不同方案的加密图像对比

3 结束语

本文针对 OFDM VLC 系统提出了一种比特级、符号级和相位联合加密的三级物理层加密方案。该方案主要有 2 个创新点：第一，引入 Logistic 映射的混沌序列加密，扩大安全密钥空间，降低发送数据的相关性，进一步增强了传输数据的安全性；同时，还能进一步降低发送信号的 PAPR，降低发射端 LED 产生非线性失真的风险，提高了系统的 BER 性能。第二，提出基于 S 替换表的星座映射，根据不同的 S 替换表，生成对应的星座映射关系，使得原始二进制比特数据和加密后生成的数字调制信号之间始终保持格雷映射的特性，保证了格雷增益，弥补了文献[11]中物理层加密导致系统 BER 性能下降的缺点。

以 Cameraman 图像和 Lena 图像数据源为例，评估了本文方案在数据传输可靠性和安全性两方面的性能。通过直方图和相关性可知，与传统方案相比，经过本文物理层加密后，数据相关性减小，加密后数据的随机化程度更高，故安全性更高。仿真结果表明：本文方案的 OFDM VLC 系统发送信号的 PAPR 值比传统方案的 OFDM VLC 系统明显减小，说明本文方案能更大程度降低 LED 非线性失真带来的性能损失。在不考虑系统非线性的情况下，本文提出的加密方案的 OFDM VLC 系统 BER 最低，因此传输可靠性更高。

参考文献：

[1] MATHEUS L, VIEIRA A, VIEIRA L F M, et al. Visible light communication: concepts, applications and challenges [J]. IEEE Communications Surveys and Tutorials, 2019, 21(4): 3204–3237.

[2] CHI N, ZHOU Y, WEI Y, et al. Visible light communication in 6G: advances, challenges, and prospects [J]. IEEE Vehicular Technology Magazine, 2020, 15(4): 93–102.

[3] 贾科军，魏少博，蔺莹，等. 可见光通信预编码光正交频分复用系统的研究[J]. 光学学报，2021，41(17)：57–64.

[4] GUO X, CHI N. Superposed 32QAM constellation design for 2×2 spatial multiplexing MIMO VLC systems [J]. Journal of Lightwave Technology, 2020, 38(7): 1702–1711.

[5] MUKHERJEE A. Secret-key agreement for security in multi-emitter visible light communication systems [J]. IEEE Communications Letters, 2016, 20(7): 1361–1364.

[6] GAO M, LI C, XU Z. Performance enhancement of LED-based indoor OFDM-VLC system using digital chaotic scheme [J]. Optics Communications, 2019, 439: 21–26.

[7] LU H, ZHANG L, CHEN W, et al. Design and analysis of physical layer security based on ill-posed theory for optical OFDM-based VLC system over real-valued visible light channel [J]. IEEE Photonics Journal, 2016, 8(6): 1–19.

[8] AL-MOLIKI Y M, ALRESHEEDI M T, AL-HARTHI Y. Robust key generation from optical OFDM signal in indoor VLC networks [J]. IEEE Photonics Technology Letters, 2016, 28(22): 2629–2632.

[9] AL-MOLIKI Y M, ALRESHEEDI M T, AL-HARTHI Y. Secret key generation protocol for optical OFDM systems in indoor VLC networks [J]. IEEE Photonics Journal, 2017, 9(2): 1–15.

[10] WANG Z, LV J. Secure image transmission in orthogonal frequency division multiplexing visible light communication systems[J]. IEEE Access, 2019, 7: 107927–107936.

[11] AL-MOLIKI Y M, ALRESHEEDI M T, AL-HARTHI Y, et al. Robust light weight-channel-independent OFDM-based encryption method for VLC-IoT networks[J]. IEEE Internet of Things Journal, 2022, 9(6): 4661–4676.

[12] BANDARA K, CHUNG Y H. Reduced training sequence using RLS adaptive algorithm with decision feedback equalizer in indoor visible light wireless communication channel [C]//IEEE. Proceedings of 2012 International Conference on ICT Convergence (ICTC), Jeju, South Korea. Jeju: IEEE, 2012, 149–154.

[13] GUAN Z, HUANG F, GUAN W. Chaos-based image encryption algorithm [J]. Physics Letters A, 2005, 346(1): 153–157.

[14] LIU L, WEI Z, XIANG H. A novel image encryption algorithm based on compound-coupled logistic chaotic map [J]. Multimedia Tools and Applications, 2022, 81(14): 19999–20019.

[15] SAENGUDOMLERT P. On the benefits of pre-equalization for a CO-OFDM and flip-OFDM indoor wireless optical transmissions over dispersive channels [J]. Journal of Lightwave Technology, 2014, 32(1): 70–80.

[16] HEYS H M. A tutorial on linear and differential cryptanalysis [J]. Cryptologia, 2002, 26: 189–221.