第 41 卷 第 16 期/2021 年 8 月/光学学报 研究论文

光学学报

基于混沌映射的 OFDM-PON 物理层加密及系统性能增强算法

周玉鑫[1]，毕美华[1,2*]，滕旭阳[1]，李齐良[1]，杨学林[2]

[1]杭州电子科技大学通信工程学院，浙江 杭州 310018；

[2]上海交通大学光纤区域网与新型光通信系统国家重点实验室，上海 200240

摘要 针对正交频分复用无源光网络(OFDM-PON)算法中数据安全性低和峰值平均功率比(PAPR)高的问题，提出了一种基于三维 Arnold 变换和混沌 Frank 序列的加密算法。该算法采用基于主成分分析的保守数字混沌系统产生的混沌序列进行加密，可解决混沌序列结构和计算精度导致的退化问题。首先，将 OFDM 信号转换为三维信号矩阵，利用三维 Arnold 变换进行置乱变换，实现对数据的加密；然后，将加密数据通过混沌序列随机选择的 Frank 序列，以降低 OFDM 信号的 PAPR。仿真实验结果表明，相比传统的 OFDM-PON 算法，本算法在互补累积分布函数的概率为 10^{-3} 时可将信号的 PAPR 约降低 2.1 dB，在误比特率为 3.8×10^{-3} 时可将接收光功率约降低 1 dB。

关键词 光通信；正交频分复用无源光网络；混沌加密；三维 Arnold 变换；主成分分析

中图分类号 TN918.4 **文献标志码** A **doi**：10.3788/AOS202141.1606002

Physical Layer Encryption and System Performance Enhancement Algorithm Based on Chaos Mapping in OFDM-PON

Zhou Yuxin[1], Bi Meihua[1,2*], Teng Xuyang[1], Li Qiliang[1], Yang Xuelin[2]

[1] *School of Communication Engineering, Hangzhou Dianzi University, Hangzhou, Zhejiang* 310018, *China*;

[2] *State Key Laboratory of Advanced Optical Communication System and Networks, Shanghai Jiao Tong University, Shanghai* 200240, *China*

Abstract In this paper, an encryption algorithm based on three-dimensional Arnold transform and chaotic Frank sequence is proposed, which is used to deal with low data security and excessive peak-to-average power ratio (PAPR) in orthogonal frequency division multiplexing passive optical network (OFDM-PON) systems. The algorithm uses the chaotic sequence generated by the conservative digital chaotic system based on the principal component analysis to encrypt, which can solve the degradation problem caused by the chaotic sequence structure and calculation accuracy. First, the OFDM signal is converted into a three-dimensional signal matrix, and the three-dimensional Arnold transform is used to perform scrambling transformation to realize the encryption of the data; then, the encrypted data is passed through the Frank sequence randomly selected by the chaotic sequence to reduce the PAPR of the OFDM signal. The simulation experiment results show that, compared with the traditional OFDM-PON algorithm, When the probability in the complementary cumulative distribution function is 10^{-3}, the algorithm can reduce the PAPR of the signal by about 2.1 dB, and when the bit error rate is 3.8×10^{-3}, the received optical power can be reduced by about 1 dB.

Key words optical communications; orthogonal frequency division multiplexing passive optical network; chaotic encryption; three-dimensional Arnold transform; principal component analysis

OCIS codes 060.4250; 060.4785; 060.4510

收稿日期：2021-01-19；**修回日期**：2021-03-04；**录用日期**：2021-03-18

基金项目：国家自然科学基金(61906055)、浙江省自然科学基金(LY20F050004，LQ19F020009)、浙江省教育厅一般科研项目(Y201942093，Y201942104，Y202044258)

通信作者：*bmhua@hdu.edu.cn

1 引 言

随着信息化社会的快速发展，各类信息传输量的增大对传统接入网提出了极大的挑战。正交频分复用无源光网络（OFDM-PON）技术具有频谱利用率高、抗光纤色散能力强以及动态资源分配等优势，成为下一代光接入网系统的研究热点[1]。由于无源光网络（PON）结构的广播特性，下行数据极易被非法用户窃取[2-3]。此外，正交频分复用（OFDM）信号的峰值平均功率比（PAPR）过高，导致其在 OFDM-PON 系统传输时会产生非线性失真，影响系统的传输性能[4-5]。

混沌序列具有的高度初值敏感性和伪随机性等特征，使其与保密通信存在着天然的联系[5]。为了有效联合处理 OFDM-PON 系统中 OFDM 信号的 PAPR 过高及 PON 系统的加密问题，人们提出了多种安全加密和降低 PAPR 的方案，包括混沌选择映射（CSLM）法[6]、混沌部分传输序列（CPTS）法[7]以及混沌预留子载波（CTR）法[8]等。但现有方案都是基于耗散型数字混沌序列[9-14]，而耗散型混沌系统自身的动力学特性会形成混沌吸引子[15]，使窃密者可以利用一段连续混沌序列以及基于神经网络的机器学习算法重构混沌系统的相空间[16]，在一定程度上降低了基于数字耗散混沌序列加密系统的保密性。保守混沌系统不存在耗散混沌的吸引子，涉及的相空间范围更大且随机性更强，且目前针对耗散混沌系统的预测手段对该系统均无效，因此，保守混沌系统的安全性更高[17]。在数字混沌序列的产生过程中，软件计算精度问题导致混沌系统中的复杂度与理想状态下的性能差异巨大，使混沌系统产生数字退化现象[18]。数字退化现象会导致混沌系统出现短周期、非遍历性，且混沌序列之间具有强相关性等缺点。针对该问题，人们提出多种解决方案，如扰动混沌状态、扰动混沌控制参数、级联多个混沌映射和随机切换多个混沌映射等方案[19-20]。但现有方案均比较复杂，不能直接用于对成本敏感的 OFDM-PON 的物理层加密系统。此外，通信系统通常用误比特率（BER）衡量数据传输的质量。用 BER 衡量系统性能时，采用基于模拟 OFDM 信号的 PON 系统中的判定标准，未考虑前向纠错码时，系统接收端的 BER 限制为 3.8×10^{-3}。即接收端的 BER 小于 3.8×10^{-3} 时，系统可以实现无差错传输[21]。若采用前向纠错码传输，可以实现数字光纤通信的系统 BER 限制为 10^{-9}。

针对上述问题，本文提出了一种基于改进保守数字混沌系统的 OFDM-PON 加密算法，并设计了一种新型改进保守混沌系统的数字混沌序列产生方案，以产生多组新型混沌序列。该混沌序列具有高随机性、高复杂度和强不可预测性，可增强系统的保密性。在此基础上，提出了一种主成分分析（PCA）法，对产生的混沌序列进行降维处理，在降低系统复杂度的同时解决了数字混沌序列的退化问题。基于选取的数字混沌序列，提出了一种结合三维（3D）Arnold 变换和 Frank 序列的矩阵生成方案，并将其用于 OFDM-PON 系统的加密和 OFDM 信号 PAPR 的降低。基于系统的参数配置搭建了仿真系统并进行了实验验证，结果表明，该加密方案通过 3D Arnold 变换和混沌 Frank 矩阵可生成约 10^{376} 的密钥空间，为数据的传输提供了良好的保密性；且相比传统的 OFDM-PON 算法，本算法在互补累积分布函数（CCDF）中的概率为 10^{-3} 时可将信号的 PAPR 约降低 2.1 dB，在 BER 为 3.8×10^{-3} 时可将接收光功率约降低 1 dB。

2 基于混沌序列的 OFDM-PON 加密及系统性能增强

基于保守数字混沌映射的 OFDM-PON 数据加密与 PAPR 降低原理如图 1 所示，其中，QAM 为正交振幅调制，PRBS 为伪随机比特流序列，P/S 为串并转换，OLT 为光线路终端，FFT 和 IFFT 为快速傅里叶变换和逆变换，CP 为循环前缀，ONU 为光网络单元。具体步骤如下。

1）改进型保守数字混沌序列的产生：利用保守混沌系统的初始值产生混沌序列，并在产生的混沌序列中加入扰动，将其拓展为若干组混沌序列，并进行 PCA 处理，选取出第一主成分的混沌序列。

2）基于保守数字混沌序列的 3D Arnold 变换的加密过程：利用混沌序列控制 3D Arnold 变换的参数，对 OFDM 符号矩阵进行加密。

3）利用改进的保守混沌序列控制抽取 Frank 序列值，并构造 Frank 矩阵，以实现 OFDM 信号 PAPR 的降低和系统的加密。

2.1 改进型保守数字混沌序列的设计

为了增强 OFDM-PON 系统的抗攻击能力，设计了一种新型数字保守混沌系统，该保守混沌系统可表示为

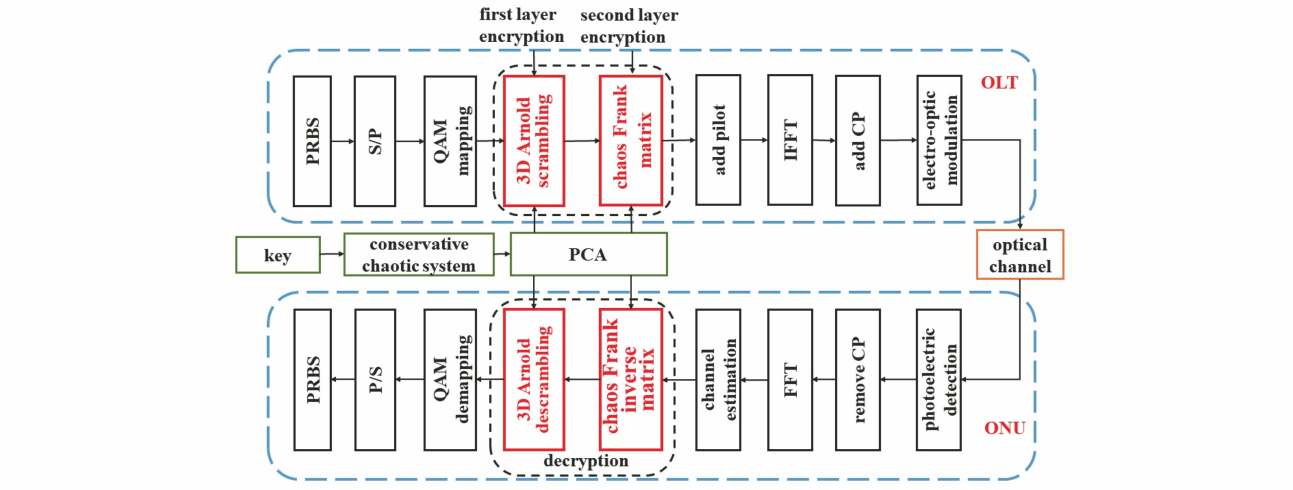

图 1　基于混沌序列的 OFDM-PON 加密及系统性能增强算法的原理

Fig. 1　Principle of OFDM-PON encryption and system performance enhancement algorithm based on chaotic sequence

$$\begin{cases} \mathrm{d}x = Ay + yz + xz \\ \mathrm{d}y = -Ax - xz \\ \mathrm{d}z = 2 - x^2 \end{cases}, \tag{1}$$

式中，$\mathrm{d}x$、$\mathrm{d}y$、$\mathrm{d}z$ 分别为对 x、y、z 的微分，$A \in [-5000, 5000]$为控制参数，实验中取 $A=10$；混沌系统的初始值$[x_1, y_1, z_1]$为$[1.01, 0.98, 1.1]$。目前，保守混沌系统的研究多为系统参数确定的系统，而该混沌系统为无平衡点的大范围保守混沌系统。保守混沌系统的李雅普诺夫指数 $L_1=0.0045$，$L_2=0$，$L_3=-0.0040$，包含正数的李雅普诺夫指数表明该系统处于混沌状态，且李雅普诺夫指数的和约为 0，因此，可以判断该系统为保守混沌系统。保守混沌系统的相图如图 2 所示，(1)式经过步长 $h=0.002$ 的四阶龙格-库塔迭代 10000 次，生成的三组混沌序列值分别为$\{x_n\}$、$\{y_n\}$、$\{z_n\}$。

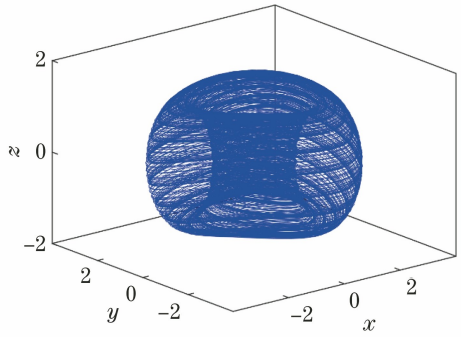

图 2　保守混沌系统的相图

Fig. 2　Phase diagram of the conservative chaotic system

受鸽洞原理和软件数字精度的影响，混沌系统迭代产生的状态数量可能会大于软件所能表示的数字状态数量，必然会产生相同的混沌迭代数值。在该状态下，经过初始状态迭代后，系统会进入一个周期循环(混沌数字退化)，导致混沌系统容易受到攻击。为了解决该问题，系统通过 PCA 进行数据降维。PCA 对高维度数据进行降维的同时能保留高维度数据的主要特征，去除数据噪声和降低数据相关性。但保守混沌序列经过 PCA 处理后会扰乱其周期性，大大降低混沌迭代进入周期循环的概率。PCA 过程可表示为

$$\begin{aligned} X_n &= X_{\mathrm{PCA}}[x_n, \cdots, x_{n+(d-1)\tau}] \\ Y_n &= X_{\mathrm{PCA}}[y_n, \cdots, y_{n+(d-1)\tau}] \\ Z_n &= X_{\mathrm{PCA}}[z_n, \cdots, z_{n+(d-1)\tau}] \end{aligned}, \tag{2}$$

式中，x_n、y_n、z_n 为(1)式生成的保守混沌序列，X_n、Y_n、Z_n 为经过 PCA 处理后的保守混沌序列，τ 为延迟时间，d 为混沌相空间的维数，$X_{\mathrm{PCA}}[x_n, \cdots, x_{n+(d-1)\tau}]$为对保守混沌序列进行 PCA 变换，$n$ 为保守混沌序列的索引。PCA 为一种线性变换，即用由混沌相空间中向量方差组成的一组新基重新描述混沌相空间，其中，方差最大的成分为第一主成分，可保持混沌序列的最大特征。选取第一主成分对系统进行加密，综合考虑计算量和复杂度的影响，实验取 $\tau=15$、$d=8$。PCA 处理后的混沌序列不利于直接加密，因此，需要对混沌序列进行整数化，可表示为

$$\begin{aligned} D_{x,n} &= \mathrm{mod}[X_{\mathrm{extract}}(X_n, m_1, m_2, m_3), M] \\ D_{y,n} &= \mathrm{mod}[X_{\mathrm{extract}}(Y_n, m_1, m_2, m_3), M] \\ D_{z,n} &= \mathrm{mod}[X_{\mathrm{extract}}(Z_n, m_1, m_2, m_3), M] \end{aligned}, \tag{3}$$

式中，$X_{\mathrm{extract}}(X_n, m_1, m_2, m_3)$函数可返回 X_n 小数部分的第 m_1、m_2、m_3 位数组合产生的整数，取值范围为 1～15。$\mathrm{mod}(P, M)$函数可返回 P 除于 M 的余数，M 为 QAM 的状态个数，实验取 $M=16$，最终返回的整数序列为$\{D_{x,n}, D_{y,n}, D_{z,n}\}$。

2.2 基于保守数字混沌序列的 3D Arnold 映射第一层加密方案

为了提高 OFDM-PON 系统的安全性，提出了一种基于保守数字混沌序列的 3D Arnold 映射加密方案，具体加密过程如下。

1) OFDM-PON 系统下行数据即 PRBS 依次进行 P/S 转换、QAM 映射和子载波分配，产生具有两个时频维度的 OFDM 信号。

2) 对于一个 OFDM 信号，首先，将每个子载波的 QAM 符号排列成一个平面；然后，将 N 个子载波按频率由低到高排列，将所有子载波组合成一个 3D 空间矩阵。将 OFDM 信号按 Z 轴(每层有一个子载波携带一个 OFDM 信号)排列，且每个子载波上具有 $H\times W$ 个 QAM 符号。图 3(a)和图 3(b)分别为任意 QAM 符号置乱前后位于 3D OFDM 信号的位置。可以发现，QAM 符号经过置乱后可能变换到任意一层的任意位置。

3) 用(3)式生成的保守混沌序列替代 3D Arnold 变换的控制变量对 3D OFDM 信号进行置乱处理。

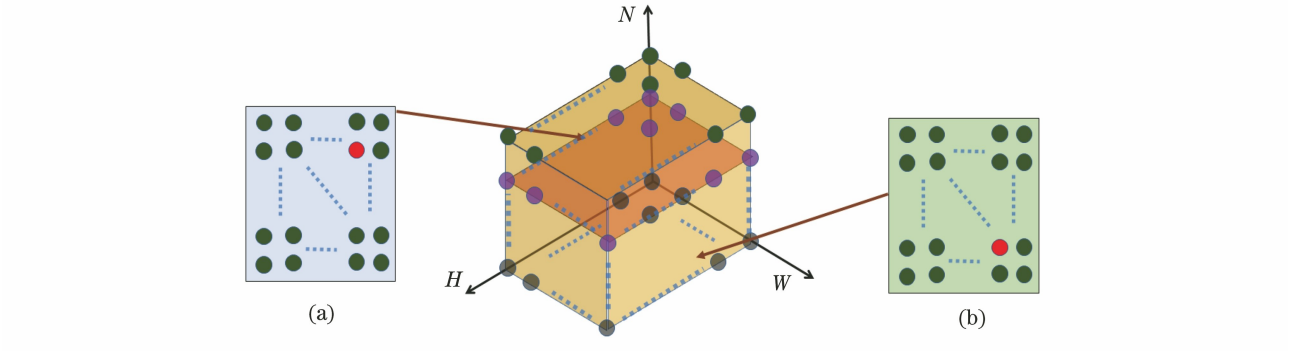

图 3　3D Arnold 变换的原理图。(a) QAM 符号变换前的位置；(b) QAM 符号变换后的位置

Fig. 3　Schematic diagram of 3D Arnold transformation. (a) Position before QAM symbol conversion; (b) position after QAM symbol conversion

Arnold 变换可将矩阵中各个位置的点重新排列，是一种保面积变换，即变换的模等于±1，且变换矩阵可逆[22]。根据该特性，构造了一种新型 3D Arnold 变换，可表示为

$$\begin{bmatrix} x' \\ y' \\ z' \end{bmatrix} = \mathrm{mod}\left\{ \begin{bmatrix} a & a+1 & a \\ 1 & 1 & b \\ a & c & d \end{bmatrix} \begin{bmatrix} x \\ y \\ z \end{bmatrix}, N \right\}, \quad (4)$$

式中，(x,y,z)为数据坐标的位置，(x',y',z')为经 3D Arnold 变换后的坐标索引，a、b、c、d 为 3D Arnold 变换的控制变量。用 mod 函数保证变换后的坐标仍然在 OFDM 信号矩阵中。为了保证 Arnold 变换矩阵的模等于 1，需保证 $d=ab(a+1)+ac-a^2-abc-1$。假定 $a=1$，$b=2$，$c=3$，则该系统的李雅普诺夫指数 $L_1=3.7430$，$L_2=-0.1011$，$L_3=-2.6419$。可以发现，三个指数中有一个指数大于零，这表明该系统具有混沌特性。为了解决 3D Arnold 变换周期性易被破解的问题，同时提高系统的加密性能，通过数字混沌序列控制变换矩阵中的参数$\{a,b,c\}$进行加密。

2.3 基于保守数字混沌序列的 Frank 序列的第二层加密及 PAPR 降低原理

为了降低 OFDM 信号的 PAPR 并进一步实现系统物理层的加密，提出了一种混沌 Frank 矩阵加密方案。Frank 序列是一种恒包络自相关序列(CAZAC)，具有良好的自相关性和弱互相关性。任意 Frank 序列组成的信号峰均比较低，长度为 L 的 Frank 序列可表示为

$$f(r\sqrt{L}+k+1)=\exp(\mathrm{j}2\pi k/\sqrt{L}), \quad (5)$$

式中，$r,k=\{1,\cdots,\sqrt{L}-1\}$，Frank 序列 $f=\{f_1,\cdots,f_L\}$。该序列的生成方式容易被外界获取，为了提高数据的安全性，用该序列生成矩阵时，利用混沌序列控制抽取的起点，可表示为

$$Q_{y,n}=\mathrm{mod}[X_{\mathrm{ceil}}(Y_n\times 10^8),L], \quad (6)$$

式中，X_{ceil} 为对输入元素进行向上取整的函数，$Q_{y,n}$ 为 Frank 序列抽取起点的索引值，其中，下标 y 为选取保守混沌序列 Y 进行操作。利用随机抽取的序列构造一个 $H\times W$ 的混沌 Frank 矩阵 $\boldsymbol{F}$，可表示为

$$\boldsymbol{F}=\begin{bmatrix} f_{Q_{y,n}} & f_{Q_{y,n}+1} & \cdots & f_{Q_{y,n}+W-1} \\ f_{Q_{y,n}+W} & f_{Q_{y,n}+W+1} & \cdots & f_{Q_{y,n}+2W-1} \\ \vdots & \vdots & & \vdots \\ f_{Q_{y,n}+(H-1)W} & f_{Q_{y,n}+(H-1)W+1} & \cdots & f_{Q_{y,n}+HW-1} \end{bmatrix}, \tag{7}$$

式中，矩阵元素的下标表示(5)式生成 Frank 序列的索引值。OFDM 符号由多个独立的调制子载波信号叠加而成，当各个子载波的相位相同或相近时，叠加信号会受到相同初始相位信号的调制，从而产生较大的瞬时功率峰值。由于 Frank 序列具有良好的自相关性和互相关特性，因此，用生成的矩阵乘以 OFDM 信号可以降低 OFDM 信号子载波之间的相关性，大大降低子副载波同相的概率，从而降低信号的 PAPR。由于矩阵 $\boldsymbol{F}$ 中各个向量之间具有正交性，使该矩阵存在逆矩阵，从而保证加密后的数据可以在接收端通过逆矩阵被正确解密。

3　仿真实验设置与结果分析

OFDM-PON 加密系统的传输仿真实验装置如图 4 所示，该系统在 Matlab 和 Optisystem 软件中进行联合仿真。发射端的 OLT 中，信号的加密在 Matlab 软件中进行离线数字信号处理(DSP)，即用 Matlab 软件生成一个长度为 1.31072×10^6 的 PRBS，并进行 16-QAM 调制，将其转换为 3.2768×10^5 个 QAM 符号。将这些 QAM 符号转换成 128×16×16 的 3D 矩阵，先进行 3D Arnold 置乱后再进行 OFDM 信号调制。其中，IFFT/FFT 的点数为 512，子载波数 $N=128$，采用厄米特(Hermitian)矩阵对称处理输出 IFFT 的实值信号。将 CP 的长度设置为 OFDM 符号长度的 1/8，将块状导频用于信道估计。在 Optisystem 软件中完成信号的传输，用生成的 OFDM 基带信号驱动马赫-曾德尔调制器(MZM)生成光 OFDM 信号，用波长为 1550 nm 的连续波激光器(CWL)作为光源产生光载波。输出的光 OFDM 信号经掺铒光纤放大器(EDFA)放大后注入长为 20 km 的标准单模光纤(SMF)进行传输。最后，光 OFDM 信号经过光电二极管检测恢复为电信号，并保存输出数据，以进行解调与解密。接收端用三个 ONU 分别模拟加密数据、原始数据和非法用户。数据的解调与解密过程同样由 Matlab 软件离线完成。为了更好地匹配实验结果，在仿真设置中所有光电器件的参数均与实验配置相同。

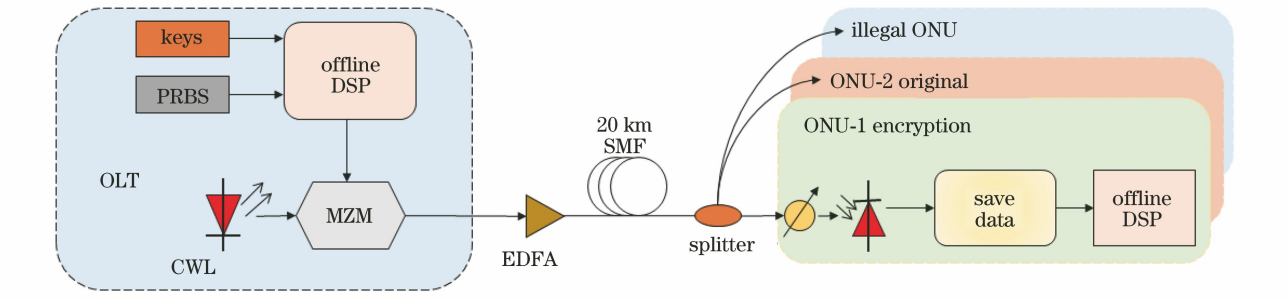

图 4　实验装置图

Fig. 4　Diagram of the experimental setup

为了验证 PCA 改进保守混沌系统生成的混沌序列的随机特性，采美国国家标准与技术研究院(NIST)推出的软件包对生成的保守混沌序列进行随机性测试。NIST 测试程序包含 15 种测试手段，可测试用于保密产生的任意长二进制序列的随机性。用改进型保守混沌序列产生 100 Mbits 的二进制数据，并将这些数据分成 1000 段进行测试。NIST 提供了两种评判序列随机性的依据，第一种是用 P-Value 测试序列的均匀分布特性，P-Value 为该序列比伪随机序列随机性好的概率。当 P-Value 大于 0.001 时，表明测试序列是分布均匀的，即通过测试；第二种评判依据是序列的通过率，当二进制序列被分为 1000 段，且序列的通过率大于 0.973 时，表明该序列的随机性较好。混沌序列的 NIST 随机性测试如表 1 所示，可以发现，PCA 改进的保守混沌序列具有良好的随机性，可作为密钥序列应用于信息加密。

表 1　基于 PCA 的保守混沌序列随机性测试

Table 1　Randomness test of conservative chaotic sequence based on PCA

Statistical test index	*P*-Value	Passing rate
Approximate entropy	0.534146	1.000
Block frequency	0.308048	0.989
Cumulative sums	0.534146	1.000
FFT	0.319084	0.992
Frequency	0.699313	1.000
Linear complexity	0.851383	1.000
Longest run	0.350485	0.992
Nonoverlapping template	0.657933	1.000
Overlapping template	0.779188	1.000
Random excursions	0.041987	0.992
Random excursions variant	0.690156	1.000
Rank	0.873987	1.000
Runs	0.123755	1.000
Serial	0.371647	0.993
Universal	0.480771	0.991

为了进一步验证生成混沌序列的随机性，计算了生成混沌序列的自相关函数图像，结果如图5所示。可以发现，基于 PCA 改进的保守混沌系统的自相关函数更接近白噪声。

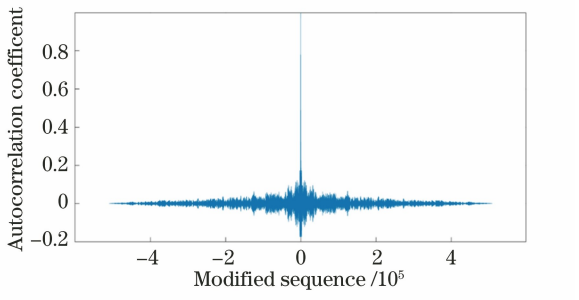

图 5　改进混沌序列的自相关系数

Fig. 5　Autocorrelation coefficient of the improved chaotic sequence

为了验证本算法对信号 PAPR 的抑制性能，用 CCDF 验证算法对 PAPR 的改善性能。图 6 为原始数据、原始 Frank 矩阵和加密 Frank 矩阵条件下信号的 PAPR 曲线，可以发现，相比原始数据，加密 Frank 矩阵与原始 Frank 矩阵具有相同的 PAPR 降低效果，且在 CCDF 为 10^{-3} 处都能使信号的 PAPR 约降低 2.1 dB，这验证了将加密 Frank 矩阵用于降低 PAPR 的可行性。同时，本方案能提升 OFDM-PON 系统的安全性能和传输性能。

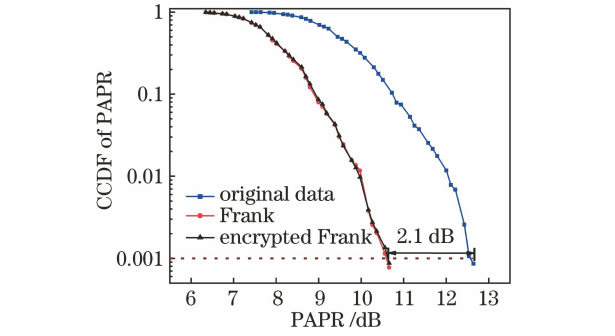

图 6　不同 OFDM 信号的 PAPR 曲线

Fig. 6　PAPR curves of different OFDM signals

为了直观展示本加密方案的效果，通过灰度图像验证系统的加密性能[23-24]，验证图像采用 USC-SIPI 图像库中尺寸为 512 pixel×512 pixel 的 8 bit 灰度图像 Barbara，结果如图 7 所示。可以发现，合法用户可以无失真地恢复图像，非法用户则无法正确恢复原始图像，且恢复的图像完全失真，这表明本加密方案具有较好的置乱效果。

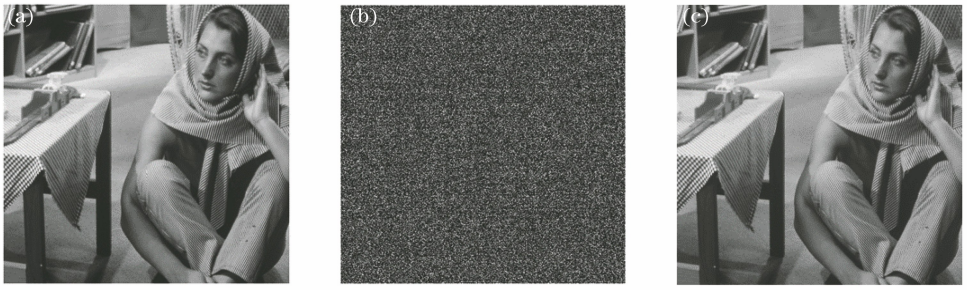

图 7　加密方案的仿真结果。(a)原始图像；(b)错误密钥解密的图像；(c)正确密钥解密的图像

Fig. 7　Simulation results of the encryption scheme. (a) Original image; (b) image is decrypted with wrong keys; (c) image is decrypted with correct keys

图 8 为无加密情况下 OFDM 信号的 BER 曲线，其中，仿真了合法和非法 ONU 在有无加密下 20 km 单模光纤和背靠背(BtB)下 ONU 的 BER 随接收光功率的变化曲线及接收光功率在 −23 dBm 时信号的星座图。可以发现，本方案无误码接收要求的 BER 限制为 3.8×10^{-3}，采用前向纠错编码后，BER 限制可以达到 10^{-9}[25]。相比未处理的情况，在 BER 为 3.8×10^{-3} 时，系统的接收光功率降低了约 1 dB，原因是 Frank 矩阵可降低 OFDM 信号的 PAPR，进一步降低了非线性失真对系统性能

的影响。而非法 ONU 接收端的误码率均在 0.5 左右，且几乎所有的星座符号都是错误的。这表明基于 3D Arnold 和混沌 Frank 矩阵的加密方案可以在保证数据安全传输的前提下，优化 OFDM 信号的传输性能。

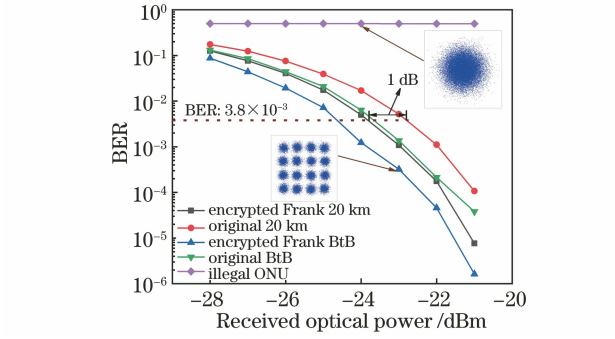

图 8 有无加密情况下 OFDM 信号的 BER 曲线

Fig. 8 BER curve of OFDM signal with or without encryption

密钥空间的大小决定着该加密系统是否能够抵抗暴力攻击，因此，可通过总密钥空间评估加密系统的安全性。针对混沌系统的初值敏感性，三个混沌初值可提供大小约为 10^{45} 的密钥空间。由于 3D Arnold 变换控制变量参数的随机性，需对全部数据点进行置乱，可产生大小约为 10^{242}（16！×16！×128！）的密钥空间。此外，混沌 Frank 矩阵的行列数为 64×64（64 为子载波数），经过列置换可以生成大小约为 10^{89} 的密钥空间。综上所述，本方案可以实现大小约为 10^{376} 的密钥空间，远大于 2^{100}，可以有效抵抗暴力攻击。

4 结 论

提出了一种 OFDM-PON 中基于 3D Arnold 变换和混沌 Frank 矩阵的保守数字混沌加密算法，并进行了仿真实验验证。首先，通过保守混沌系统产生混沌序列解决耗散混沌系统易被重构和预测的问题；然后，采用 PCA 技术处理混沌序列，以解决混沌序列的数字退化问题；最后，利用混沌序列控制 3D Arnold 变换的参数，实现对 OFDM 信号的置乱，提高系统的安全性，并利用混沌 Frank 矩阵降低系统的 PAPR。仿真实验结果表明，本方案可使系统的 PAPR 约降低 2.1 dB，在接收端 BER 相同的情况下，接收光功率约降低 1 dB。

参 考 文 献

[1] Abbas H S, Gregory M A. The next generation of passive optical networks: a review[J]. Journal of Network and Computer Applications, 2016, 67: 53-74.

[2] Tang M Z, Sun H, He R X, et al. Energy-efficient dynamic wavelength and bandwidth allocation algorithm supporting differentiated services for TWDM-PON[J]. Laser & Optoelectronics Progress, 2019, 56(18): 180601.
唐明珠, 孙皓, 何荣希, 等. TWDM-PON 中支持区分服务的节能动态波长带宽分配算法[J]. 激光与光电子学进展, 2019, 56(18): 180601.

[3] Li S S, Cheng M F, Chen Y T, et al. Enhancing the physical layer security of OFDM-PONs with hardware fingerprint authentication: a machine learning approach [J]. Journal of Lightwave Technology, 2020, 38(12): 3238-3245.

[4] Han M X, Wu Y T, Zhang Q W, et al. Secure algorithm for suppressing peak-to-average power ratio in OFDM-PON systems [J]. Acta Optica Sinica, 2019, 39(5): 0506004.
韩梦欣, 吴雅婷, 张倩武, 等. OFDM-PON 系统中一种抑制峰均功率比的安全算法[J]. 光学学报, 2019, 39(5): 0506004.

[5] Ni W L, Zheng Y F, Feng C Y. Application of pilot-assisted peak-to-average power ratio reduction technology in optical orthogonal frequency division multiplexing communication system [J]. Laser & Optoelectronics Progress, 2019, 56(14): 140601.
倪玮隆, 郑玉甫, 冯楚滢. 导频辅助降低 PAPR 技术在光正交频分复用通信系统中的应用[J]. 激光与光电子学进展, 2019, 56(14): 140601.

[6] Xiao Y Q, Wang Z Y, Cao J, et al. Time-frequency domain encryption with SLM scheme for physical-layer security in an OFDM-PON system[J]. IEEE/OSA Journal of Optical Communications and Networking, 2018, 10(1): 46-51.

[7] Hu X N, Yang X L, Shen Z W, et al. Chaos-based partial transmit sequence technique for physical layer security in OFDM-PON[J]. IEEE Photonics Technology Letters, 2015, 27(23): 2429-2432.

[8] Zhuo X H, Bi M H, Hu Z R, et al. Secure scheme for OFDM-PON system using TR based on modified Henon chaos [J]. Optics Communications, 2020, 462: 125304.

[9] Li C H, Wu Y T, Yu Y, et al. Dynamic encryption scheme based on channel phase information in OFDM-PON system[J]. Acta Optica Sinica, 2020, 40(10): 1006004.
李春华, 吴雅婷, 余衍, 等. OFDM-PON 系统中基于信道相位信息的动态加密方案[J]. 光学学报, 2020, 40(10): 1006004.

[10] Zhao J Y, Liu B, Mao Y Y, et al. High security

OFDM-PON with a physical layer encryption based on 4D-hyperchaos and dimension coordination optimization[J]. Optics Express, 2020, 28(14): 21236-21246.

[11] Xiao Y Q, Chen Y T, Long C X, et al. A novel hybrid secure method based on DNA encoding encryption and spiral scrambling in chaotic OFDM-PON[J]. IEEE Photonics Journal, 2020, 12(3): 1-15.

[12] Chen Y X, Huang Y T, Han Y, et al. Multi scrolls chaotic encryption scheme for CO-OFDM-PON[J]. Optics Express, 2020, 28(14): 19808-19817.

[13] Wu T W, Zhang C F, Wei H H, et al. PAPR and security in OFDM-PON via optimum block dividing with dynamic key and 2D-LASM [J]. Optics Express, 2019, 27(20): 27946-27961.

[14] Bi M H, Zhuo X H, Yang G W, et al. Chaotic Arnold transform and chirp matrix encryption scheme for enhancing the performance and security of OFDM-PON[J]. Optical Fiber Technology, 2019, 51: 64-70.

[15] Cang S J, Li Y, Xue W, et al. Conservative chaos and invariant tori in the modified Sprott A system [J]. Nonlinear Dynamics, 2020, 99(2): 1699-1708.

[16] Seleznev A, Mukhin D, Gavrilov A, et al. Bayesian framework for simulation of dynamical systems from multidimensional data using recurrent neural network [J]. Chaos, 2019, 29(12): 123115.

[17] Xia C. Design of new dissipative and conservative chaotic systems and its synchronous control [D]. Chongqing: Chongqing University of Posts and Telecommunications, 2018.
夏诚. 新型耗散与保守混沌系统的设计及其同步控制[D]. 重庆: 重庆邮电大学, 2018.

[18] Liu Y Q. Degradation analysis, optimization strategy and application for the digital chaotic systems [D]. Guilin: Guangxi Normal University, 2018.
刘运祺. 数字混沌系统退化分析、优化策略及其应用研究[D]. 桂林: 广西师范大学, 2018.

[19] Yuan F, Deng Y, Li Y X, et al. A cascading method for constructing new discrete chaotic systems with better randomness [J]. Chaos: an Interdisciplinary Journal of Nonlinear Science, 2019, 29(5): 053120.

[20] Liu C Y, Ding Q. A modified algorithm for the logistic sequence based on PCA [J]. IEEE Access, 2020, 8: 45254-45262.

[21] Hu Z Y, Chan C K. A 7-D hyperchaotic system-based encryption scheme for secure fast-OFDM-PON [J]. Journal of Lightwave Technology, 2018, 36 (16): 3373-3381.

[22] Guo Y, Jing S W, Zhou Y Y, et al. An image encryption algorithm based on Logistic-Fibonacci cascade chaos and 3D bit scrambling [J]. IEEE Access, 2020, 8: 9896-9912.

[23] Liu X Y, Cao Y P, Lu P. Research on optical image encryption technique with compressed sensing [J]. Acta Optica Sinica, 2014, 34(3): 0307002.
刘效勇, 曹益平, 卢佩. 基于压缩感知的光学图像加密技术研究[J]. 光学学报, 2014, 34(3): 0307002.

[24] Tao S, Tang C, Lei Z K. Image encryption based on vector decomposition and chaotic random phase mask [J]. Laser & Optoelectronics Progress, 2020, 57 (4): 041002.
陶珊, 唐晨, 雷振坤. 基于矢量分解和混沌随机相位掩模的图像加密[J]. 激光与光电子学进展, 2020, 57(4): 041002.

[25] Tian Y H. Research on channel estimation and coding in OFDM-PON[D]. Shanghai: Shanghai Jiao Tong University, 2014.
田月华. 正交频分复用无源光网络系统的信道估计和编码研究[D]. 上海: 上海交通大学, 2014.