基于神经网络与复合离散混沌系统的双重加密方法

肖成龙[①] 孙 颖[①②] 林邦姜[②] 汤 璇*[②] 王珊珊[①] 张 敏[②]
谢宇芳[②] 戴玲凤[②] 骆佳彬[②]

[①](辽宁工程技术大学软件工程学院 葫芦岛 125105)
[②](中国科学院海西研究院泉州装备制造研究中心 泉州 362200)

摘 要：正交频分复用(OFDM)已被广泛应用于无线通信系统，其数据传输安全具有一定的实际意义。该文提出了一种双重加密方案，采用神经网络生成置乱矩阵实现第1次加密，通过基于Logistic映射与Sine映射的复合离散混沌系统产生的混沌序列进行第2次加密。该双重加密方案极大提升了OFDM通信系统的保密性，可以有效地防止暴力攻击。相比于单一的1维Logistic映射的混沌系统，基于Logistic映射与Sine映射的复合离散混沌系统具有更大的密钥空间。该文运用Lyapunov指数与NIST测试验证了该混沌系统的混沌特性及随机性，并仿真验证了双重加密方案的保密性能。仿真结果表明，该文所提出的加密方案密钥空间为4×10^{93}，Lyapunov指数提高到0.9850，NIST测试中最大P值为0.9995。该双重加密方案可在不影响传输性能下极大提升OFDM通信系统的安全性。

关键词：保密通信；正交频分复用；复合离散混沌系统；神经网络；NIST测试

中图分类号：TN918.91 **文献标识码**：A **文章编号**：1009-5896(2020)03-0687-08

DOI: 10.11999/JEIT190213

Double Encryption Method Based on Neural Network and Composite Discrete Chaotic System

XIAO Chenglong[①] SUN Ying[①②] LIN Bangjiang[②] TANG Xuan[②]
WANG Shanshan[①] ZHANG Min[②] XIE Yufang[②] DAI Lingfeng[②] LUO Jiabin[②]

[①](*School of Software*, *Liaoning Technical University*, *Huludao* 125105, *China*)
[②](*Quanzhou Institute of Equipment Manufacturing*, *Haixi Institutes*,
Chinese Academy of Sciences, *Quanzhou* 362200, *China*)

Abstract: Orthogonal Frequency Division Multiplexing(OFDM) is widely used in wireless communication systems, and its data transmission security has certain practical significance. A double encryption scheme is proposed which enhances the confidentiality of the OFDM communication system and can prevent brute force attacks significantly. Specifically, the first encryption is achieved by using neural network to generate the scrambling matrix, and the second encryption is implemented by chaotic sequence generating by composite discrete chaotic system based on Logistic mapping and Sine mapping. Moreover, it has larger secret key space compared with the single one-dimensional Logistic mapping chaotic system. The performance of double encryption is measured by verifying its chaotic characteristics and randomness (Lyapunov exponent and NIST) as well as its security performance in simulation. The results show that Lyapunov index is increased to 0.9850, and the maximum P-value in the NIST test is 0.9995 by using the proposed double encryption in this paper. It indicates such double encryption significantly improve the confidentiality of the OFDM communication system without affecting the transmission performance.

Key words: Secure communication; Orthogonal Frequency Division Multiplexing(OFDM); Composite discrete chaotic system; Neural networks; NIST test

收稿日期：2019-04-03；改回日期：2019-09-18；网络出版：2019-10-15

*通信作者： 汤璇 xtang@fjirsm.ac.cn

基金项目：国家自然科学基金(61404069)，辽宁省教育厅一般科研项目(LJYL048)，辽宁省教育厅青年基金(LJ2017QL033)
Foundation Items: The National Natural Science Foundation of China(61404069), The Liaoning Provincial Department of Education General Research Project(LJYL048), The Liaoning Provincial Department of Education Youth Fund Project(LJ2017QL033)

1 引言

正交频分复用(Orthogonal Frequency Division Multiplexing, OFDM)已经广泛应用于现代无线技术通讯网络中。传统的OFDM信号由于其独特的时间和频率特性而易受恶意窃听的影响。混沌系统已成功应用于无线系统、多媒体等方面，用来提高系统的安全性[1]，如混沌加扰[2–4]，混沌星座操作[5–7]，以及混沌IQ加密技术[8,9]等。基于混沌的通信系统由于其鲁棒性和安全性备受关注，混沌系统的研究推动了保密通信的发展。现有的混沌映射可以分为两类：1维(1D)混沌映射和高维(HD)混沌映射。1维混沌映射的例子包括Logistic, Sine和Chebyshev映射。通常高维混沌结构比1维结构更加复杂，实现起来更加困难。通过对简单1维混沌映射进行改进使混沌系统能够在有限的区域内均匀分布[10]，能够提升加密性能。因此，改进简单的1维混沌系统用于加密也是较好的选择。基于保密通信的理论研究，研究人员已经提出了几种基于OFDM的安全技术。例如文献[11]提出了一种基于混沌编码的正交幅度调制(Quadrature Amplitude Modulation, QAM)的加密方法，在加密的QAM符号中，由改进的Logistic映射产生密钥序列对实部(I)和虚部(Q)分别编码。文献[12]提出了一种基于伪随机星座旋转与插入人工噪声的加密方案，利用混沌系统生成伪随机密钥，通过无线信道的不可逆性来保证OFDM系统的物理层安全。上述的方法中所用的混沌映射形式相对简单，而且插入人工噪声的方式会使信道的资源利用率降低。文献[13]利用无线信道的互易性，位置相关和时变的特性，提出了一种通过动态子载波坐标交织的新型反窃听OFDM系统。此外，还可以采用发送波束成形[14]，人工噪声[15]和协作发送[16]来提高基于OFDM传输的安全性。但是这些加密技术可能还需要额外的资源，如协作终端、信道资源和多个天线。这些基于数字混沌系统的方法由于具有显著的伪随机特性，差别很小的初始条件产生的混沌序列轨迹将快速发散并且从不重复。混沌序列由于具有对初始值的敏感性、巨大的参数空间[17–19]等特点，而成为OFDM系统加密的研究热点，使它能够增强加密的安全性。同时，已经提出了不同的安全策略，并得以证明。

本文针对OFDM通信系统提出了一种新的加密方案，实现了对OFDM系统中传输的数据信息进行保护。该加密方案利用复合离散混沌系统生成伪随机混沌序列，经过人工神经网络，生成置乱矩阵实现第1次加密，使用不同的混沌序列进行2次加密。该加密方案可以根据发送数据的大小动态调整置乱矩阵的大小、灵活性高，能够更大限度地防御暴力攻击，并且保密效果良好。

2 复合离散混沌系统

本节主要描述现有的两个混沌映射：1维Sine映射和1维Logistic映射，它们是复合离散混沌系统的基础。本文通过Lyapunov指数和NIST测试工具来证明复合离散混沌系统产生混沌序列的随机性。

2.1 复合离散混沌系统的组成

2.1.1 Logistic映射与Sine映射

Logistic映射与Sine映射在OFDM系统加密方案中应用十分广泛，其映射方程分别为

$$x_{n+1} = \mu x_n(1 - x_n) \tag{1}$$

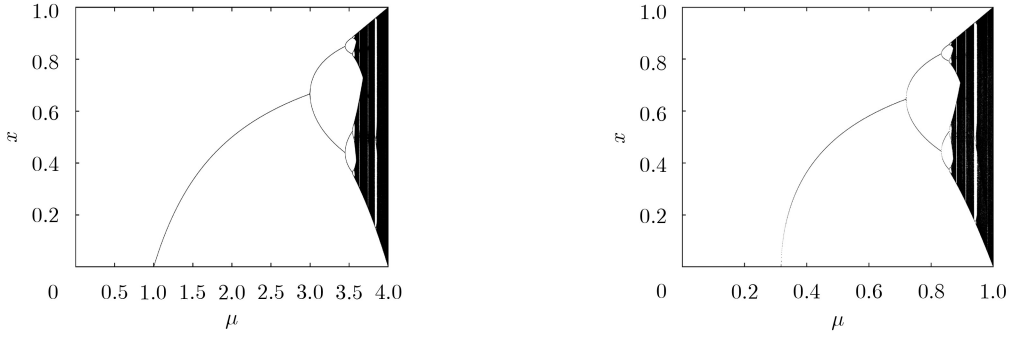
$$x_{n+1} = \mu \sin(\pi x_n) \tag{2}$$

其中，x表示迭代值，μ表示控制参数。

如图1(a)所示，迭代的初始值为0.3，迭代次数为1500次，省略前500个点，可以看出当$\mu = 4.0$时，Logistic系统的复杂性最大。图1(b)的迭代初始值为0.3，迭代次数为3000次，省略前1000次。当$\mu \in [0.87, 1]$时，Sine映射具有混沌特性。

2.1.2 复合离散混沌系统

令复合离散混沌系统为$f(x)$, $f(x)$是由$h(x)$和$g(x)$构成。其中$h(x)$是定义在$[0, 1]$区间的Logistic映



(a) Logistic 映射　　(b) Sine映射

图 1 Logistic映射与Sine映射

射。$g(x)$是Sine混沌系统，复合离散混沌系统的映射方程为

$$f(x)=f(h(x)+g(x))=\begin{aligned}&\mod(4\mu x_n(1-x_n)\\&+(1-\mu)\sin(\pi x_n),1)\end{aligned}\quad(3)$$

由于Logistic映射仅在小范围内存在混沌特性，本文将两个具有不同参数的Logistic混沌系统与Sine混沌系统先进行线性变换，再进行非线性运算。图2为复合离散混沌系统分岔图，混沌序列的初始值为0.3，参数μ取值为$[0,1]$，每间隔5×10^{-4}取1个μ值，共迭代了1000次，省略了前500次结果。从图2中可以看出将混沌区间扩展到了$[0,1]$区间。同理，若参数μ取值为$[0,4]$，则该混沌序列分布在$[0,4]$区间之间。

为了检测该混沌系统的性能，将该系统生成的混沌序列 $X=\{X_1,X_2,\cdots,X_n\}$转化为二值序列$K=\{K_1,K_2,\cdots,K_n\}$。采用选取平均值的方式确定阈值，$\bar{X}$表示混沌序列X的平均值。公式为

$$K=\begin{cases}0, & 0\le X<\bar{X}\\ 1, & \bar{X}\le X\le 1\end{cases}\quad(4)$$

2.2 Lyapunov指数

Lyapunov指数是验证混沌序列的随机性与混沌特性的重要指标。公式为

$$\lambda=\lim_{i\to\infty}\left\{\frac{1}{i}\sum_{n=0}^{i-1}\ln|f'(x_n)|\right\}\quad(5)$$

根据式(5)，若该混沌系统的Lyapunov指数为正值表明该混沌系统具有混沌特性，正值越大表明该混沌系统的混沌特性越好。令$b(x)=h(x)+g(x)$，则$f(x)=f(b(x))$。Lyapunov指数的计算公式为

$$\begin{aligned}\lambda&=\lim_{i\to\infty}\left\{\frac{1}{i}\sum_{n=0}^{i-1}\ln|f'(b(x_n))|\right\}\\&=\lim_{i\to\infty}\left\{\frac{1}{i}\sum_{n=0}^{i-1}\ln|f'(b(x_n))\cdot b'(x_n)|\right\}\\&=\lim_{i\to\infty}\left\{\frac{1}{i}\sum_{n=0}^{i-1}(\ln|f'(b(x_n))|+\ln|b'(x_n)|)\right\}\\&=\lim_{i\to\infty}\left\{\frac{1}{i}\sum_{n=0}^{i-1}\ln|f'(b(x_n))|+\frac{1}{i}\sum_{n=0}^{i-1}\ln|b'(x_n)|\right\}\\&=\lim_{i\to\infty}\left\{\frac{1}{i}\sum_{n=0}^{i-1}\ln|f'(b(x_n))|\right\}\\&=+\lim_{i\to\infty}\left\{\frac{1}{i}\sum_{n=0}^{i-1}\ln|b'(x_n)|\right\}\\&=\lambda_{f(x)}+\lambda_{b(x)}\end{aligned}\quad(6)$$

由于$f(x)$是两个混沌系统经过线性变换后再进行模1运算，并不影响Lyapunov值的大小，所以$\lambda_{f(x)}>0$。由于$b(x)$是由Logistic映射与Sine映射进行线性变换求得，由于混沌系统的可加性，所以$\lambda_{b(x)}>0$。根据式(6)得出，复合离散混沌系统的Lyapunov指数大于0，所以该混沌系统具有混沌特性。各个混沌映射的Lyapunov指数如表1所示。

3　神经网络生成置乱矩阵

在图形图像加密方案中经常会使用矩阵置乱图像像素的方法，由于不同图像的像素矩阵大小相同，生成的置乱矩阵一般都为像素矩阵的大小，故缺少随机性，使得加密的随机性能降低。但是在通信领域中由于加密的密文矩阵大小不确定，可以生成不同大小的随机矩阵对数据进行加密，大大提高了保密的安全性。本文采用神经网络的方法对OFDM系统中的星座图进行双重扰乱。神经网络架构如图3所示。

神经网络由输入层、隐含层和输出层构成，每层中的神经元之间以全连接的形式相连。神经网络

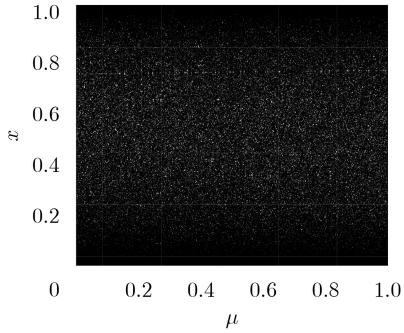


图 2 复合离散混沌系统

表 1　混沌系统Lyapunov指数

混沌系统	Logistic映射	Sine映射	复合离散混沌系统
Lyapunov指数	0.6118	0.5381	0.9850

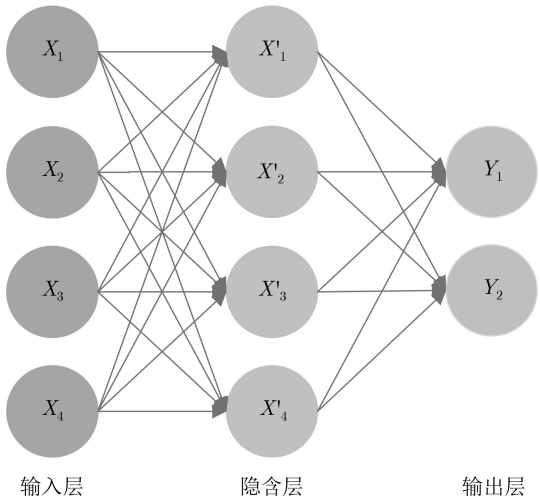


图 3 神经网络架构

通过输入层输入数据，传入隐含层，隐含层将收到数据进行处理后传入输出层，输出层收到数据进一步处理后输出，该过程称为神经网络的传播过程。本文采用神经网络是为了产生OFDM系统第1次加密过程中的置乱矩阵，因此每一次迭代中的$\boldsymbol{W}, \boldsymbol{B}$和$\boldsymbol{Z}$矩阵均为随机的，其中$\boldsymbol{W}=\{\boldsymbol{W}_1, \boldsymbol{W}_2\}$, $\boldsymbol{B}=\{\boldsymbol{B}_1, \boldsymbol{B}_2\}$。并且是已经训练好的网络，不需要考虑学习效率的影响。

神经网络中的输入层是从混沌序列X中随机选取数据。输出层为Y，由Y_1, Y_2 构成。Y_1, Y_2经过进一步处理为Y_1', Y_2'来表示置乱矩阵的行值和列值。传输函数由函数$L(x)$, $M(x)$和$T(x)$构成，以实现对输入数据的处理。

$$\boldsymbol{I}=[X_1, X_2, X_3, X_4] \tag{7}$$

函数$L(x)$将输入值I分别乘以权值加上偏置得到下一层的输入值，变换后的矩阵为$\boldsymbol{I}'$，即

$$\boldsymbol{I}'=\boldsymbol{W}_1 I+\boldsymbol{B}_1=[X_1', X_2', X_3', X_4']^{\mathrm{T}} \tag{8}$$

其中，$\boldsymbol{W}_1$的大小为4×4(行列)的方阵，$\boldsymbol{B}_1$的大小为4×1。$\boldsymbol{I}'$通过传输函数$M(x)$和$T(x)$得到输出值Y_1, Y_2，其公式为

$$Y=M(T(\boldsymbol{W}_2\boldsymbol{I}'+\boldsymbol{B}_2), \boldsymbol{Z}) \tag{9}$$

其中，$\boldsymbol{W}_2$的大小为2×4, $\boldsymbol{B}_2$的大小为2×1。$\boldsymbol{W}_1$和$\boldsymbol{B}_1$是输入层到隐含层的权值和偏置矩阵，$\boldsymbol{W}_2$和$\boldsymbol{B}_2$是隐含层到输出层的权值和偏置矩阵。权值和偏置矩阵均从混沌序列中随机选取数值。$\boldsymbol{Z}$为函数$M(x)$的判断参数，大小为2行1列。$M(x)$和$T(x)$分别为

$$M(T(x), Z)=\begin{cases} T(x)/Z, & 0<T(x)\le Z \\ (1-T(x))/(1-Z), & Z<T(x)<1 \end{cases} \tag{10}$$

$$T(x)=1/(1+\mathrm{e}^{-x}) \tag{11}$$

经过式(11)的运算，使得$0<T(x)<1$，这时$M(x)$刚好与$T(x)$的区间相符，Z为判断参数，并且$0<Z<1$。为了保证每次循环Z值的差异性，每运行1次函数得到输出的Y值和Z值都将更新1次，更新后的Z值为

$$Z=(0.3\times Y)+0.6 \tag{12}$$

神经网络每运行1次，就会产生2个随机的Y_1, Y_2值。更新Z值后，采用更新后的值循环运行神经网络计算得到新的输出值Y_1, Y_2。假设所要生成的置乱矩阵的大小为$F\times N$，所以需要将神经网络的输出Y_1, Y_2进行下一步操作得到置乱矩阵的行值和列值。公式为

$$\left.\begin{aligned} Y_1' &= \mathrm{mod}(\mathrm{ceil}(\mathrm{Y}_1\times 10^{15}), F) \\ Y_2' &= \mathrm{mod}(\mathrm{ceil}(\mathrm{Y}_2\times 10^{15}), N) \end{aligned}\right\} \tag{13}$$

当产生的Y_1', Y_2'这一对值与已产生数值均不相同，则保留该数值，当产生的矩阵为$F\times N$时，则停止运行。

4 加解密算法

本文中所提出的加密算法与明文密切相关。由于混沌序列对初始值非常敏感，即使初值的差别很小但所产生混沌序列的差别却很大，有效地防止了攻击者对密钥的破解。为了抵抗暴力攻击，基于混沌的加密算法密钥长度应该大于100位[20]。采用神经网络的方式生成置乱矩阵$[F, N]$，其中$F, N>100$，共进行2次置乱，首先对OFDM生成的星座图中各个星座点进行第1次置乱，其次再对串并转换加入导频之后的数据进行2次置乱。为了进一步提高保密性能，两次置乱采用不同的混沌序列。本文加密算法设计图如图4所示。

4.1 加密算法

当置乱矩阵的大小为$F\times N$时，读取发送数据序列中前$F\times N$位二进制数值，用于计算混沌系统的参数μ和初始值x_0。其中μ的取值为$[0, 4]$，x_0的取

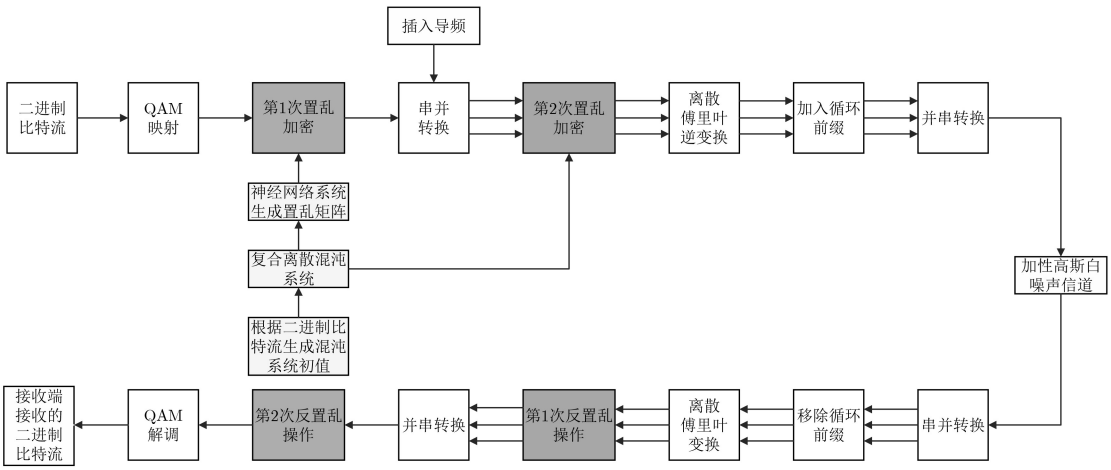


图 4 OFDM系统加密方案

值为[0, 1]。计算复合离散混沌系统的参数μ和初始值x_0的公式为

$$\left.\begin{aligned}\mu &= \mathrm{mod}(\mathrm{sum}, 4)\\ x_0 &= \mathrm{mod}(\mathrm{sum}, 10)\times 0.1\end{aligned}\right\} \tag{14}$$

不同的初值$x_0 = x_0 \times f$产生不同的混沌序列，运行复合离散混沌系统，迭代$N_0 + g$次，选取后g次迭代作为可用的密钥序列。式(14)中的sum表示OFDM系统输入数据的二进制序列中$[1, F\times N/2]$与$[F\times N/2+1, F\times N]$按位进行异或运算并求和。$f$表示sum除以$F\times N/2$求取的平均值。根据式(14)每运行1次混沌系统选取不同的初值，生成不同的混沌序列。本文中需要选取4个不同的混沌序列X_l, X_s, X_q, X_m。加密算法步骤如下所示。

步骤 1　读取OFDM系统中输入数据的二进制矩阵，假设生成的置乱矩阵的小为$F\times N$，计算出复合离散混沌系统的初值x_0与参数μ，生成混沌序列X_l, X_s, X_q, X_m;

步骤 2　随机选取序列X_l中的数值作为输入数据I。权值和偏置矩阵$\boldsymbol{W}_1$, $\boldsymbol{B}_1$与$\boldsymbol{W}_2$, $\boldsymbol{B}_2$分别从序列X_s, X_q中随机选取。运行神经网络生成Y_1, Y_2，将每次生成的Y_1, Y_2值分别处理为$[1, F]$和$[1, N]$区间的整数Y_1', Y_2'，并把每次迭代产生的Y_1', Y_2'分别存储在矩阵$\boldsymbol{H}$, $\boldsymbol{R}$中。如果Y_1', Y_2'与已产生数值均不相同，则保留该数值，直到生成行矩阵$\boldsymbol{H}$的长度为F，列矩阵$\boldsymbol{R}$的长度为N为止;

步骤 3　进行第1次加密，根据置乱矩阵对应的行列索引对OFDM系统中星座图进行置乱，将星座图矩阵转换为F行N列矩阵。若星座图中的星座点大于$F\times N$，则可以将星座矩阵分为k个$F\times N$矩阵，其中$k = 1, 2, \cdots, n$，这时可以运行k次神经网络生成k个不同的置乱矩阵，分别对k个矩阵进行置乱加密。令星座图的矩阵为$\boldsymbol{C}$，置乱后的矩阵为$\boldsymbol{D}$。置乱公式为

$$\begin{aligned}\boldsymbol{D}_k(i,j) = \boldsymbol{C}_k(H_k(i), R_k(j)),\quad i = 1, 2, \cdots, F,\\ j = 1, 2, \cdots, N\end{aligned} \tag{15}$$

其中，$\boldsymbol{D}_k$表示第k个置乱后的矩阵，$\boldsymbol{C}_k$表示第k个星座图矩阵，$H_k(i)$表示置乱矩阵中行矩阵的每个值，$R_k(j)$表示列矩阵的每个值;

步骤 4　在进行第1次置乱后，将k个置乱后的矩阵转换成行值为1的矩阵;

步骤 5　选取混沌序列X_m中的值，取出每个值的小数点后15位数字存储在数组中，将这15位数字去除重复的数字后去除0和9，判断数组的长度是否为8，若不为8则舍掉该数组。则保留下来数组中的数值为[1, 8]。将保留下来的数组按照从小到大的顺序排序，排序后的数组记作A，然后通过数组A中数据的顺序保存每个数据在原来数组中的位置，生成用于第2次加密的位置矩阵$\boldsymbol{A}'$;

步骤 6　重复步骤5，生成加密所需的全部位置矩阵;

步骤 7　对串并转换插入导频后的数据利用步骤6生成的位置矩阵进行第2次置换加密，直到串并转换的循环全部结束，至此，第2次加密结束。

4.2 解密算法

解密算法为加密算法的逆过程。接收端收到加密后的数据，第1步根据位置矩阵进行反置乱得到矩阵$\boldsymbol{D}$，第2步根据置乱矩阵将$\boldsymbol{D}$进行反置乱即可得到原始的矩阵$\boldsymbol{C}$。

5 仿真结果

本文使用的仿真环境为Matlab 2015b，通过仿真实现混沌系统与OFDM系统的数据传送与接收。

5.1 混沌系统NIST测试分析

本文采用NIST测试工具对复合离散混沌系统产生的混沌序列进行随机性测试。NIST测试工具是由15个测试组成，用于测试加密过程中使用的二进制序列的随机性。每个测试都会产生一个P值，它是区间[0, 1]上的实数。如果P值大于显著性水平α(α默认等于0.01)，则分析的二进制序列通过测试，表明该序列被认为是随机的，置信度为99%，并且P值越大表明序列的随机性越好。

将混沌序列经过式(5)处理成0, 1二进制数据。本文随机选取了20组混沌序列进行测验，每个序列的长度为$n = 1000000$ bit。表2的第3列表示20组序列所测P值的平均值。测试结果显示，每个测试的

表 2　NIST测试结果

序号	测试项目	P 值	测试结果
1	Frequency	0.7188	Success
2	Block Frequency	0.3721	Success
3	Cumulative Sums	0.5153	Success
4	Runs	0.9995	Success
5	Longest Run of Ones	0.6147	Success
6	Rank	0.8624	Success
7	Discrete Fourier Transform	0.9268	Success
8	Nonperiodic Template Matchings	0.9889	Success
9	Overlapping Template Matchings	0.7125	Success
10	Universal Statistical	0.6124	Success
11	Approximate Entropy	0.1522	Success
12	Random Excursions	0.4998	Success
13	Random Excurisions Variant	0.3114	Success
14	Serial	0.2962	Success
15	Linear Complexity	0.9855	Success

P值均大于0.01，即置信度为99%，表明该复合混沌系统所产生的混沌序列都是随机的[21]。

总而言之，该混沌系统在扩展Logistic混沌系统映射区间的同时，保证了混沌系统的随机性能，使得混沌序列的取值范围更广泛，生成的有效密钥更多，并且育有良好的加密特性。

5.2 加密结果及性能分析

通过仿真，验证了该加密方案在OFDM系统下的安全性。本文所采用的OFDM系统参数如表3所示。第1次加密过程中生成的置乱矩阵大小为$[124, 100]$。串并转换循环次数为100次，插入的导频数目共400个，第2次加密矩阵的大小为$[1600, 8]$。

表 3 OFDM系统参数

特性	参数	特性	参数
调制方式	4QAM	FFT点数	128
数据子载波	128	内插导频	4
循环前缀	4	OFDM符号数	100
信道类型	AWGN	–	–

接收端收到未还原及未解调数据的散点图如图5所示。

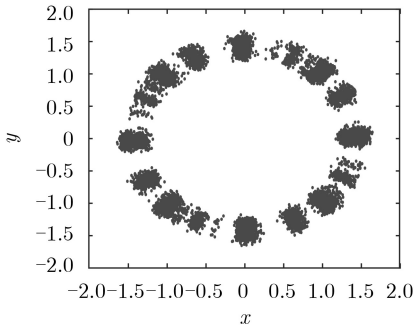


图 5 接收端未还原散点图

传统OFDM系统、星座旋转与本文所提出的双重加密的信噪比与误码率之间的关系如图6所示。当窃听者的误码率为0.5时，表明窃听者无法还原有用数据。本文所提出的加密方案和文献[12]中提出的加密方案都具有安全性，但是文献[12]提出的方法需要增加额外的人工噪声，当数据量十分庞大时会极大的浪费系统资源。图6所示，与OFDM本身相比，本文提出的加密方案没有明显衰落，即加密方案并没有使OFDM系统的稳定性与性能降低。当信噪比为13 dB时，误码率小于10^{-6}。

由本文提出的加密方案可知，密钥由复合离散混沌系统的参数N_0, x_0和μ以及X_l, X_s, X_q, X_m共同组成。N_0次初始迭代选取1000，μ的取值为$[0, 4]$区间，x_0的取值为$[0, 1]$区间。由于x_0, μ, X_l, X_s,

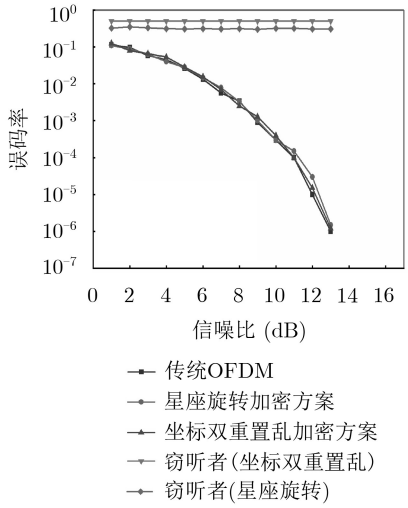


图 6 传统OFDM系统、星座旋转与双重位置置乱的误码率性能对比

X_q, X_m的取值均为浮点数，根据电气和电子工程师协会(IEEE)浮点标准[22]，64位双精度数的计算精度约为10^{-15}。所以该加密算法的密钥空间为$10^3 \times (1 \times 10^{15})^4 \times 4 \times 10^{15} \times 1 \times 10^{15} = 4 \times 10^{93} \approx 2^{311}$，大于文献[4,8,9,11,17,18]的密钥空间。由于搜索正确的密钥需要大量的时间，因此该密钥空间可以有效地防止窃听，并且该密钥空间大于2^{100}，满足文献[20]中建议的密钥空间要求，可以很好地抵抗暴力攻击。

从仿真结果来看，使用本文中所提出的双重加密方案能够保障发送者和合法接受者之间安全通信，提高了OFDM通信系统的安全性，并且该加密方案不需要插入人工噪声，可以有效防止信道资源的浪费。若窃听者没有正确的密钥，则不能得到正确的发送数据。与缺乏安全机制的传统OFDM系统相比，该方案仅产生可忽略的误码率。

6 结束语

本文提出了一种双重加密方案，并且运用复合离散混沌系统生成混沌序列密钥。密钥的生成与系统传输的数据密切相关，通过Lyapunov指数和NIST测试两个方面，证明了该混沌系统的混沌特性与混沌序列的随机性。利用神经网络的方式生成置乱矩阵对QAM调制后的星座点进行置乱，在串并转换加入导频之后运用不同的混沌序列进行第2次加密置乱。若窃听者没有正确地还原数据信息则无法确定混沌系统的初始值与控制参数。当窃听者没有解密密钥时，窃听者无法正确还原数据信息。传输过程中的数据与复合离散混沌系统构成一个整体，使得在整个加密过程中，明文可以作为生成密钥的一部分。通过仿真证明，该方案与传统的

OFDM系统相比，误码率可以忽略不记。当数据量过于庞大时，生成置乱矩阵的时间也将会提高，当需要生成多个置乱矩阵时可以考虑使用并行计算的方式来减少大量计算所用的时间，下一步工作是当数据量过大时降低系统计算的时间并且不断探索更好的加密方式。

参 考 文 献

[1] 禹思敏, 吕金虎, 李澄清. 混沌密码及其在多媒体保密通信中应用的进展[J]. 电子与信息学报, 2016, 38(3): 735–752. doi: 10.11999/JEIT151356.
YU Simin, LÜ Jinhu, and LI Chengqing. Chaos cipher and its application in multimedia secure communication[J]. *Journal of Electronics & Information Technology*, 2016, 38(3): 735–752. doi: 10.11999/JEIT151356.

[2] ZHANG Wei, ZHANG Chongfu, CHEN Chen, *et al*. Brownian motion encryption for physical-layer security improvement in CO-OFDM-PON[J]. *IEEE Photonics Technology Letters*, 2017, 29(12): 1023–1026. doi: 10.1109/LPT.2017.2702159.

[3] ZHANG Lijia, XIN Xiangjun, LIU Bo, *et al*. Physical secure enhancement in optical OFDMA-PON based on two-dimensional scrambling[J]. *Optics Express*, 2012, 20(26): B32–B37. doi: 10.1364/OE.20.000B32.

[4] ZHANG Chongfu, ZHANG Wei, CHEN Chen, *et al*. Physical-Enhanced secure strategy for OFDMA-PON using chaos and deoxyribonucleic acid encoding[J]. *Journal of Lightwave Technology*, 2018, 36(9): 1706–1712. doi: 10.1109/JLT.2018.2789435.

[5] ZHONG Ju, YANG Xuelin, and HU Weisheng. Performance-Improved secure OFDM transmission using chaotic active constellation extension[J]. *IEEE Photonics Technology Letters*, 2017, 29(12): 991–994. doi: 10.1109/LPT.2017.2700861.

[6] HAJOMER A A E, YANG Xuelin, and HU Weisheng. Chaotic walsh-hadamard transform for physical layer security in OFDM-PON[J]. *IEEE Photonics Technology Letters*, 2017, 29(6): 527–530. doi: 10.1109/LPT.2017.2663400.

[7] ZHANG Lijia, LIU Bo, and XIN Xiangjun. Secure optical generalized filter bank multi-carrier system based on cubic constellation masked method[J]. *Optics Letters*, 2015, 40(12): 2711–2714. doi: 10.1364/OL.40.002711.

[8] ZHANG Wei, ZHANG Chongfu, CHEN Chen, *et al*. Joint PAPR reduction and physical layer security enhancement in OFDMA-PON[J]. *IEEE Photonics Technology Letters*, 2016, 28(9): 998–1001. doi: 10.1109/LPT.2016.2522965.

[9] ZHANG Wei, ZHANG Chongfu, CHEN Chen, *et al*. Hybrid chaotic confusion and diffusion for physical layer security in OFDM-PON[J]. *IEEE Photonics Journal*, 2017, 9(2): 7201010. doi: 10.1109/JPHOT.2017.2683501.

[10] 臧鸿雁, 黄慧芳, 柴宏玉. 一类2次多项式混沌系统的均匀化方法研究[J]. 电子与信息学报, 2019, 41(7): 1618–1624. doi: 10.11999/JEIT180735.
ZANG Hongyan, HUANG Huifang, and CHAI Hongyu. Homogenization method for the quadratic polynomial chaotic system[J]. *Journal of Electronics & Information Technology*, 2019, 41(7): 1618–1624. doi: 10.11999/JEIT180735.

[11] ZHANG Wei, ZHANG Chongfu, JIN Wei, *et al*. Chaos coding-based QAM IQ-Encryption for improved security in OFDMA-PON[J]. *IEEE Photonics Technology Letters*, 2014, 26(19): 1964–1967. doi: 10.1109/LPT.2014.2343616.

[12] MA Ruifeng, DAI Linglong, WANG Zhaocheng, *et al*. Secure communication in TDS-OFDM system using constellation rotation and noise insertion[J]. *IEEE Transactions on Consumer Electronics*, 2010, 56(3): 1328–1332. doi: 10.1109/TCE.2010.5606266.

[13] LI Hao, WANG Xianbin, and ZOU Yulong. Dynamic subcarrier coordinate interleaving for eavesdropping prevention in OFDM systems[J]. *IEEE Communications Letters*, 2014, 18(6): 1059–1062. doi: 10.1109/LCOMM.2014.2315648.

[14] WANG Huiming, YIN Qinye, and XIA Xianggen. Distributed beamforming for physical-layer security of two-way relay networks[J]. *IEEE Transactions on Signal Processing*, 2012, 60(7): 3532–3545. doi: 10.1109/TSP.2012.2191543.

[15] El SHAFIE A, TOURKI K, and AL-DHAHIR N. An artificial-noise-aided hybrid TS/PS scheme for OFDM-Based SWIPT systems[J]. *IEEE Communications Letters*, 2017, 21(3): 632–635. doi: 10.1109/LCOMM.2016.2642105.

[16] DING Zhiguo, LEUNG K K, GOECKEL D L, *et al*. On the application of cooperative transmission to secrecy communications[J]. *IEEE Journal on Selected Areas in Communications*, 2012, 30(2): 359–368. doi: 10.1109/JSAC.2012.120215.

[17] CHENG M, DENG L, WANG X, *et al*. Enhanced secure strategy for OFDM-PON system by using hyperchaotic system and fractional fourier transformation[J]. *IEEE Photonics Journal*, 2014, 6(6): 7903409. doi: 10.1109/JPHOT.2014.2363427.

[18] SHEN Zanwei, YANG XueLin, HE Hao, *et al*. Secure transmission of optical DFT-S-OFDM data encrypted by digital chaos[J]. *IEEE Photonics Journal*, 2016, 8(3): 7904609. doi: 10.1109/JPHOT.2016.2564438.

[19] HU Zhouyi and 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. doi: 10.1109/JLT.2018.2841042.

[20] ALVAREZ G and LI Shujun. Some basic cryptographic requirements for chaos-based cryptosystems[J]. *International Journal of Bifurcation and Chaos*, 2006, 16(8): 2129–2151. doi: 10.1142/S0218127406015970.

[21] RUKHIN A, SOTO J, NECHVATAL J, *et al*. A statistical test suite for Random and pseudorandom number generators for cryptographic applications[R]. Special Publication 800-22 Revision 1a, 2010.

[22] IEEE Computer Society. ANSI/IEEE Std 754-1985 IEEE standard for binary floating-point arithmetic[S]. New York: IEEE Computer Society, 1985.

肖成龙：男，1984年生，副教授，研究方向为信号处理与软硬件协同设计.

孙 颖：女，1994年生，硕士生，研究方向为保密通信与混沌密码学.

林邦姜：男，1987年生，副研究员，研究方向为无线光通信.

汤 璇：女，1984年生，研究员，研究方向为无线光通信.

王珊珊：女，1984年生，副教授，研究方向为软硬件协同设计与并行计算.

张 敏：女，1992年生，助理工程师，研究方向为无线光通信.

谢宇芳：女，1992年生，助理工程师，研究方向为无线光通信.

戴玲凤：女，1980年生，工程师，研究方向为无线光通信.

骆佳彬：男，1991年生，助理工程师，研究方向为无线光通信.