

# 基于混沌与自编码相融合的扩频码构造方法

张晓蓉<sup>1</sup> 吴成茂<sup>1</sup> 李文学<sup>2</sup>

(西安邮电大学电子工程学院 西安 710121)<sup>1</sup> (中国人民解放军理工大学国防工程学院 南京 210007)<sup>2</sup>

**摘要** 针对传统扩频码周期短及安全性差的不足,提出混沌映射与自编码相融合的扩频码构造方法。该方法首先将 Logistic 混沌映射产生的序列进行同态均匀映射以获取高平衡度伪随机序列,其次与其不等长子序列复合重复迭代并生成长度随迭代次数呈几何级数增加的复合符号序列,最后与自编码序列经二维 Henon 映射相融合产生高质量复合随机序列。以混沌和自编码为基础分析该方法的有效性,并与现有扩频码进行仿真测试比较,结果表明新扩频码具有良好的相关特性和较高的复杂性,并能获得较低的扩频误码率。

**关键词** 自编码,均匀映射, Henon 映射,扩频码,误码率

**中图分类号** TN914.14 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2015.3.009

## Method of Constructing Spread-spectrum Code Based on Chaos and Self-coded

ZHANG Xiao-rong<sup>1</sup> WU Cheng-mao<sup>1</sup> LI Wen-xue<sup>2</sup>

(School of Electronic Engineering, Xi'an University of Posts and Telecommunications, Xi'an 710121, China)<sup>1</sup>

(National Defense College of Engineering, PLA University of Science and Technology, Nanjing 210007, China)<sup>2</sup>

**Abstract** Aiming at traditional spreading codes with short period and poor security, a method of spreading codes constructed by means of combination chaotic maps with self-coded was proposed. The method firstly makes a homomorphic uniform mapping to a sequence generated by Logistic chaotic mapping to obtain a high degree of balance pseudo-random sequence, and then repeats iteration with the sub-sequence of different length to obtain the complex symbol sequence of which length increases geometrically by the time of iterations. Finally, it is combined with the self-coded sequence to generate a high quality composite random sequence through the dimensional Henon map. To analyze the effectiveness of the method based on Chaos and self-coded, we compared it by simulation test. The result shows the new spreading code has better correlation and a higher degree of complexity, and obtains a lower spread bit error rate.

**Keywords** Self-coded, Uniform map, Henon map, Spreading code, Bit error rate

## 1 引言

扩频是指将信息带宽进行扩展传输的通信抗干扰技术体制<sup>[1]</sup>。扩频通信主要包括直接序列扩频、跳频扩频和跳时扩频 3 大类。扩频通信广泛应用于现代移动通信和军事作战指挥系统等领域。直接序列扩频通信是扩频通信中应用最为广泛的一种通信方式,其关键在于如何构造性能优良的扩频码序列。m 序列是广泛应用于直接序列扩频通信的一种扩频码,因采用线性移位寄存器产生,其存在周期短、互相关性差、码组数目有限,以及序列复杂度低等缺陷<sup>[2]</sup>,采用累积检测法易于侦破且难以满足多址通信中地址码的要求。Gold 码序列是基于 m 序列的一种改进拟正交码序列,具有良好周期自相关性和互相关性,但是码数量依然有限且周期短,易被复制和侦查,导致其扩频通信保密性差<sup>[3]</sup>。为了克服这些经典扩频码的不足,大量文献探讨了类 Gold 序列、Walsh 序列、双重 BCH 序列、Kasami 序列、Bent 序列、Baker 序列、Williad 序列

和 Neuman-Hofman 序列等在扩频通信中的应用<sup>[4]</sup>。扩频通信在雷达、导航、测距和定位等领域广泛应用,其安全性和抗干扰性要求甚高,这使得现有扩频码难以满足其高可靠性的需要。于是,学者们开始研究具有良好复杂性和随机性的混沌理论在扩频通信中的应用<sup>[5-10]</sup>,以获得良好相关性的长周期扩频码。Bateni 等人<sup>[5]</sup>较早地利用混沌映射构造随机 PN 序列并应用于 CDMA 扩频系统。后来,学者们不断提出了奇偶相关的 Chebyshev 映射<sup>[6]</sup>、Logistic 映射<sup>[7]</sup>、拟 Tent 映射<sup>[8]</sup>、二维 Ikeda 映射<sup>[9]</sup>等构造扩频序列并应用于 DS/CDMA 系统;Youssef 等人<sup>[10]</sup>还研究了混沌序列在剩余数扩频系统的实现问题。针对混沌映射所产生扩频序列具有互相关性较差的缺点, Martoyo 等人<sup>[11]</sup>提出了正交混沌扩频码构造法,它能极大地改善混沌扩频通信系统的性能。最近,针对 Logistic 映射、Tent 映射本身的弱混沌特性的不足,文献<sup>[12-14]</sup>提出了一种分段型 Logistic 映射、分段 Skew Tent 映射以及三维混沌映射产生高性能扩频码的方法。鉴于扩频通信对

到稿日期:2014-04-15 返修日期:2014-07-20 本文受国家自然科学基金重点项目(90607008),国家自然科学基金项目(61073106),陕西省自然科学基金项目(2014JM8331,2014JQ5183,2014JM8307),陕西省教育厅自然科学基金项目(2013JK1129),西安邮电大学研究生创新基金项目资助。

张晓蓉(1989—),女,主要研究方向为扩频通信,E-mail:971701590@qq.com;吴成茂(1968—),男,高级工程师,硕士生导师,主要研究方向为多媒体通信和图像处理、扩频通信技术;李文学(1990—),男,主要研究方向为国防作战指挥。

扩频码具有较高安全性的需要,学者们对混沌序列的复杂性和安全性作了进一步研究<sup>[15,16]</sup>,证明了混沌序列作为扩频码比传统 m 序列、Gold 序列、Walsh 序列等更有利于扩频通信的需要。但是混沌序列作为扩频码与传输信源信息无关,不能保证扩频序列随传输信源信息变化而发生改变,有可能出现传输不同信源信息而使用的扩频序列完全相同的现象,不利于军事战场环境中信息对抗的需要。针对上述这些扩频码与传输信源信息无关的不足,学者们提出采用线性滤波法从不断变化的信源序列中提取一种称为自编码的伪随机序列作为扩频码<sup>[17-19]</sup>并用于扩频通信,以保证扩频码与传输信源信息之间紧密关联且随信源信息发生改变而改变,极大地提高了抗扩频码检测能力,但是这种自编码扩频序列具有复杂性低、周期短的缺陷。于是,本文提出将混沌序列与自编码序列通过 Henon 混沌映射相融合,获得一种新的复合序列作为扩频码,它充分利用了混沌序列所具有的高复杂性和随机性,以及自编码序列所具有的良好相关性、平衡性和信源关联性,能满足高安全性要求的信息对抗环境扩频通信的需要。通过多用户扩频通信系统仿真测试表明,本文所提出的扩频码构造法是有用的,同时其传输误码率相比现有混沌扩频码、自编码扩频码都有了显著降低,能提高扩频通信系统的可靠性和安全性,有利于强电磁环境下信息对抗通信的需要。

## 2 Logistic 映射及平衡随机序列

混沌是 20 世纪发展起来的动力系统理论,它已广泛用于控制等众多领域。近十多年来,混沌理论在信息安全、通信等方面也取得了长足发展,特别是当前的混沌通信已引起众多学者的高度关注。本文重点探讨混沌映射用于扩频序列的构造,其中应用最广泛的混沌映射是一维 Logistic 映射,它具有运算简单且易于实现等优点,已成为产生离散伪随机序列的重要方法之一。

### 2.1 Logistic 映射

Logistic 映射是一种典型的非线性动态系统,它所产生的序列呈随机性,对该映射的初始值和参数极为敏感。相比传统线性同余法所产生的伪随机序列,Logistic 映射所产生的随机序列数量多、相关性好、保密性强且易再现。

Logistic 映射描述为<sup>[12]</sup>

$$x_{n+1} = \mu x_n (1 - \mu x_n), n=0, 1, \dots \quad (1)$$

其中,  $\mu$  是映射参数,当  $3.569946 \leq \mu \leq 4$  时, Logistic 映射进入混沌状态;当  $\mu=4$  时为满映射,其输入和输出都分布在区间  $(0, 1)$  上。这种混沌映射所产生的序列具有理想的相关特性。本文利用它产生初始离散伪随机序列,其方法如下:

$$x_n^* = \begin{cases} 1, & x_n > 0.5 \\ 0, & x_n \leq 0.5 \end{cases}, n=0, 1, \dots \quad (2)$$

### 2.2 平衡伪随机序列构造

为满足平衡伪随机序列的构造需要,下面引入 3 个基本概念<sup>[20]</sup>。

**定义 1** 设  $X = \{x_i\}_1^{N_1}$  是一个长为  $N_1$  的符号序列,状态集为  $A = \{a_1, a_2, \dots, a_k\}$ ,若  $X$  在状态集  $A$  的符号分别由状态集  $B = \{0, 1\}$  的有限序列  $B_1, B_2, \dots, B_k$  替换得到长度为  $N_2$  的符号序列,则称  $Y = \{y_i\}_1^{N_2}$  为复合符号序列。

**定义 2** 如果将复合符号序列  $Y = \{y_i\}_1^{N_2}$  的长度为  $d$  的子序列视为二进制实数,顺序得到的  $N_2 - d + 1$  个数构成一个时间序列  $Z$ ,若  $Z$  为混沌的,则称  $Z$  为复合符号混沌序列。

**定义 3** 设  $X = \{x_i\}_1^{N_1}$  为一个混沌时间序列,均匀映射的定义为

$$y_n = U(x_n) = \frac{1}{N} K(x_n), n=1, 2, \dots, N \quad (3)$$

其中,  $N$  是实值序列的长度,  $K(x_n)$  是  $x_n$  在序列  $\{x_n\}_1^N$  中按升序排列的序号。

另外,为了将实值序列转换为二值序列,定义转换函数  $T(x)$  为

$$T(x_n) = \begin{cases} 0, & x_n \in \bigcup_{d=1}^m B_{2d}^{2m} \\ 1, & x_n \in \bigcup_{d=1}^m B_{2d}^{2m} \end{cases} \quad (4)$$

其中,  $2m$  是正整数,  $B_0^{2m}, B_1^{2m}, B_2^{2m}, \dots, B_{2m}^{2m}$  是区间  $[0, 1]$  上的  $2m$  个等分区间。

针对 Logistic 映射所产生的初始离散伪随机序列,下面给出平衡伪随机序列生成的算法。

**步骤 1** 产生初始伪随机序列  $P$ 。首先给定初始值  $x_0$  和参数  $\mu$ ,由 Logistic 映射迭代产生离散伪随机序列  $\{x_n\}_1^{N_1}$ 。通过式(2)和式(3)得到长度为  $N_1$  的伪随机序列  $P = \{p_i | i=1, 2, \dots, N_1, p_i \in \{-1, 1\}\}$ 。

**步骤 2** 产生伪随机符号序列  $M$ 。 $P$  序列中相邻 3 位  $(p_i, p_{i+1}, p_{i+2})$  共有 8 种状态,将它们分别记为 'a', ..., 'h', 得到状态集  $A = \{a, b, c, d, e, f, g, h\}$ ,长度为  $N_1 - 1$  的伪随机序列  $M$ 。

**步骤 3** 产生复合符号序列  $Y$ 。用状态集  $B = \{-1, 1\}$  的任意 8 个有限序列  $\{B_i | i=1, \dots, 8\}$  替换  $M$  序列中 8 种状态,得到长度为  $N_2$  的序列  $Y$ 。

**步骤 4** 产生平衡伪随机序列  $S$ 。将  $Y$  序列中长度为  $d$  的子序列看作一个二进制实数,依次得到的  $N_2 - d + 1$  个实数构成时间序列  $Z$ ,再利用式(2)和式(3)得到长度为  $N_3 = N_2 - d + 1$  的二值伪随机序列  $S = \{s_i | s_i \in \{-1, 1\}\}_1^{N_3}$ ,再将  $S$  序列作为  $M$  序列返回步骤 2,直到序列长度符合要求,得到的平衡伪随机序列又称平衡复合符号序列。

## 3 自编码序列构造

自编码序列是采用线性滤波法从不断变化的信源序列中提取的一种伪随机序列,将其作为扩频码并用于扩频通信,能保证扩频码与传输信源信息紧密关联且随信源信息发生改变而改变,极大地提高了抗扩频码检测能力,保证了扩频序列的随机性、通信隐蔽性和低截获率,但是这种自编码扩频序列存在复杂性低、周期短的缺陷。根据谱估计理论,由高度相关的观测值组成的时间序列  $u(n)$ ,通过一系列统计独立的冲击激励函数为  $H(w)$  的线性滤波器产生,该冲击为零均值的高斯白噪声序列,记为  $v(n)$ 。针对自回归模型 (AR) 滤波模型,本文介绍自编码序列产生方法。定义  $P$  为 AR 滤波器的阶数,  $A(i) (i=1, 2, \dots, p)$  为滤波器的各阶参数,  $r(i) = E[u(n) * u(n+i)]$  是  $u(n)$  的相关函数,则 AR 滤波器参数与自相关函数之间的关系可用尤利-沃克方程表示如下:

$$\begin{pmatrix} r(0) & r(-1) & \dots & r(-p+1) \\ r(1) & r(0) & \dots & r(-p+2) \\ \vdots & \vdots & \ddots & \vdots \\ r(p-1) & r(p-2) & \dots & r(0) \end{pmatrix} \begin{pmatrix} A(1) \\ A(2) \\ \vdots \\ A(p) \end{pmatrix} = - \begin{pmatrix} r(1) \\ r(2) \\ \vdots \\ r(p) \end{pmatrix} \quad (5)$$

其中,  $R$  表示相关矩阵,  $A$  表示滤波器参数矩阵。假设自相关矩阵  $R$  可逆, 可得式(5)的解为

$$A = -R^{-1} \times r \quad (6)$$

由式(6)可知, 求出信源  $u(n)$  的相关矩阵  $A$ , 便可获得滤波器的各阶参数, 同时得到系统函数  $H(w)$ 。若信源  $u(n)$  输入系统函数为  $1/H(w)$  的反向 AR 滤波器, 则获得服从  $N(0, \sigma_v^2)$  分布的高斯白噪声序列  $v(n)$ 。由于  $v(n)$  取值连续, 将其二值离散化并得到称为自编码的扩频序列  $\{y(n) | n=0, 1, \dots\}$ , 其离散方法为  $y(n) = \begin{cases} -1, & v(n) \leq 0 \\ 1, & v(n) > 0 \end{cases}$ 。

基于 AR 模型的自编码扩频通信系统如图 1 所示。

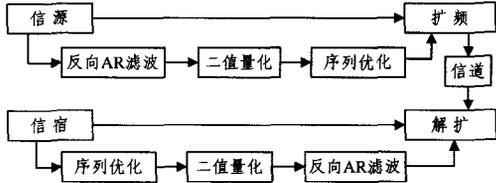


图 1 自编码扩频通信系统

## 4 复合扩频序列构造方法

为了构造性能优良的扩频序列, 本文将混沌映射所产生的高复杂性离散伪随机序列与自编码序列相融合, 获得一种具有两种不同离散序列优点的新序列, 以满足扩频通信需要。

### 4.1 离散二值随机序列融合原理

一般而言, 将两个二值离散随机序列融合为一个二值离散随机序列的典型方法有异或、同或等运算法, 这些方法已在传统密码学等领域得到广泛应用, 但由于具有拟线性运算特性, 抗差分攻击等的能力不足。为此, 本文探讨两个二值离散随机序列融合的新方法, 其原理描述如下:

首先将二值离散随机序列分割成长度为 8 的子块, 将每个子块转化为 0 至 255 的整数值。将两个二值离散随机序列所对应的整数序列作为二元非线性函数的输入, 其二元非线性函数的一个输出作为两个整数变量的融合输出结果, 另一个输出反馈到二元非线性函数的输入端, 并与其中一个输入整数值相加模 256 的余数作为二元非线性函数的一个输入变量。最后, 将二元非线性函数输出的整数序列通过二进制转化, 获得最终融合的二值离散随机序列, 将其作为扩频码应用扩频通信。

### 4.2 离散二值随机序列融合算法

为了满足二值离散随机序列的融合需要, 本文利用混沌理论中一种称为 Henon 映射的混沌函数, 将其离散所得的具有保面积且可逆的离散 Henon 映射作为非线性融合函数, 以解决现有二值序列异或、同或融合所存在的缺陷。为此, 下面首先介绍二维 Henon 映射及其离散方法。

#### 4.2.1 二维 Henon 映射

Henon 映射是二维非线性保面积且可逆的混沌映射函数, 相比一维 Logistic 映射具有良好的随机性、复杂度和非线性<sup>[16]</sup>。Henon 映射可描述为<sup>[21]</sup>

$$\begin{cases} x' = 1 + y - ax^2 \\ y' = bx \end{cases} \quad (7)$$

其中, 当参数  $a=1.4, b=0.3$  时, 该映射进入混沌状态。将二维连续 Henon 映射离散化处理, 获得有限域上的非线性表达

式为

$$\begin{cases} x_{n+1} = (1 - ax_n^2 + by_n) \bmod G \\ y_{n+1} = (cx_n) \bmod G \end{cases} \quad (8)$$

其中,  $a, b, c \in \{1, 2, \dots, G-1\}$  且  $\gcd(b, G)=1, \gcd(c, G)=1$ ,  $G$  是正整数。针对本文应用需要, 选取  $G=256$ 。利用式(8)可解决两个整数序列的非线性融合问题。

#### 4.2.2 离散二值随机序列融合算法

利用离散 Henon 映射实现两个二值离散随机序列融合时, 离散 Henon 映射参数  $b=c=1$ , 参数  $a$  是随融合过程发生变化的, 其具体值仍是利用 Logistic 混沌映射产生的。下面给出具体融合算法步骤。

假设融合的两个二值离散随机序列长度为  $N=8N_1$ , 这里  $N_1$  是正整数。两个二值离散随机序列分别为  $k_1(l), k_2(l)$  ( $l=1, 2, \dots, N$ ), 将其整数化处理为  $k_1^*(l), k_2^*(l) \in \{0, 1, \dots, G-1\}$  ( $l=1, 2, \dots, N_1$ )。

步骤 1 利用 Logistic 混沌映射产生长度为  $N_1$  的整数序列  $a_l \in \{1, 2, \dots, G-1\}$  ( $l=1, 2, \dots, N_1$ )。其详细过程为:

首先初始化 Logistic 映射  $x(0) \in (0, 1)$ , 选取混沌参数  $\mu \in (3.957, 4.0)$ , 重复迭代 Logistic 混沌映射 1000 次并将产生的值扔掉, 然后产生长度为  $N_1$  的实数序列  $x_n^*(l) \in (0, 1)$  ( $l=1, 2, \dots, N_1$ ), 将其整数化处理为

$$b^*(l) = \lfloor 255 \times x_n^*(l) \rfloor, l=1, 2, \dots, N_1 \quad (9)$$

最后, 将  $b^*(l)$  处理为

$$b_l = \begin{cases} b_l^*, & 0 < b_l^* < G \\ 1, & b_l^* = 0 \end{cases}, l=1, 2, \dots, N_1 \quad (10)$$

将序列  $b_l$  ( $l=1, 2, \dots, N_1$ ) 作为离散 Henon 映射融合两个整数随机序列时其参数  $b$  的动态取值。

步骤 2 两个整数化随机序列  $k_1^*(l), k_2^*(l)$  ( $l=1, 2, \dots, N_1$ ) 融合产生新的整数化随机序列  $z^*(l)$  ( $l=1, 2, \dots, N_1$ ) 的过程如下:

若  $l=1$ , 利用二维离散 Henon 映射产生融合值  $z^*(1)$  为

$$\begin{cases} z^*(1) = (1 - (k_1^*(1))^2 + b_1 \cdot k_2^*(1)) \bmod G \\ w^*(1) = k_1^*(1) \bmod G \end{cases} \quad (11)$$

否则, 利用二维离散 Henon 映射产生融合值  $z^*(l)$  ( $l=2, 3, \dots, N_1$ ) 为

$$\begin{cases} z^*(l) = (1 - (k_1^*(l))^2 + b_l \cdot g(k_2^*(l), w^*(l-1))) \bmod G \\ w^*(l) = k_1^*(l) \bmod G \end{cases} \quad (12)$$

$$l=2, 3, \dots, N_1$$

其中, 函数  $g(x, y) = (x + y) \bmod G$  或  $g(x, y) = x \oplus y$ , 实验测试时仅选择后者。

步骤 3 将融合所得整数序列  $z^*(l)$  ( $l=1, 2, \dots, N_1$ ) 进行二进制转化, 获得长度为  $N$  的二值离散伪随机序列, 将其用作扩频码实现扩频通信。

### 4.3 改进离散二值随机序列生成法

为了获得高性能的离散二值随机序列, 利用均匀映射  $U(x)$  和转换函数  $T(x)$  将 Logistic 混沌映射所产生的单位区间上实值序列转化为均匀序列后再离散化处理, 从而得到高质量的初始伪随机序列; 再与随机子序列复合后重复迭代, 从而得到长度随迭代次数呈几何级数增加的随机序列; 最后与自编码序列通过二维离散取模处理的 Henon 映射相融合产

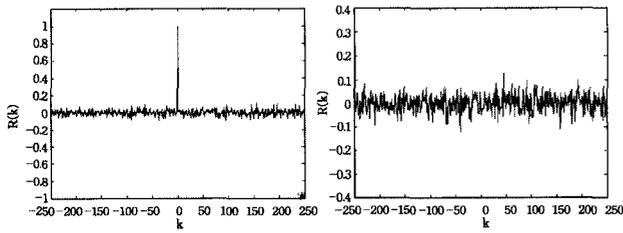
生改进的离散二值伪随机序列。

## 5 离散二值随机序列特性分析

为了能广泛应用本文所产生的离散二值随机序列作为扩频码实现扩频通信,需要对离散二值随机序列的相关性、随机复杂性等进行分析。

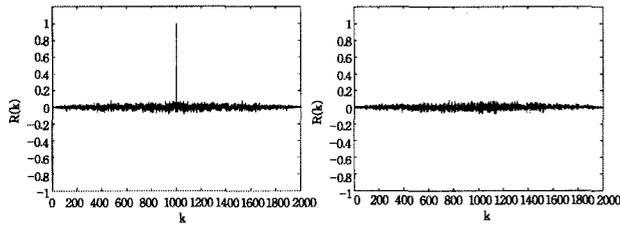
### 5.1 相关性分析

在扩频通信中,相关性是衡量扩频序列特性的一个重要技术指标,即扩频码序列相关性的好坏与扩频通信系统的抗多径干扰能力有着直接影响。本文对混沌映射所产生的随机序列、自编码序列,以及本文所产生的复合随机序列的相关性进行测试分析,结果如图 2—图 5 所示,图中的横轴  $k$  表示时延,纵轴  $R(k)$  表示相关性。



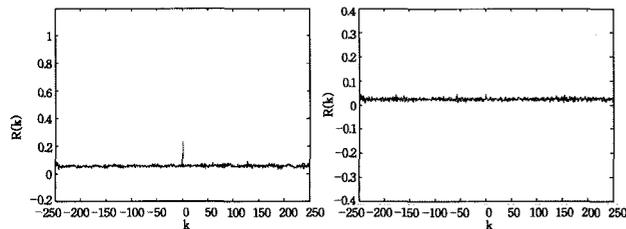
(a) 自相关性 (b) 互相关性

图 2 Logistic 映射产生随机序列的相关性



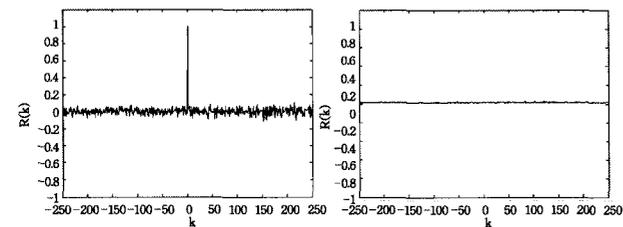
(a) 自相关性 (b) 互相关性

图 3 AR 自编码序列的相关性



(a) 自相关性 (b) 互相关性

图 4 离散二值随机序列的相关性



(a) 自相关性 (b) 互相关性

图 5 改进离散二值随机序列的相关性

从图 2—图 5 所示的 4 种随机序列的相关性测试来看,本文通过非线性融合方法构造的改进离散二值随机序列自相关峰非常尖锐,自相关函数类似  $\delta$  函数,具有白噪声性能,互

相关值非常小,几乎接近于零,相比其他序列有更好的相关性,这说明本文构造的随机序列作为扩频通信信息传输的扩频码是可行的。由相关性可知,改进的离散二值随机序列具有较强的抗干扰能力,有利于扩频通信系统信息的保密传输,满足强电磁环境下信息对抗通信的需要。

### 5.2 随机特性分析

二值随机序列的随机特性主要有平衡性、复杂性、初始值敏感性以及 Lyapunov 指数等。限于篇幅,本文重点分析平衡性和复杂性。

#### 5.2.1 平衡性

码平衡性是判断扩频序列安全性能的重要指标之一。良好的码平衡特性有利于防止高频载波泄露,保障通信系统的安全性。序列的平衡性由扩频序列中“0”和“1”的统计分布决定。设序列的长度为  $N$ ,序列中“0”和“1”的个数分别为  $P$  和  $Q$ ,则该序列的平衡度  $E$  定义为

$$E(N) = \frac{1}{N} |P - Q| \times 100\% \quad (13)$$

Logistic 混沌序列、自编码序列与本文所提多离散二值随机序列的平衡度  $E$  与序列长度  $N$  的关系,如表 1 所列。

表 1 不同随机序列的平衡度(%)

序列	序列长度					
	500	700	900	2000	3000	10000
Logistic	4.59	4.29	5.01	0.52	0.04	0.02
自编码	2.00	2.80	1.56	0.20	0.15	0.08
离散序列	1.60	0.78	0.00	0.08	0.00	0.03
改进序列	0.20	0.00	0.10	0.05	0.00	0.01

从表 1 可知,4 种随机序列长度越长,平衡性越好。一般而言,随机序列长度大于 2000 时,其序列能满足扩频通信的需要。另外,通过对比 4 种随机序列,发现本文构造的改进离散二值随机序列平衡性明显好于混沌序列和自编码序列的平衡性,表明改进离散二值随机序列具有良好的随机性,更进一步表明本文所建议的混沌序列和自编码相融合构造崭新随机序列的方法是有效的。

#### 5.2.2 复杂度

复杂度对提高扩频通信系统安全性具有重要意义,也是判断扩频序列安全性的重要指标之一。本文利用近似熵 (ApEn) 来分析混沌序列、自编码序列和新的随机序列的复杂度,因为信号经常会受到突发干扰而出现异常数据,而 ApEn 具有较好的鲁棒性,对实测信号的分析很有利。定义近似熵为

$$ApEn = \Phi^m(r) - \Phi^{m+1}(r) \\ = \langle \ln C_r^m(r) - \ln C_r^{m+1}(r) \rangle \quad (14)$$

其中,“ $\langle \rangle$ ”是对不同  $i$  求平均,  $C_r^m(r)$  表示以序列  $y(i)$  为中心,在窗口长度为  $m$ 、容许偏差为  $r$  时,其余矢量  $y(i)$  与  $y(j)$  的距离小于  $r$  的概率,  $\Phi^m(r)$  是矢量序列  $\{y(i)\}$  的平均自相关程度。分别计算不同长度时传统 Logistic 序列、自编码序列和本文所提出的新的随机序列的近似熵,结果如表 2 所列。

表 2 不同随机序列的近似熵比较

序列	序列长度					
	300	500	700	800	900	1000
Logistic	0.18	0.22	0.29	0.30	0.33	0.46
自编码	0.16	0.21	0.27	0.31	0.35	0.38
离散序列	0.81	0.98	1.05	1.11	1.15	1.18
改进序列	0.84	1.05	1.12	1.14	1.19	1.21

由表 2 可知, Logistic 混沌序列的复杂度高于自编码序列的, 而本文提出的非线性融合构造的离散二值随机的复杂度要远远高于混沌序列和自编码的复杂度, 这说明该方法构造的随机序列更有利于扩频通信系统信息的高安全保密传输。

## 6 扩频通信仿真分析

为了进一步验证本文建议的基于 Henon 映射将混沌序列与自编码序列相融合生成的离散二值随机序列作为扩频码所具有的良好特性, 将 Logistic 映射、自编码序列和本文构造的离散二值随机序列作为扩频码应用到多用户扩频通信系统并测试其误码率。

多用户扩频通信原理如图 6 所示。假设各用户同步, 且各用户信号功率相同。在发送端, 随机产生一个二进制信号作为信源。不同用户采用不同随机序列作为扩频码, 扩频后的数据通过脉冲成形滤波器加入到 AWGN 信道。在接收端, 不同用户将会接收到不同信号, 各个用户采用与发送端相同的扩频码作为解扩码对接收到的信号进行相关解扩。

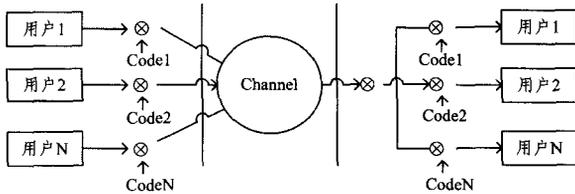


图 6 多用户扩频通信框图

针对高斯白噪声(AWGN)信道, 本文测试了不同扩频码通信时的误码率。实验测试采用信噪比的变化范围为  $E_b/N_0 = 0:2:20$ , 每种信噪比下发送符号数为  $n_{Symbol} = 1000$ , 脉冲成形滤波器的参数中升余弦滤波器时延为  $delay = 10$ , 滤波器过采样数  $F_s = 8$ , 升余弦滤波器滚降因子  $rolloff = 0.5$ 。下面将不同随机序列作为扩频码应用到多用户扩频系统, 其误码率测试结果如表 3 至表 7 所列。

表 3 Logistic 混沌序列的误码率

用户数	信噪比				
	2	4	6	8	10
1	0.1725	0.1670	0.1595	0.1590	0.1520
4	0.1785	0.1660	0.1665	0.1580	0.1490
7	0.1815	0.1730	0.1620	0.1650	0.1645

表 4 自编码序列的误码率

用户数	信噪比				
	2	4	6	8	10
1	0.1000	0.0450	0.0150	0.0100	0.0015
4	0.1238	0.0338	0.0175	0.0025	0.0013
7	0.1330	0.0735	0.0445	0.0205	0.0039

表 5 平衡伪随机符号序列的误码率

用户数	信噪比				
	2	4	6	8	10
1	0.0640	0.0250	0.0070	0.0033	0.0006
4	0.0853	0.0423	0.0201	0.0078	0.0033
7	0.0968	0.0560	0.0328	0.0188	0.0159

表 6 离散二值随机序列的误码率

用户数	信噪比				
	2	4	6	8	10
1	0.0465	0.0175	0.0035	0.0011	0.0003
4	0.0710	0.0371	0.0145	0.0059	0.0008
7	0.0944	0.0503	0.0316	0.0174	0.0099

表 7 改进离散二值随机序列的误码率

用户数	信噪比				
	2	4	6	8	10
1	0.0130	0.0060	0.0020	0.0010	0.0001
4	0.0374	0.0256	0.0156	0.0016	0.0005
7	0.0531	0.0328	0.0188	0.0048	0.0021

由表 3 至表 7, 对比分析不同随机序列作为扩频码的误码率, 发现本文所建议的融合法所产生的扩频码的误码率较低。详细分析信噪比和用户数对多用户扩频系统误码率的影响如下:

(1) 信道信噪比对系统误码率的影响: 当信噪比  $E_b/N_0$  取值在 2~10dB 变化时, 本文构造的改进离散二值随机序列在多用户系统的误码率明显低于其他扩频序列的误码率, 在用户数一定的情况下, 随着信噪比的增大, 其误码率逐渐降低, 特别是改进离散二值随机序列所对应的误码率降低得更显著, 能够满足多个用户的通信要求。

(2) 用户数对系统误码率的影响: 测试中用户数分别取 1、4、7, 当信噪比  $E_b/N_0$  一定时, 随着用户数的增加, 误码率增大。从整体上看, 本文所构造的改进离散二值随机序列的扩频系统误码率相对较低, 这说明该方法构造的扩频码性能更优越, 具有良好的抗多址干扰能力和较高的安全性, 并能获得较低误码率, 有效地解决了多用户通信中信道干扰问题, 更有利于高安全保密通信环境的需要。

**结束语** 随着扩频通信在军事作战指挥系统、无人机通信、导弹测速等方面的广泛应用, 提高其安全性和可靠性显得尤为重要。本文利用 Henon 映射将混沌随机序列和自编码序列相融合产生一种新的离散二值随机序列, 它同时具有现有两种随机序列的优势, 能满足信息对抗环境扩频通信的需要。仿真测试表明, 采用本文建议的非线性融合方法来构造高性能扩频码方法是可行的, 同时为扩频码的构造提供了一种崭新的思路。

## 参考文献

- [1] Dixon R C. 扩展频谱系统[M]. 王守仁, 等译. 北京: 国防工业出版社, 1982
- [2] Hill P C J, Ridley M E. Blind estimation of direct-sequence spread spectrum m-sequence chip codes[C]// 2000 IEEE Sixth International Symposium on Spread Spectrum Techniques and Applications. Parsippany, NJ, 2000: 305-309
- [3] Pursley M B, Sarwate D V. Performance evaluation for phased-coded spread-spectrum multiple access communication-Part 11: Code sequence analysis[J]. IEEE Trans. Communications, 1977, 25(8): 800-803
- [4] Jack K H. Spread Spectrum for GNSS and Wireless communications[M]. Beijing: Publishing House of Electronics Industry, 2013
- [5] Heidari-Bateni G, Mcgille C D. Chaotic sequences for spread spectrum: An alternative to PN-sequences[C]// Proceedings of the IEEE International Conference on Selected Topics in Wireless Communications. Vancouver, BC, 1992: 437-440
- [6] Kohda T, Tsuneda A. Even-and odd-correlation functions of chaotic Chebyshev bit sequences for CDMA[C]// Proceedings of the IEEE International Symposium on Spread Spectrum Techniques and Applications. Oulu, 1994: 391-395

(下转第 70 页)

- [3] 杨博,刘大, Liu Ji-ming, 等. 复杂网络聚类方法[J]. 软件学报, 2009, 20(1): 54-66
- [4] 程学旗, 沈华伟. 复杂网络的社区结构[J]. 复杂系统与复杂性科学, 2011, 8(1): 57-70
- [5] 樊鹏翼, 王晖, 姜志宏, 等. 微博网络测量研究[J]. 计算机研究与发展, 2012, 49(4): 691-699
- [6] 郭岩, 白硕, 杨志峰, 等. 网络日志规模分析和用户兴趣挖掘[J]. 计算机学报, 2005, 28(9): 1483-1496
- [7] Palla G, Derényi I, Farkas I, et al. Uncovering the overlapping community structure of complex networks in nature and society [J]. Nature, 2005, 435(7043): 814-818
- [8] 陈克寒, 韩盼盼, 吴健. 基于用户聚类的异构社交网络推荐算法[J]. 计算机学报, 2013, 36(2): 349-358
- [9] Gopalan P K, Blei D M. Efficient discovery of overlapping communities in massive network [J]. Proceedings of the National Academy of Science of the United States of American, 2013, 110(36): 14534-14539
- [10] Wainwright M J, Jordan M I. Graphical Models, Exponential Families, and Variational Inference [J]. Foundations and Trends in Machine Learning, 2008, 1(1/2): 1-305
- [11] Airoldi E M, Blei D M, Fienberg S E, et al. Mixed membership stochastic block models [J]. Journal of Machine Learning Research, 2008, 9: 1981-2014
- [12] Hoffman M, Blei D M, Wang Chong, et al. Stochastic variational inference [J]. Journal of Machine Learning Research, 2013, 14: 1303-1347
- [13] Hastings M B. Community detection as an inference problem [J]. Physical Review E-PHYS REV E, 2006, 74(3)
- [14] Gopalan P, Wang Chong, Blei D M. Modeling overlapping communities with node popularities [C] // Advances in Neural Information Processing Systems. 2013; 2850-2858
- [15] Danon L, Diaz-Guilera A, Duch J, et al. Comparing community structure identification [J]. Journal of Statistical Mechanics: Theory and Experiment, 2005(9): P09008
- [16] Blei D M, Ng A Y, Jordan M I. Latent dirichlet allocation [J]. Journal of Machine Learning Research, 2003, 3: 993-1022
- [17] 沈华伟, 程学旗, 陈海强, 等. 基于信息瓶颈的社区发现[J]. 计算机学报, 2008, 31(4): 677-686
- [18] Robbins H, Monro S. A stochastic approximation method [J]. The Annals of Mathematica Statistics, 1951, 22(3): 400-407
- [19] 杨楠, 弓丹志, 李饮, 等. Web 社区发现技术综述 [J]. 计算机研究与发展, 2005, 42(3): 439-447
- [20] 林友芳, 王天宇, 唐锐, 等. 一种有效的社会网络社区发现模型和算法 [J]. 计算机研究与发展, 2012, 49(2): 337-345
- [21] Gregory S. Find overlapping communities in networks by label propagation [J]. New Journal of Physics, 2010, 12(10): 103018
- [22] Yan B, Gregory S. Detecting community structure in network using edge prediction methods [J]. Journal of Statistical Mechanics: Theory and Experiment, 2012(9): P09008
- [23] Blondel V D, Guillaume J L, Lambiotte R, et al. Fast unfolding of communities in large network [J]. Journal of Statistical Mechanics: Theory and Experiment, 2008(9): P10008
- [24] He Dong-xiao, Liu Da-you, Zhang Wei-xiong, et al. Discovering link communities in complex networks by exploiting link dynamics [J]. Journal of Statistical Mechanics: Theory and Experiment, 2012(10): P10015

(上接第 46 页)

- [7] Wang H, Hu J D. Logistic-Map chaotic spread spectrum sequence [J]. ACTA Electronica Sinica, 1997, 25(1): 19-23
- [8] Jessa M. The period of sequences generated by tent-like maps [J]. IEEE Trans. Circuits Syst. I, Fundam. Theory Appl, 2002, 49(1): 84-88
- [9] Kurian A P, Puthussery S, Htut S M. Performance enhancement of DS/CDMA system using chaotic complex spreading Sequence [J]. IEEE Transactions on Wireless Communications, 2005, 4(3): 984-989
- [10] Youssef M I, Zahara M, Emam E. Chaotic Sequences Implementations on Residue Number Spread Spectrum System [J]. International Journal of communications, 2008, 2(2): 143-154
- [11] Ihan M, Philip, Andi S. Chaos Codes vs. Orthogonal Codes for CDMA [C] // ISSSTA 2010. Taichung, Taiwan, China, 2010: 189-193
- [12] 张薇, 谢红梅, 王保平. 一种新型的分段 Logistic 混沌扩频通信算法 [J]. 计算机科学, 2013, 40(1): 59-62
- [13] 王保平, 李文康, 吴成茂. 改进分段 Skew Tent 映射及其在扩频通信中应用 [J]. 红外与激光工程, 2013, 42(10): 2772-2777
- [14] Nazila R, Siamak T. Performance comparison of chaotic spreading sequences generated by two different classes of chaotic systems in a chaos-based direct sequence-code division multiple access system [J]. IET Communications, 2013, 10(7): 1024-1031
- [15] Zan L, C Jue-ping, C Yi-lin. Determining the Complexity of FH/SS Sequence by Approximate Entropy [J]. IEEE Transactions on Communications, 2009, 57(3): 812-820
- [16] 刘金梅, 丘水生. 混沌伪随机序列复杂性的一种量度方法 [J]. 计算机应用, 2009, 29(4): 938-941
- [17] Nguyen L. Self-encoded spread spectrum communications [C] // Proceedings IEEE MILCOM '99. Atlantic City, NJ, 1999: 182-186
- [18] Wei M, Li Z L, Yin F. Analysis and Simulation of AR-SESS System Performance [C] // 2005 International Conference on Communications, Circuits and Systems. Chengdu, China, 2005: 160-164
- [19] Duraisamy P, Nguyen L. Coded-sequence self-encoded spread spectrum communications [C] // Proceedings of the IEEE Global Telecommunications conference Hawaii. Honolulu, HI, 2009: 1-5
- [20] 王福来. 基于复合符号混沌的伪随机数生成器及加密技术 [J]. 物理学报, 2011, 60(11): 191-197
- [21] 张瀚, 王秀峰, 李朝晖, 等. 一种基于混沌系统及 Henon 映射的快速图像加密算法 [J]. 计算机研究与发展, 2005, 42(12): 2137-2142