doi:10.3772/j.issn.1002-0470.2014.11.006

基于分段 Logistic 和自编码的扩频码构造①

张晓蓉② 吴成茂③ 李文学

(西安邮电大学电子工程学院 西安 710121)
(解放军理工大学国防工程学院 南京 210007)

摘 要 针对现有随机序列用于扩频通信时可靠性和安全性差的情况,提出了将混沌映射与自编码相融合的扩频序列构造方法,以实现高动态通信条件下信息的可靠安全传输。该方法借鉴离散标准映射的构造思想,对二维 Henon 变换进行改进,并将分段 Logistic 混沌映射产生序列与 AR 自编码序列相融合产生高质量复合随机序列作为扩频码。以混沌和自编码为基础分析了该方法有效性、提高了序列的复杂度。仿真结果表明,与现有方法相比,该方法改善了序列的随机性,产生的扩频序列的抗干扰能力更好,并能获得较低的扩频误码率。

关键词 分段 Logistic 混沌映射, AR 自编码, Henon 变换, 扩频序列, 误码率

0 引 言

扩频技术是目前军事通信广泛采用的基本抗干扰技术体制,其关键是选取性能优良的扩频码序列。传统扩频通信采用 m 序列、Gold 序列以及改进的拟正交 Gold 序列等,文献[1,2]已证明它们具有良好的自相关性,但互相关性有较大的尖峰,码数量有限且周期短,容易被破译,系统保密性很差。为此,学者们研究了具有良好复杂性和随机性的各种混沌序列在扩频通信中的应用[3-7]。针对传统 Logistic 混沌扩频通信存在的不足,Martoyo 提出了正交 Logistic 混沌扩频码[8]构造法,它能极大改善混沌扩频通信系统的性能。由于单一混沌映射所产生的序列可利用非线性逆推法快速估计混沌参数,导致存在安全隐患,同时单一混沌映射的扩频系统抗干扰能力较弱,于是文献[9,10]提出了 Tent 映射和 Logistic 映射相结合的复合扩频码构造法,以及传统 m 序列和混沌随机序列相结合产生复合扩频序列的方法,它们极大地增强了系统抗破解能力。为了研究混沌序列的性能对扩频通信的影响,学者们研究了混沌序列的复杂性、随机性、安全性等[11-13],研究表明混沌序列可满足扩频通信的需要。近十多年来,自编码[14]成为扩频序列的重要构造方法,已在直扩和跳频通信系统中得到成功应用[15,16]。文献[17-19]的研究表明自编码序列具有良好的相关特性、游程特性、平衡性和线性复杂度,正逐渐被大量扩频通信系统采用。文献[20]把基于自回归(auto-regression, AR)滤波器提取的自编码扩频技术应用于卫星测控通信中,表明该随机序列能够满足卫星扩频测控通信的要求,能降低传输信号的截获率,提高通信的隐蔽性和安全性。但是,自编码扩频序列本身存在复杂性低的缺陷还未引起学者们的重视。为了进一步完善自编码扩频通信系统的安全性和可靠性,本文采用了标准映射的构造思想对二维 Henon 变换进行改进,并通过它将分段 Logistic 映射产生的混沌序列与 AR 自编码序列相融合获得一种新的复合序列作为扩频码,它兼有混沌序列的高复杂性、随机性和 AR 自编码序列良好的相关性、平衡性和信源关联性,满足了高安全性要求的信息对抗环境扩频通信需要。通过多用户扩频通信系统仿真测试表明,本文所提出的复合扩频码构造法是有效的,其相关性、随机性和复杂性等都得到了一定程度改善,同时其传输误码率相比现有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。

① 国家自然科学基金(61136002, 61073106),陕西省自然科学基金(2014JM8331, 2014JQ5183, 2014JM8307)和陕西省教育厅自然科学资金(2013JK1129)资助项目。
② 女,1989 年生,硕士;研究方向:扩频通信技术等; E-mail: 971401590@qq.com
③ 通信作者,E-mail: wuchengmao123@sohu.com
(收稿日期:2014-05-22)

1 混沌序列构造

混沌是非线性确定系统由于内在随机性而产生的外在复杂表现,是一种特殊的动力学系统。混沌序列由于具有优良的特性已经应用于航空航天、信息处理、模糊和神经网络的融合等。近多年来,混沌理论在图像加密、信息安全、通信保密等方面得到广泛应用[21,22],尤其是当前的混沌通信已受到广大学者的重视。本文重点探讨分段 Logistic 混沌映射用于构造复合离散随机序列的方法。

1.1 Logistic 映射

Logistic 映射是在实际系统中存在的最简单的非线性差分方程,是一个被广泛研究的动态系统。它所产生的序列具有非周期、非收敛等特点,对初始值极为敏感。Logistic 映射由于其表达式简单、随机性能良好,因而被广泛应用于混沌保密通信的各个领域。该映射描述为[23]

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

其中μ是映射参数,若 $3.569946 \leqslant \mu \leqslant 4$ 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。

1.2 分段 Logistic 混沌映射

由于 Logistic 混沌映射的控制参数取值范围小,其混沌特性较弱,并不完全适合扩频通信信息传输的需要。针对 Logistic 混沌映射的缺点,文献[24]提出了分段 Logistic 混沌映射。其中第一种分段 Logistic 混沌映射描述为

$$a_{n+1} = \begin{cases} 4\mu a_n(0.5 - a_n), & 0 \leqslant a_n \leqslant 0.5 \\ 4\mu(a_n - 0.5)(1 - a_n), & 0.5 \leqslant a_n \leqslant 1 \end{cases} \tag{2}$$

其中μ是映射参数,若 $3.569946 \leqslant \mu \leqslant 4$ 时,该映射进入混沌状态,$a_0 \in (0,1)$。当$\mu = 4$时为满映射。

第一种分段 Logistic 映射曲线关于 x 坐标轴在 0.5 处具有对称性,不利于产生离散二值序列 0、1 个数均衡性需要。于是,提出了第二种分段 Logistic 映射,具体描述为

$$a_{n+1} = \begin{cases} 4\mu a_n(0.5 - a_n), & 0 \leqslant a_n \leqslant 0.5 \\ 1 - 4\mu(a_n - 0.5)(1 - a_n), & 0.5 \leqslant a_n \leqslant 1 \end{cases} \tag{3}$$

其中μ是映射参数,若 $3.569946 \leqslant \mu \leqslant 4$ 时,此映射进入混沌状态,$a_0 \in (0,1)$。当$\mu = 4$时为满映射。本文利用它产生初始离散伪随机序列,其方法如下

$$x_n^* = \begin{cases} 1, & x_n > 0.5 \\ 0, & x_n \leqslant 0.5 \end{cases}, \quad n = 0,1,\cdots \tag{4}$$

其中,x_n^* 表示离散随机序列。

2 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(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,$A(i)(i = 1,2,\cdots,p)$ 为滤波器的各阶参数,$r(i) = E[u(n) \times u(n+i)]$ 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-沃克方程表示为

$$\begin{pmatrix} r(0) & r(-1) & \cdots & r(-p+1) \\ r(1) & r(0) & \cdots & r(-p+2) \\ \vdots & \vdots & \vdots & \vdots \\ r(p-1) & r(p-2) & \cdots & r(0) \end{pmatrix} \begin{pmatrix} A(1) \\ A(2) \\ \vdots \\ A(P) \end{pmatrix} = - \begin{pmatrix} r(1) \\ r(2) \\ \vdots \\ r(p) \end{pmatrix} \tag{5}$$

$R = r(i)$ $(i = 1,2,\cdots,p)$ 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,可得方程式(4)的解为

$$A = - R^{-1} \times r \tag{6}$$

由式(6)可知,求出信源 $u(n)$ 的相关矩阵 A,便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,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 $\{y(n) \mid n = 0,1,\cdots\}$,其离散方法为 $y(n) = \begin{cases} -1, & v(n) \leqslant 0 \\ 1, & v(n) > 0 \end{cases}$。

3 复合随机序列构造方法

为了构造性能优良的扩频序列,本文针对 Logistic 混沌映射的控制参数取值范围小,其混沌特性

较弱,提出将分段 Logistic 映射所产生的混沌随机序列与线性滤波法产生的 AR 自编码随机序列通过改进离散 Henon 变换相融合,获得一种兼有两种随机序列优点的新复合随机序列。

3.1 复合随机序列融合原理

一般而言,将两个离散随机序列融合为一个离散随机序列的典型方法有异或、同或等运算法,但这些方法已在传统密码学等领域得到广泛应用。由于异或、同或运算具有拟线性运算特性,缺乏抗差分攻击等能力,为此,本文探讨了两个离散随机序列融合新方法,其融合原理框图如图 1 所示。其原理分析如下:

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。然后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并获得最终融合的二值离散随机序列,将其作为扩频码应用于扩频通信。

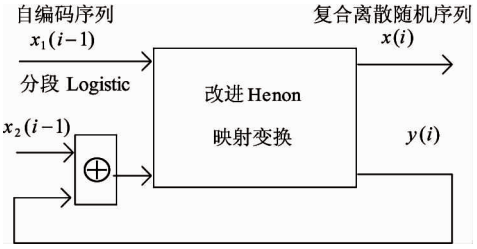

图 1 融合原理框图

3.2 复合随机序列融合算法

为了实现二值离散随机序列的融合需要,本文利用混沌理论中一种二维非线性保面积且可逆的 Henon 混沌映射函数,它较低维混沌映射具有良好的随机性、复杂性等,对其进一步改进后作为非线性融合函数,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 变换,其次提出二维 Henon 变换改进方法。

3.2.1 二维 Henon 变换及其改进

为了提高扩频通信信息传输的安全性和可靠性,本文利用了离散标准映射[25,26]的构造思想,将二维 Henon 映射进行改进。首先,标准映射为

$$\begin{aligned} s_1(x,y) &= (x+y)\bmod 2\pi \\ s_2(x,y) &= (y-k\sin(x+y))\bmod 2\pi \end{aligned} \tag{7}$$

其中 k 为一正常数,易将表达式推广为一般形式为

$$\begin{aligned} s_1(x,y) &= (x+f(y))\bmod 2\pi \\ s_2(x,y) &= (y-g(s_1))\bmod 2\pi \end{aligned} \tag{8}$$

为了满足扩频通信信息安全保密的传输,可将表达式(8)离散为

$$\begin{aligned} x_{n+1} &= (x_n+f(y_n))\bmod N \\ y_{n+1} &= (y_n-g(x_{n+1}))\bmod N \end{aligned} \tag{9}$$

二维 Henon 变换可描述为[26]

$$\begin{cases} x_{n+1} = 1-ax_n^2+by_n \\ y_{n+1} = cx_n \end{cases} \tag{10}$$

其中 a,b,c 为系统参数。当 $a=1.4$, $b=1$, $c=0.3$ 时,系统(式(10))处于混沌状态,且当 $c=1$ 时,系统在运动中保持相平面积不变。

本文利用以上离散标准映射的构造思想来改进二维 Henon 变换(式(10)),将二维连续 Henon 映射离散化并进行改进,得到表达式为

$$\begin{cases} x_{n+1} = (1-ax_n^2+by_n)\bmod N \\ y_{n+1} = (cx_n+x_{n+1}^2)\bmod N \end{cases} \tag{11}$$

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

3.2.2 复合离散随机序列融合算法

利用改进离散 Henon 映射实现两个二值离散随机序列融合时,其中改进离散 Henon 映射参数 $b=c=1$,参数 a 是随融合过程发生变化的,其具体值是利用分段 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 $k_1(l)$, $k_2(l)(l=1,2,\cdots,N)$,将其整数化处理为 $k_1^*(l)$, $k_2^*(l)\in\{0,1,\cdots,N-1\}(l=1,2,\cdots,N_1)$。

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

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

$$b^*(l)=\lfloor 255\times x_b^*(l)\rfloor,\ l=1,2,\cdots,N_1 \tag{12}$$

最后,对 $b^*(l)$ 处理为

$$b_l = \begin{cases} b_l^*, & 0 < b_l^* < G \\ 1, & b_l^* = 0 \end{cases}, \ l = 1,2,\cdots,N_1 \tag{13}$$

将序列 $b_l(l = 1,2,\cdots,N_1)$ 作为改进后离散 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 $k_1^*(l)$，$k_2^*(l)$ $(l = 1,2,\cdots,N_1)$ 融合产生新的整数化随机序列 $z^*(l)$ $(l = 1,2,\cdots,N_1)$，过程如下：

若 $l = 1$ 时，利用改进离散 Henon 映射产生融合值 $z^*(1)$ 为

$$\begin{cases} z^*(1) = (1 - (k_1^*(1))^2 + b_1 \cdot k_2^*(1)) \bmod N \\ w^*(1) = (k_1^*(1) + z^*(1)^2) \bmod N \end{cases} \tag{14}$$

否则，利用改进离散 Henon 映射产生融合值 $z^*(l)$ $(l = 2,3,\cdots,N_1)$ 为

$$\begin{cases} z^*(l) = (1 - (k_1^*(l))^2 \\ \qquad + b_l \cdot g(k_2^*(l), w^*(l-1))) \bmod N \\ w^*(l) = (k_1^*(l) + z^*(l)^2) \bmod N \end{cases} \quad l = 2,3,\cdots,N_1 \tag{15}$$

其中函数 $g(x,y) = (x + y) \bmod N$ 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 $z^*(l)(l = 1,2,\cdots,N_1)$ 进行二进制转化并获得长度为 N 的复合离散伪随机序列，将其用作扩频码实现扩频通信。

4 复合随机序列特性分析

为了广泛应用本文所产生的复合随机序列作为扩频码实现扩频通信，需要对复合随机序列的相关性、随机复杂性等进行分析。

4.1 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随机序列、自编码序列，以及本文所产生复合随机序列的相关性进行测试分析，其图示中的横轴 k 表示时延，纵轴 $R(k)$ 表示相关性（图 2 ~ 图 7）。

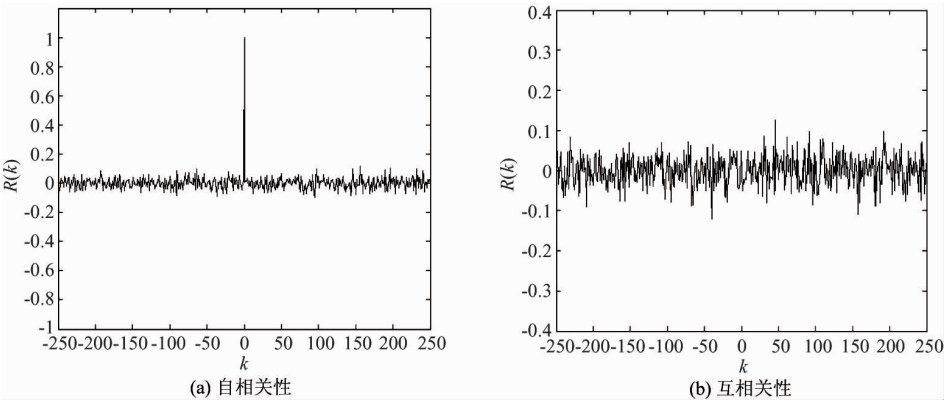

图 2 Logistic 映射产生随机序列相关性

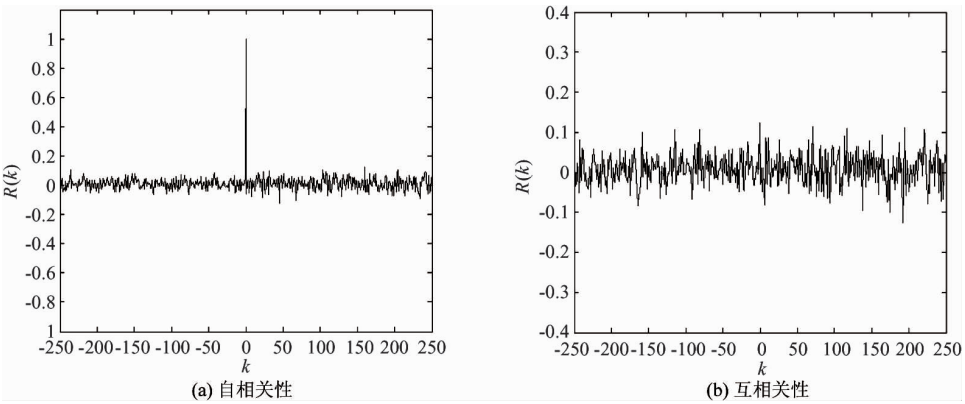

图 3 第一种分段 Logistic 混沌序列相关性

从图 2 至图 7 所示的 6 种随机序列的相关性测试来看,本文通过改进方法构造的复合离散随机序列自相关峰非常尖锐,自相关函数类似 δ 函数,具有白噪声性能,互相关值非常小,几乎接近于零,相比现有随机序列相关性得到了明显改善。说明本文构造的复合离散随机序列作为扩频通信信息传输的扩频码是可行的,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,满足复杂的强电磁环境下信息对抗通信的需要。

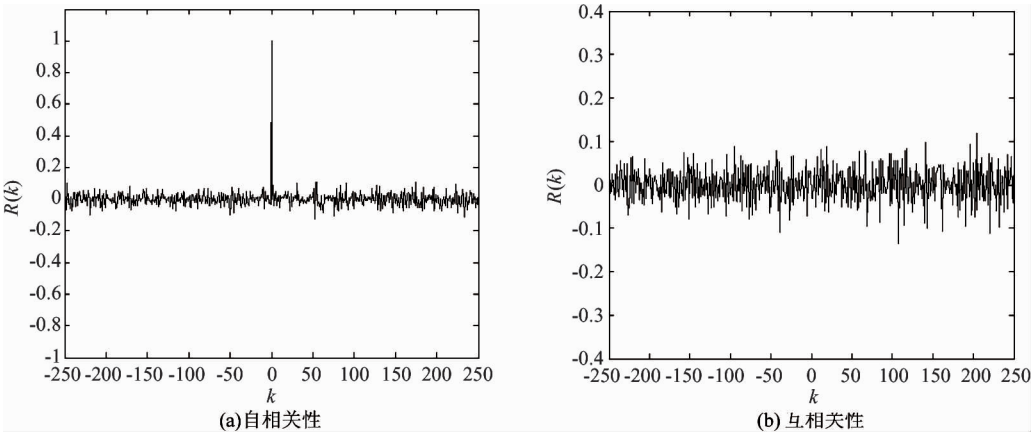

图 4　第二种分段 Logistic 混沌序列相关性

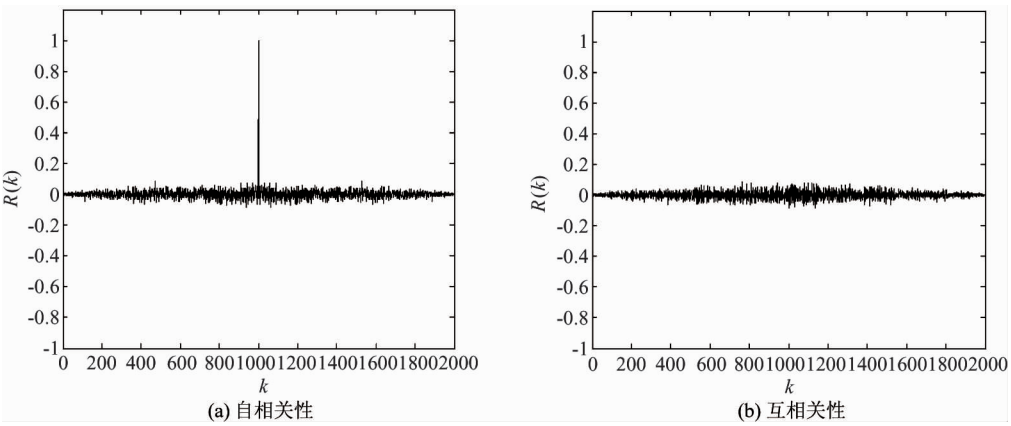

图 5　AR 自编码序列的相关性

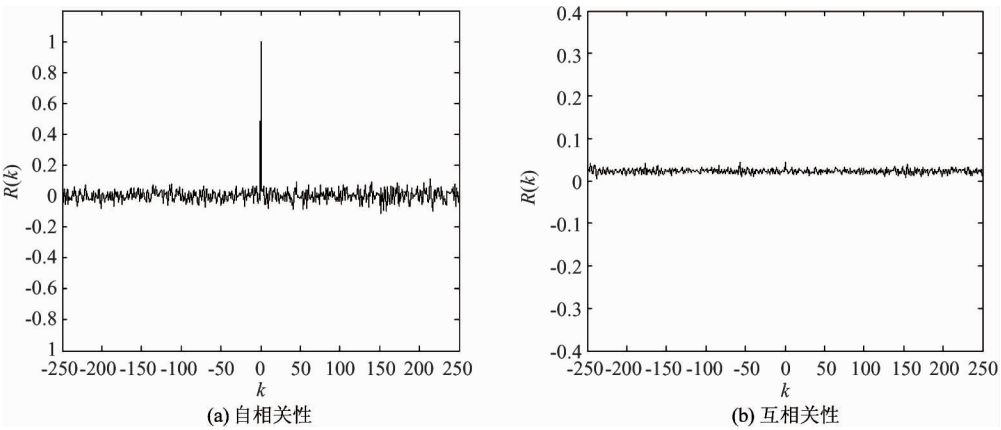

图 6　复合随机序列 1 的相关性

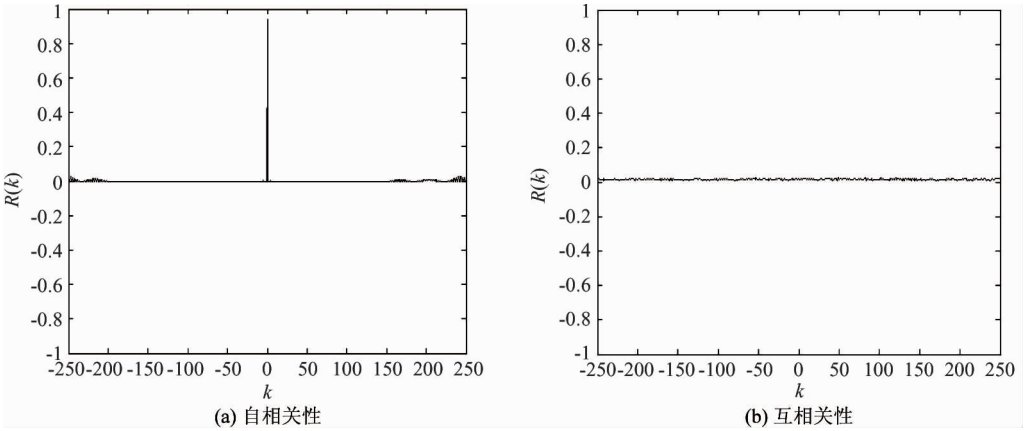

图 7 复合随机序列 2 的相关性

4.2 随机特性分析

二值离散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,本文重点分析其平衡性和复杂性。

4.2.1 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,保障通信系统安全性。序列的平衡性是由扩频序列中"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 N, 则该序列的平衡度 E 定义为

$$E(N) = \frac{1}{N} | P - Q | \times 100\% \tag{16}$$

下面测试不同离散随机序列的平衡度 E 与序列长度 N 关系。如表 1 所示。

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
第一种分段	4.85	4.63	4.95	1.20	0.18	0.12
第二种分段	4.36	4.21	4.32	0.32	0.03	0.02
自编码序列	2.00	2.80	1.56	0.20	0.15	0.08
复合序列 1	1.60	0.78	0.00	0.08	0.00	0.03
复合序列 2	0.16	0.00	0.08	0.02	0.00	0.01

从表 1 可知,以上随机序列的长度越长,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,通过对比以上随机序列发现,自编码序列的平衡性明显优于混沌序列。第一种分段 Logistic 混沌序列的平衡性较 Logistic 混沌序列的平衡性差,说明它的随机性相对较差,第二种分段 Logistic 混沌序列的随机性相对较好。而本文构造的复合离散随机序列平衡性得到了极大的改善,且复合随机序列 2 相对复合随机序列 1 平衡性更好,表明复合离散随机序列 2 具有相对良好的随机性,进一步表明本文所建议的复合随机序列的构造方法是有效的。

4.2.2 复杂度

复杂度对提高扩频通信系统安全性具有重要意义,它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)来分析不同随机序列的复杂度。由于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

$$\begin{aligned} ApEn &= \Phi^m(r) - \Phi^{m+1}(r) \\ &= \langle \ln C_i^m(r) - \ln C_i^{m+1}(r) \rangle \end{aligned} \tag{17}$$

其中"〈〉"是对不同 i 求平均, $C_i^m(r)$ 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 $\{y(i)\}$ 平均自相关程度。分别计算不同长度时,不同随机序列的近似熵。计算结果如表 2所示。

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
第一种分段	0.21	0.23	0.34	0.38	0.42	0.51
第二种分段	0.34	0.39	0.42	0.48	0.52	0.59
自编码序列	0.16	0.21	0.27	0.31	0.35	0.38
复合序列 1	0.81	0.98	1.05	1.11	1.15	1.18
复合序列 2	0.86	1.08	1.16	1.18	1.21	1.23

由表 2 可知,混沌序列的复杂度高于自编码序列的,这与理论上的混沌系统是一种非线性系统具有极高的复杂度基本吻合。其中分段 Logistic 混沌序列的复杂度相对于 Logistic 混沌序列的复杂度明显得到了改进,为本文构造的复合离散随机序列的方法提供了依据。从表中可看出本文提出的非线性融合构造的复合离散随机的复杂度要远远高于混沌序列和自编码的复杂度,说明了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。

5 扩频通信仿真分析

为了进一步验证本文建议的方法所产生的复合离散随机序列作为扩频码所具有的良好特性,本文在加性高斯白噪声(AWGN)信道下,仿真不同扩频码序列通信时的误码率。实验仿真采用信噪比的变化范围为 $Eb/No = 2:2:20$,每种信噪比下发送符号数为 $nSymbol = 1000$,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 $Fs = 8$,升余弦滤波器滚降因子 $rolloff = 0.5$。首先通过蒙特卡罗仿真模型对不同随机序列作为扩频码在扩频通信系统中测试信噪比、用户数与误码率的关系如图 8 和图 9 所示。

图 8 中在用户数为 4 一定的情况下,选取序列长度为 1000 时,将现有扩频序列和本文所构造的扩频码序列分别应用于扩频通信系统中相应的误码率曲线。可以看出,不同扩频序列的误码率随着信噪比的增大逐渐变小,这是由于随着信噪比的增大,系统多址干扰成为影响系统性能的关键因素,而本文

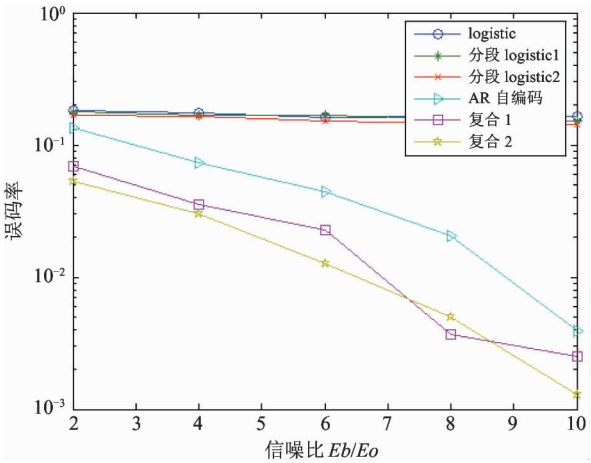

图 8 误码率与信噪比的关系

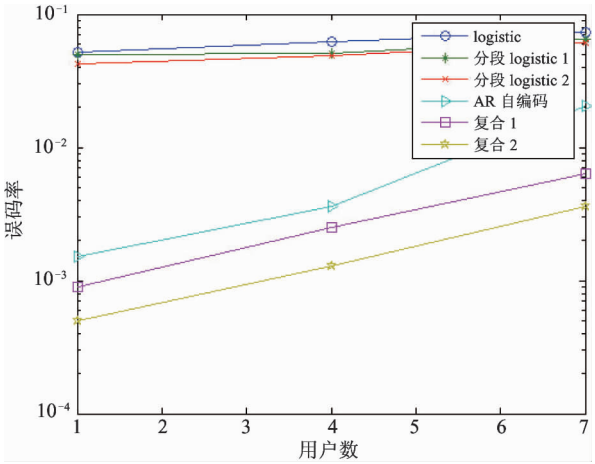

图 9 误码率与用户数的关系

方法所构造的扩频序列在相同信噪比下的误码率比现有方法构造的扩频序列的误码率要小,因此,本文所提的这种扩频序列的抗多径干扰性能更好。

由图 9 可看出,在信噪比一定时,不同扩频序列的误码率都会随用户数增多而升高,但相比而言,本文所提的新扩频序列的误码率明显小于现有扩频序列,也就是说这种新扩频序列可以承载的用户数目更多。说明了该方法构造的扩频序列的性能更优越,具有良好的抗多址干扰能力和较高的安全性,并能获得较低的误码率,有效地解决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。

6 结 论

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,提高通信的安全性和可靠性显得尤为重要。本文引用标准映射的思想对 Henon 变换进行改进,并利用它将分段 Logistic 混沌随机序列和 AR 自编码序列相融合产生一种新的复合离散随机序列。此方法产生的复合序列兼有两种随机序列的优势,并与现有构造方法相比,该方法对随机序列的性能得到了极大的改善,提高了随机序列的复杂性和随机性,同时相比现有扩频码其传输误码率也有了显著降低,更有利于高动态通信条件下信息可靠安全传输。

参考文献

[1] Hill P C J, Ridley M E. Blind estimation of direct-sequence spread spectrum m sequence chip codes. In: Proceeings of 2000 IEEE Sixth International Symposium on Spread Sprectrum Techniques and Applications, Parsip-

pany, USA, 2000. 305-309

[2] Pursley M B, Sarwate D V. Performance evaluation for phased-coded spread spectrum multiple access communication-Part 11: Code sequence analysis. *IEEE Trans Communications*, 1977, 25 (8):800-803

[3] 余金峰, 杨文革, 路伟涛等. 满映射 Logistic 数字混沌序列的产生及性能分析. 电讯技术, 2013,53(2):140-145

[4] Kohda T, Tsuneda A. Even- and odd-correlation functions of chaotic Chebyshev bit sequences for CDMA. In: Proceedings of the IEEE Internation Symposium on Spread Spectrum Techniques and Applications, Oulu, Finland, 1994. 391-395

[5] Jessa M. The period of sequences generated by tent-like maps. *IEEE trans Circuits syst I, Fun- dam Teory appl*, 2002, 49(1):84-88

[6] 张薇, 谢红梅, 王保平. 一种新型的分段 Logistic 混沌扩频通信算法. 计算机科学, 2013,40(1):59-62

[7] 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. 红外与激光工程, 2013,42(10):2772-2777

[8] Ihan M, Philip, Andi S. Chaos codes vs. orthogonal codes for CDMA. In: Proceedings of the ISSSTA 2010, Taichung, Taiwan, China, 2010. 189-193

[9] Wei P C, Zhang W, Yang H Q. A novel chaotic stream cryptographic algorithm based on Henon map and m-sequences. *Computer Science*, 2005,32(6):69-72

[10] 易新兵, 易凯. 复合混沌码的直扩系统优化及抗干扰性能研究. 计算机工程与设计, 2012,33(10):3715-3719

[11] 罗松江, 丘水生, 陈旭. 一种混沌伪随机序列复杂度分析方法. 华南理大学学报, 2010,38(1):18-21

[12] 王光义, 袁方. 级联混沌及其动力学特性研究. 物理学报, 2013,62(2):1-9

[13] Li Z, Cai J P, Chang Y. Determining the complexity of FH/SS sequence by approximate entropy. *IEEE Transactions on Communications*, 2009,57(3):812-820

[14] Nguyen L. Self-encoded spread spectrum communications. In: Proceedings of the IEEE Military Communications Conference, Atlantic City, USA, 1999. 182-186

[15] Yin F, Li Z L. A new method to produce SESS codes with the algorithm of estimation of PSD. In: Proceedings of the 2004 International Conference on Communication, Circuits and Systems, Chendu, China, 2004. 117-120

[16] Stephen F F, Lim N. Self-encoded spread spectrum communications with FH-MFSK. In: Proceedings of 2010 Second International Conference on Advances in Satellite and Space Communications, Athens, Greece, 2010. 82-89

[17] 魏梅, 李仲令. AR 自编码扩频系统中扩频序列的特性研究. 电子与信息学报, 2007,29(2):291-294

[18] Wei M, Li Z L, Yin F. Analysis and simulation of AR-SESS system performance. In: Proceedings of the 2005 International Conference on Communications Circuits and Systems, Chengdu, China, 2005. 160-164

[19] Duraisamy P, Nguyen L D. Perormance of self-encoded spread spectrum under pulsed-noise jamming. In: Proceedings of 2010 IEEE 11th International Symposium on Spread Spectrum Techniques and Applications, Taichung, Taiwan, China, 2010. 170-174

[20] 刘辉峰. 基于 AR 自编码扩频的卫星测控通信技术. 通信技术, 2008, (8):57-59

[21] Alvarez G, Montoya F, Romera M, et al. Breaking two secure communication systems based on chaotic masking. *IEEE transactions on circuits and systems-II*, 2004, 51(10):505-506

[22] Zhang H, Wang X F. A new image encryption algorithm based on chaos system. In: Proceedings of the International Conference on Robotics, Intelligent Systems and Signtal Processing, Chang-sha, China, 2003. 778-782

[23] 范九伦, 张雪峰. 分段 Logistic 混沌映像及其性能分析. 电子学报, 2009,29(7):720-725

[24] 刘金梅, 丘水生. 混沌伪随机序列复杂性的一种量度方法. 计算机应用, 2009,29(4):938-941

[25] 李昌刚, 韩正之, 张浩然. 一种基于随机密钥及"类标准映射"的图像加密算法. 计算机学报, 2003,26(4):465-470

[26] 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. 计算机研究与发展, 2005,42(12):2137-2142

Construction of spread-spectrum codes based on piecewise logistic and self-coded

Zhang Xiaorong, Wu Chengmao, Li Wenxue
(School of Electronic Engineering, Xi'an University of Posts and Telecommunications, Xi'an 710121)
(National Defense College of Engineering, PLA University of Science and Technology, Nanjing 210007)

Abstract

The poor communication reliability and safety of the existing random sequence when it is used in spread spectrum communication are paid attention, and a method for construction of spread spectrum sequences by combining chaotic maps with self-coded codes is proposed to achieve information's reliable and secure transmission under high-dynamic communication conditions. This method uses the constructing thought of discrete standard mapping to improve the two-dimensional Henon transform, and combines the sequence generating a sequence piecewise logistic chaotic map with the self-coded sequence to generate a high quality composite random sequence as the spreading code. The effectiveness of the method is analyzed based on Chaos and self-coded. The simulation results show that compared with the existing method, the proposed method improves the randomness of the sequence and increases the complexity of the sequence, and the generated spread spectrum sequece has the better anti-jamming capability and a lower spread bit error rate.

Key words: piecewise logistic chaotic map, AR self-coded, Henon transform, spread spectrum sequence, bit error rate