改进型 Hénon 映射生成混沌伪随机序列及性能分析*

李家标† 曾以成 陈仕必 陈家胜

(湘潭大学光电工程系智能光电技术研究所, 湘潭 411105)

(2010 年 8 月 19 日收到;2010 年 9 月 17 日收到修改稿)

提出一种改进传统 Hénon 映射的方法. 该方法通过引入绝对值项改变映射系统的内部结构,大大提高了映射系统的线性复杂度和初值敏感性. 利用混沌系统生成伪随机序列,进一步对比分析了映射系统生成的伪随机序列的性能. 理论分析和实验仿真表明,改进后的映射系统比原系统生成的序列质量有很大提高,验证了该方法的有效性.

关键词: Hénon 映射, 伪随机序列, 性能分析

PACS: 05.45.Ac, 05.45.Pq, 05.45.Vx

1. 引 言

扩频通信具有抗干扰、抗多径等优越性,而良好随机性和相关特性的扩频序列在其中起着决定性作用[1]. m 序列和 Gold 序列等往往存在可用码组数目少以及序列复杂度低等不足[1],因此设计容量大,相关性好,安全性强的扩频序列仍然是扩频通信的重要研究问题.

混沌信号有伪随机性,宽带白谱和存在不变分布等性质,利用混沌序列作为扩频码,是一个新的研究方向. 混沌信号在通信中的应用,研究工作主要集中在连续混沌信号上,系统实现可用模拟电路来完成,特点是它对电路固有参数以及误差很敏感,容易导致发送端和接收端信号不匹配和通信的保密性下降. 离散混沌系统所产生的时间序列同样适用于通信中,混沌序列数目大,又互不相关,满足扩频多址通信中对扩频序列码的要求,电路实现更方便[2]. 1990 年,Habutsu 等给出了一种基于线性的 Tent 映射的混沌加密系统;1994 年, Biance 利用 Logistic 映射产生实数序列,该序列被转换成二值序列用作扩频序列. Hénon 映射是一个二次方型二维混沌映射,相对于一维混沌系统具有更高的线性复杂度. 文献[3,4]研究了 Hénon 映射的参数分布及其在扩频通信中的应用,表明了 Hénon 映射在扩频通信中的应用价值. 2002 年 Richter 设计了理论上可无限维的广义 Hénon 映射[5],优点是系统复杂度相比 Hénon 映射有所提高,但系统生成的序列的随机性不是很理想.

为提高混沌扩频序列的质量,常见的解决方案是应用不同的混沌系统进行多重迭代[6—8],这样做提高了系统的安全性,但增加了计算量,降低了效率. 既能提高系统的安全性,又能保证效率,提高混沌系统的线性复杂度是一种途径. 本文在传统 Hénon 映射的基础上提出一种改进型 Hénon 映射,即在原系统中引入绝对值项,系统的复杂性和随机性都得到了较好的改善,由改进后混沌系统产生的二值序列各项性能较好,是一类实用的扩频序列.

2. 改进型 Hénon 映射及特性分析

Hénon 映射的方程为

$$\begin{aligned} x_{n+1} &= -ax_n^2 + y_n + 1, \\ y_{n+1} &= bx_n. \end{aligned} \tag{1}$$

参数 $a = 1.4$, $b = 0.3$ 时,系统有最大 Lyapunov 指数. 为了提高混沌系统的复杂性、初值敏感性,引

* 国家自然科学基金(批准号: 60972147)资助的课题.

† E-mail: lijiabiao_2008yahoo.cn

入绝对值项来改变系统的内部结构,得到如下映射

$$\begin{aligned} x_{n+1} &= -ax_n^2 + |y_n| + 1, \\ y_{n+1} &= bx_n. \end{aligned} \tag{2}$$

参数仍然设为 $a = 1.4, b = 0.3$. 我们把这种新的混沌映射称作 New-Hénon 映射系统,把原映射系统称作 Old-Hénon. 下面对新旧映射的特性做一个对比分析.

2.1. 分岔图

图 1(a)是 Old-Hénon 映射系统随参数 a 变化的分岔图($a \in [0, 1.4], b = 0.3$). 图 1(b)是 New-Hénon 映射系统随参数 a 变化的分岔图($a \in [0, 1.4], b = 0.3$). 可以看出,New-Hénon 映射系统同样随参数 a 呈现倍周期分岔,且比 Old-Hénon 映射更早进入混沌状态,且周期窗口不明显,可避免落入周期窗口产生周期序列.

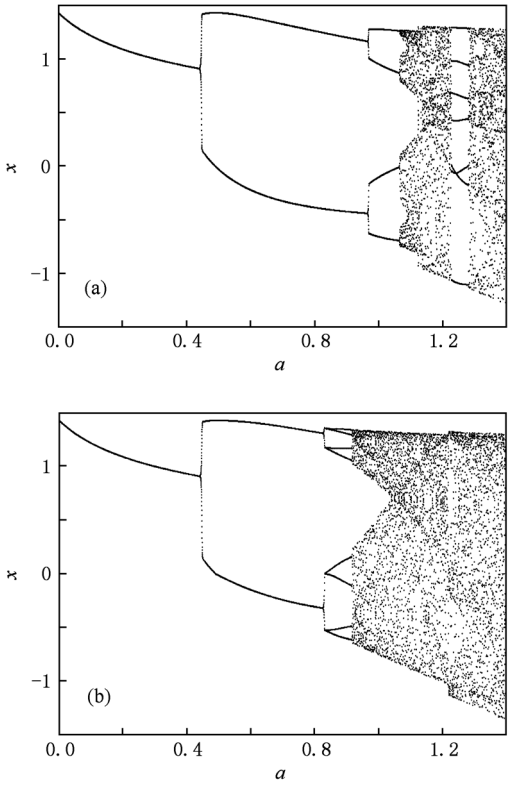

图 1 (a) Old-Hénon 映射分岔图; (b) New-Hénon 映射分岔图

2.2. Lyapunov 指数

根据 Lyapunov 指数定义[9]:

$$\lambda = \lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} \log |f'(x_n)|. \tag{3}$$

计算可知,在选定参数下,New-Hénon 映射的最大 Lyapunov 指数为 0.563, 比 Old-Hénon 映射的 0.412 要大. 图 2 所示是两个映射的变量 x 随参数 a 的 Lyapunov 指数谱,可见,在相同参数条件下,New-Hénon 系统的 Lyapunov 指数要比 Old-Hénon 系统的大,这也体现了改进后的混沌映射具有更好的初始值敏感性.

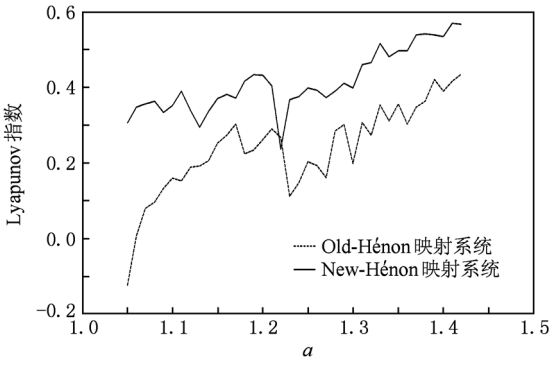

图 2 不同 a 下,混沌映射系统对应的 Lyapunov 指数谱

2.3. 线性复杂度

线性复杂度是系统安全性的一个重要指标. Bandt 等[10]提出的复杂性度量的排列组合熵(permutation entropy, 简记为 PE)算法,算法简单、易于实现. 它的具体步骤如下:(1)对长度为 N 的序列 $\{x_1, x_2, x_3, \cdots, x_N\}$ 进行 n 维相空间重构,得到 n 维向量集 $\{X_1, X_2, \cdots, X_{N-n+1}\}$,其中 $X_i = [x_i, x_{i+1}, \cdots, x_{i+n-1}]$, $1 \leqslant i \leqslant N-n+1$;(2)将重构后的 $(N-n+1)$ 个 n 维向量进行分类,按相对大小排序一致的向量数计为 A_k ($k \leqslant 2^n$),并求出所有分类的概率 $P_k = A_k/(N-n+1)$;(3)排列组合熵为 $H(n) = -\sum_{i=1}^{k} P_i \cdot \ln P_i$;(4)当 $P_k = 1/p!$ 时,$H(p)$ 就达到了最大值 $\ln(p!)$,据文献[11]的讨论,实际中,$H(p) \leqslant \ln(N-p+1)$. 为了方便,通常将 $H(p)$ 用 $\ln(N-p+1)$ 进行标准化处理,即

$$0 \leqslant h(p) = \frac{H(p)}{\ln(N-p+1)} \leqslant 1. \tag{4}$$

据此计算得到两种映射的线性复杂度如表 1 所示,比较可见,改进后的 New-Hénon 混沌系统具有更高的线性复杂度.

表 1 不同嵌入维数下混沌系统的排列组合熵(PE)

嵌入维数 n	4	5	6	7
Old-Hénon 映射系统	0.3214	0.4369	0.557	0.6641
New-Hénon 映射系统	0.3617	0.4996	0.6244	0.7266

3. 混沌二值序列的产生

混沌序列经过判决和量化后得到的序列可称为混沌伪随机序列. 方法有很多种,大多数文献常采用门槛函数方法,这种方法简单易行,对硬件电路的要求比较低,但判别基准难以确定,而且数据的精度也会受到限制. 二进制化方法相对门槛函数方法实现较为繁琐,对硬件的要求较高,但是其序列在相同的迭代次数下的周期比较长,并且克服了有限精度的限. 本文采用二进制化方法,将混沌序列转换为二值序列.

将实值数列转化二进制序列[12]:

$$|x_n| = 0.b_1(x_n)b_2(x_n)\cdots b_i(x_n)\cdots b_m(x_n)\quad (b_i(x_n)\in\{0,1\}), \tag{5}$$

其中 $b_i(x_n) = \mathrm{sng}_{0.5}(2^{i-1}|x_n| - \lfloor 2^{i-1}|x_n|\rfloor)$,$\lfloor x\rfloor$表示向下取整,

$$\mathrm{sng}_{0.5}(x) = \begin{cases} 0 & (x < 0.5), \\ 1 & (x \geqslant 0.5). \end{cases}$$

得到新的二进制数列$\{x_n\}$为

$$\begin{aligned} |x_0| &= 0.b_1(x_0)b_2(x_0)\cdots b_i(x_0)\cdots, \\ |x_1| &= 0.b_1(x_1)b_2(x_1)\cdots b_i(x_1)\cdots, \\ |x_2| &= 0.b_1(x_2)b_2(x_2)\cdots b_i(x_2)\cdots, \\ &\vdots \\ |x_n| &= 0.b_1(x_n)b_2(x_n)\cdots b_i(x_n)\cdots. \end{aligned} \tag{6}$$

在(6)式中取$\{x_n\}$的第 i 位,则可以得到我们所需的二值序列$\{b_i(x_n)\}$,$b_i(x_n)\in\{0,1\}$. 由文献[13]知道二值序列$\{b_i(x_n)\}$的均匀性随 i 的增大而增强,为了更好的反映新旧 Hénon 映射产生伪随机序列的性能差异,在本文的伪随机序列性能分析中,我们选取 $i=1,2,3$ 时组成长度为 10000 的序列进行随机性能分析.

4. 序列性能分析

4.1. 相关特性

相关特性是伪随机序列的一个很重要的性质. 理想的伪随机序列其自相关为 δ 函数,互相关函数恒等于 0,序列之间相互正交[1]. 对两个二值序列 $a_i(N)$ 和 $a_j(N)$,其相关定义如下:

$$R_{ij}(\tau) = \frac{\sum_{l=1}^{N} a_i(l)a_j(l+\tau)}{\sum_{l=1}^{N}[a_i(l)]^2}. \tag{7}$$

当 $i=j$ 时表示自相关,$i\neq j$ 时表示互相关.

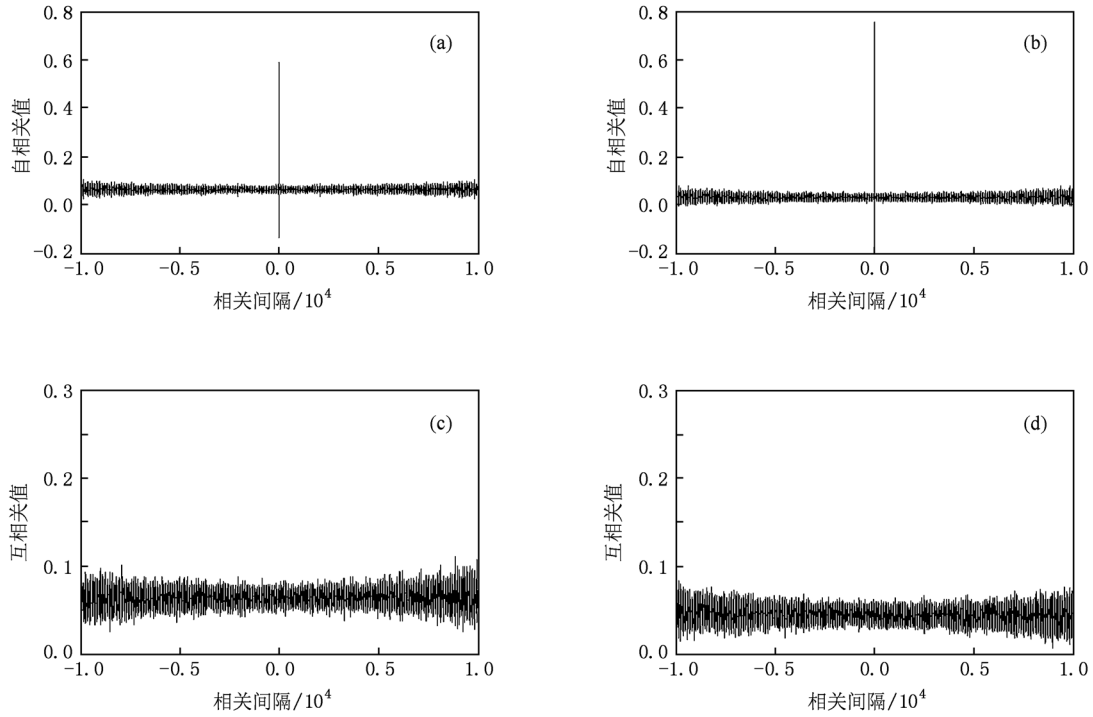

图 3 (a) Old-Hénon 映射序列自相关;(b) New-Hénon 映射序列自相关;(c) Old-Hénon 映射序列互相关;(d) New-Hénon 映射序列互相关

根据(7)式,对 Old-Hénon 映射和 New-Hénon 映射生成序列的自相关和互相关进行计算,图3是 $i=2$,序列长度为10000时两种序列的相关特性图.其中图(a)表示 Old-Hénon 映射产生的伪随机序列自相关特性,图(b)表示 New-Hénon 映射产生的伪随机序列自相关特性,图(c)表示 Old-Hénon 映射生成伪随机序列的互相关特性,图(d)表示 New-Hénon 映射生成伪随机序列的互相关特性.从图3可以看出 New-Hénon 映射产生的伪随机序列相比 Old-Hénon 映射产生的伪随机序列,具有更接近 δ 函数的自相关性和接近于0的互相关性.

4.2. 平衡性

在理想状态下,混沌伪随机序列的0与1的个数应该相等[1].设 A 和 B 分别表示序列中"1"与"0"的个数,则序列的平衡度 E[14]为

$$E = \frac{|A - B|}{N}. \tag{8}$$

表2是选取 $i=1,2,3$,序列长度为10000,改进前后两种系统生成的伪随机序列的平衡性.通过对比我们可以发现,改进后的 New-Hénon 映射系统产生的混沌伪随机序列,平衡度更接近于0,平衡性更好.

表2 不同映射系统产生长度为10000的伪随机序列平衡性

序列	映射系统	1的个数	0的个数	平衡度 E
$\{b_1(x_n)\}$	Old-Hénon	5128	4872	0.0256
	New-Hénon	4901	5099	0.0198
$\{b_2(x_n)\}$	Old-Hénon	5058	4942	0.0116
	New-Hénon	5031	4969	0.0062
$\{b_3(x_n)\}$	Old-Hénon	4949	5051	0.0102
	New-Hénon	5035	4966	0.0070

4.3. 游程特性

把随机序列中连续出现0或1的子序列称为游程.连续的0或者1的个数称为游程长度.随机序列中长度为1的游程约占游程总数的1/2,长度为2的游程约占游程总数的 $1/2^2$,…,长度为 k 游程占游程总数的 $1/2^k$,且任意长度的0的游程个数和1的游程个数相等[1].在表3中我们统计了 $i=1,2,3$,序列长度为10000时,改进前后两种映射产生的混沌伪随机序列中游程长度分别为1,2,3,4,5的游程数占游程总数的比值,结果如表3所示.对比发现,New-Hénon 映射产生的伪随机序列相比 Old-Hénon 映射产生的伪随机序列,具有更好的游程特性.

表3 不同映射系统产生长度为10000的伪随机序列游程特性

序列	映射系统	1	2	3	4	5
$\{b_1(x_n)\}$	Old-Hénon	0.5184	0.2386	0.1191	0.0579	0.0347
	New-Hénon	0.5081	0.2436	0.1218	0.0629	0.0315
$\{b_2(x_n)\}$	Old-Hénon	0.5077	0.2461	0.1276	0.0575	0.0303
	New-Hénon	0.4952	0.2526	0.1239	0.0610	0.0326
$\{b_3(x_n)\}$	Old-Hénon	0.5017	0.2528	0.1291	0.0621	0.0285
	New-Hénon	0.5007	0.2545	0.1228	0.0626	0.0327

5. 结 论

提出了通过引入绝对值项对传统 Hénon 映射进行改进.分析了改进后映射系统的基本动力学特性,包括分岔图,线性复杂度和最大 Lyapunov 指数,并对其生成的混沌伪随机序列的相关性,平衡性和游程特性进行了详细分析.数值结果表明,改进后的混沌系统较原系统其线性复杂度、初值敏感性等都有了很大提高,系统产生的伪随机序列的质量也有了一定的提高,并且和理论值比较接近.所以,基于改进后的混沌系统,可以生成性能优良,数量众多,适合应用于扩频通信的伪随机序列.

[1] Fu Z J, Zeng Y C, Xu M L 2008 *Acta Phys. Sin.* **57** 4014 (in Chinese) [付志坚、曾以成、徐茂林 2008 物理学报 **57** 4014]

[2] Li H 2004 *Chao. Digi. Commun.* (Beijing: Qinghua University Press) p142 (in Chinese) [李 辉 2004 混沌数字通信 (北京: 清华大学出版社) 第142页.]

[3] Zheng F, Tian X J, Song J Y, Li X Y 2008 *J. China Univers.*

Posts. Telecommun. **15**(3) 64
[4] Ernesto P, Borges A, Ugur Tirnakli B 2004 *Physica* D **193** 148
[5] Richter H 2002 *Inter. J. Bifurcat. Chaos* **12** 1371
[6] Shawn D P, Ned J 2006 *Phys. Rev. Lett.* **96** 034105
[7] Pellicer-Lostao C, Lo'pez-Ruiz R 2008 *arXiv*: **0801** 3982
[8] Chieko M, Wakako M 2002 *Chaos Solit. Fract.* **14** 1
[9] Luo L J, Li Y S, Li T, Dong Q T 2005 *Compu. Simulat.* **12** 0285 (in Chinese)[罗利军、李银山、李 彤、董青田 2005 计算机仿真 **12** 0285]
[10] Bandt C, Pompe B 2002 *Phys. Rev. Lett.* **88** 174102.
[11] Sun K H, Tan G Q, Sheng L Y 2008 *Acta Phys. Sin.* **57** 3359 (in Chinese)[孙克辉、谈国强、盛利元 2008 物理学报 **57** 3359]
[12] Wang X G, Zhan M, Gong X F 2005 *Phys. Lett.* A **334** 30
[13] Sheng L Y, Xiao Y Y, Sheng Z 2008 *Acta Phys. Sin.* **57** 4007 (in Chinese)[盛利元、肖燕予、盛 喆 2008 物理学报 **57** 4007]
[14] Yu Z B, Feng J C 2008 *Acta Phys. Sin.* **57** 1409 (in Chinese)[余振标、冯久超 2008 物理学报 **57** 1409]

Modified Hénon map generated chaotic pseudorandom-bit sequences and performance analysis*

Li Jia-Biao† Zeng Yi-Cheng Chen Shi-Bi Chen Jia-Sheng
(*Department of Optoelectronic Engineering, Institute of Intelligent Optoelectronic Technology, Xiangtan University, Xiangtan* 411105, *China*)

(Received 19 August 2010; revised manuscript received 17 September 2010)

Abstract

A method of improving the traditional Hénon map is proposed in the paper. The internal structure of the system is changed by adopting absolute value term. The linear complexity and sensitivity to initial conditions of the proposed system have been greatly enhanced. The performance of pseudorandom-bit sequences which are generated by the proposed system is analyzed in comparison with the ones that are generated by chaotic system. The performance of the sequence generated by the proposed system is improved compared with the original system. Theoretical analysis and the simulation results show the feasibility of the method.

Keywords: Hénon map, pseudorandom-bit sequences, performance analysis
PACS: 05.45.Ac, 05.45.Pq, 05.45.Vx

* Project supported by the National Natural Science Foudation of China (Grant No. 60972147).

† E-mail: Lijiabiao_2008@yahoo.cn