

广义映射混沌扩频序列及其特性分析

廖旒焕^① 高金峰^②

^①(华北水利水电学院 动力工程系 郑州 450008)

^②(郑州大学 电气工程系 郑州 450002)

摘要 该文从扩频通信对扩频码序列的要求出发,提出采用广义映射产生混沌数字序列的思路。通过对广义映射混沌数字序列相关性和平衡性的分析,给出一种改进的广义映射混沌数字序列生成方法。计算机模拟分析表明,使用该文方法生成的混沌序列具有良好的平衡性和保密性,更适合在码分多址通信中应用。

关键词 扩频通信, 广义映射, 扩频序列, 相关性, 平衡性

中图分类号: TN914.42

文献标识码: A

文章编号: 1009-5896(2006)07-1255-03

The Chaotic Spreading Sequences Generated by the Extended Chaotic Map and Its Performance Analysis

Liao Ni-huan^① Gao Jin-feng^②

^①(Dapt. of Power Eng., North China Institute of Water Conservancy and Hydroelectric Power, Zhengzhou 450008, China)

^②(School of Electric Eng., Zhengzhou University, Zhengzhou 450002, China)

Abstract In view of the performance of the spreading sequences for spread-spectrum communication system, a novel method of obtaining chaotic digital sequences based on the extended chaotic map is given in this paper. The correlation and balance performances of the new sequences are analysed, furthermore, an advanced method of generating the digital sequences is proposed, in order to get excellent balance performance. The simulation results show that the chaotic spreading sequences generated by the advanced method possess excellent performance and security, specially for CDMA communication system.

Key words Spread-spectrum communication, Extended chaotic map, Spreading sequences, Correlation performance, Balance performance

1 引言

扩频码序列在扩频通信中具有十分重要的作用,不仅频谱的展宽是由扩频码序列调制产生,而且直扩系统的一些良好性能,如抗干扰性、低截获率、抗多径干扰、码分多址等都与扩频码序列有着密切的关系。传统扩频通信中,常用 m 序列作为扩频码序列。然而 m 序列具有周期性、数量有限、保密性低等缺点。混沌信号具有宽带、连续频谱、对初始条件敏感依赖性等特点,可以产生大量的、相关性能良好的随机序列,能够满足扩频通信的需要。

理想混沌序列具有非周期性,但应用于数字通信的混沌序列是被截断为有限长度的混沌序列,数字实现上的有限精度效应,容易导致序列呈周期性。如何克服周期性同样是混沌扩频序列走向实用化的关键。从保密性角度讲,由一维迭代产生的混沌扩频序列^[1,2],尽管有比较理想的相关性能,却容易用预测技术破解,保密性不好。因而在实用中尽量使混沌映射复杂化,增强破解难度。

本文以文献[3]提出的广义映射模型概念为基础,进一步研究广义映射模型产生混沌序列的相关性和平衡性。由于广

义映射混沌序列在不同的时段由不同的混沌映射迭代产生,不同时间段的序列对应于不同的混沌吸引子,提高了序列的复杂度,相应延长了序列的周期,使序列保密性更好。计算机模拟发现,广义映射直接产生的混沌序列的平衡性并不理想,针对序列平衡性不理想的问题,提出了一种改进广义映射序列生成方法,研究表明改进的序列不仅有理想的平衡性,而且进一步提高了序列的抗破译能力。

2 序列的生成

广义映射就是要构建一个统一的结构模式,且在此模式下,根据参数变化系统表现为不同的映射。能够在统一结构模式里实现的混沌映射一定要保证其值域范围一致,这样才能使各个映射的输入不会超出其值域范围。logistic 映射,立方映射, Tent 映射,人字映射, Chebyshev 映射等的值域范围都在 $(-1, 1)$ 之间。由文献[1,2]可知,由 logistic 映射,立方映射和 Chebyshev 映射产生的混沌序列具有良好的相关性。因此,该文选取 logistic 映射,立方映射, Chebyshev 映射构建一种广义混沌映射:

$$x_{n+1} = a_0 + a_1 x_n + a_2 x_n^2 + a_3 x_n^3 + a_4 \cos(k \cos^{-1} x_n) \quad (1)$$

选取合适的参数 a_i 及 k , 式(1)对应于不同的混沌映射。

当 $a_0 = 1, a_2 = -2, a_1 = a_3 = a_4 = 0$ 时, 式(1)对应于 logistic 混沌映射; 当 $a_1 = 3, a_3 = -4, a_0 = a_2 = a_4 = 0$ 时, 式(1)对应于立方混沌映射; 当 $a_0 = a_1 = a_2 = a_3 = 0, a_4 = 1, k = 4$ 时, 式(1)为 Chebyshev 混沌映射。可见通过一定的参数切换方式, 使式(1)在不同的时间段具有不同的参数, 对应于不同混沌映射, 也就是在一种结构下实现了多种混沌映射。

首先根据式(1)模型, 研究由其产生混沌序列的性能。参数的切换原则可根据需要任意确定。可以采用等序列间隔, 也可以用不等序列间隔, 甚至使用随机序列间隔。为分析方便, 下面讨论的序列 x_n 由等序列间隔参数切换原则产生。序列 x_n 的总长度 $N = 1500$, 每 300 个点切换一次参数, 对应的映射依次为 logistic 映射、立方映射、Chebyshev 映射。实际应用中将 x_n 数字化的方法很多, 可以采用符号函数, 也可以采用文献[4]提出的中间多比特量化方法。本文采用符号函数, 即

$$b_n = \text{sgn}(x_n) \tag{2}$$

3 序列相关性分析

在扩频通信中, 扩频码的自相关特性决定了扩频系统的捕捉、跟踪、多址和抗干扰的能力, 扩频码的互相关函数特性决定了扩频系统的抗多址干扰的能力, 因此, 扩频码的相关特性的好坏对扩频系统的工作性能影响极大。长度为 N 的二值混沌序列 b_n 的自相关函数定义为

$$ac(m) = \frac{1}{N} \sum_{i=1}^{N-m} b_i b_{i+m} \tag{3}$$

初值不同的两个二值混沌序列 b_{1n}, b_{2n} 的互相关函数定义为

$$cc_{12}(m) = \begin{cases} \frac{1}{N} \sum_{i=1}^{N-m} b_{1i} b_{2(i+m)}, & 0 \leq m \leq N \\ \frac{1}{N} \sum_{i=1}^{N-m} b_{1(i+m)} b_{2i}, & -N \leq m < 0 \\ 0, & \text{其他} \end{cases} \tag{4}$$

用 MATLAB 计算序列 b_n 的归一化自相关函数和互相关函数如图 1 和图 2 所示。

通过选择不同的初值进行大量的计算机模拟发现, 初值对广义映射序列的相关性没有显著的影响, 几乎任意初值的广义映射产生的混沌序列都具有良好的相关性, 这与单一映射混沌序列性质一致。

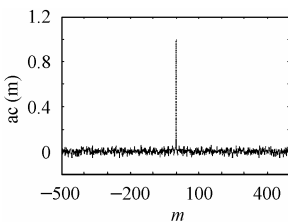


图 1 广义映射序列自相关图
Fig.1 Auto-correlation of the sequences generated by the extended chaotic map

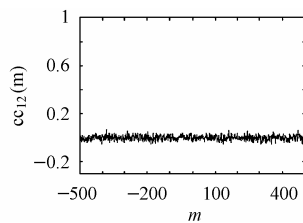


图 2 广义映射序列互相关图
Fig.2 Cross-correlation of the sequences generated by the extended chaotic map

对于广义映射混沌序列来说, 参数切换原则直接影响混沌序列复杂度, 参数切换原则越复杂, 生成的混沌序列越复杂, 越难以预测。然而通过对多种切换原则的计算机模拟表明, 参数切换原则对相关性也没有明显的影响。不管采用何种切换原则, 生成的序列都具有良好的相关性, 与单一映射相同, 所取序列的长度越长, 相关性就越好。

4 序列平衡性分析

在码分多址通信中, 扩频码序列的平衡性与多址通信系统载波抑制有密切的关系, 扩频码序列的平衡性不好, 则系统的载波泄漏大, 因此在多址通信中要求选取平衡性好的扩频序列。文献[5]详细分析了 logistic 序列, Chebyshev 序列的平衡性与混沌映射的参数, 初值的关系。初值对 Chebyshev 序列的平衡性基本不产生影响。对 logistic 序列来说, 除了几个特殊的初值点会引起平衡性峰值外, 初值对序列的平衡性影响也不明显。因此在选取广义映射的初值时, 应避免引起平衡性峰值的特殊初值点。

分析表明, 一定参数情况下的单一映射混沌序列, 序列越长, 平衡性则越好。但广义映射序列没有这一性质。从表 1 给出的结果可以看出, 广义映射序列的平衡性与参数切换的频度、长度都没有明显的关系。即其平衡性既不随参数切换频度变低(对应的单一映射长度相应变长)而有较好的平衡性, 也不是象单一映射序列一样, 序列越长, 平衡性越好。图 3 给出了不同初值下序列的平衡性与参数切换序列间隔的关系, 从图上可以直观地看出广义映射混沌序列的这一性质。

表 1 $N=3000$ 时的平衡性分析

Tab.1 The balance performance analysis when $N=3000$					
平衡性 E	初 值				
间隔 n	0.0101	0.2101	0.3425	0.4096	0.5723
200	0.0652	0.0413	0.1027	0.0407	0.076
300	0.0060	0.0073	0.016	0.0047	0.0147
400	0.0220	0.0193	0.0493	0.0200	0.0020
500	0.0133	0.0067	0.0273	0.0013	0.0093
600	0.0033	0.0573	0.0147	0.0647	0.0033
700	0.0027	0.0180	0.016	0.0227	0.0313
800	0.093	0.0113	0.0213	0.0120	0.0087
900	0.0047	0.0947	0.0080	0.0373	0.0047
1000	0.0087	0.0273	0.0267	0.0113	0.0153

注: 表中 $E = |p - q| / N$, p 为 b_n 中 1 的个数, q 为 b_n 中 0 的个数。

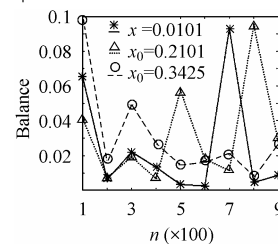


图 3 序列的平衡性与参数切换原则的关系
Fig.3 Relation between the balance performance and the parameter switching rules

从保密性角度讲, 希望参数有较高的切换频度和复杂的切换原则; 从保证序列的平衡性讲, 要在众多的初值及参数切换原则中优选。因此, 如何在实际中使二者统筹兼顾确实是一项比较繁琐且有意义的工作。

5 序列平衡性改进方法

由于广义映射混沌序列需要解决平衡性不理想及如何进一步增强保密性问题, 此处提出一种改进的广义映射序列的生成方法。该方法既可改善序列的平衡性, 又可进一步提高序列的保密性或复杂性。

映射模型仍采用式(1), 但对每次参数切换生成的实值序列进行抽样, 即由

$$x_{n+1} = f^{(p)}(x_n) = \underbrace{f(f(\dots(f(x_n))))}_p \quad (5)$$

生成混沌序列^[6]。通过对函数 $x_{n+1} = f(x_n)$ 每迭代 p 次取一个点, 获得的新序列。对新序列进行二值化处理, 处理过程不再对整个序列二值化, 而是分段进行。即对每次参数切换后的单一映射序列分别进行处理, 二值化函数用门限函数

$$b'_n = \begin{cases} 0, & x < c \\ 1, & x \geq c \end{cases} \quad (6)$$

式中的 c 为对应各段实值序列的中值, 它随系统参数的不同而不同。对应的映射、初值点不同时, c 的取值不同。由文献[6]可知, 经过中值门限数字化的二值混沌序列, 当序列长度为偶数时, 序列平衡性 $E = 0$; 序列长度为奇数时, 序列的平衡性 $E = 1/N$ 。所以此种序列具有近似理想的相关性能。进一步, 由于在抽样过程中丢弃了很多混沌映射的信息, 序列更难以用预测的方法重构, 从而提高了保密性。图 4 与图 5 给出了 $p=3$, 序列间隔为 300, 长度 $N=1500$ 时一典型序列的相关图。由相关图可以看出, 在初始条件和长度都一样的条件下, 改进混沌序列的相关性和原序列的相关性相比没有显著变化。在实现相同长度的混沌序列时, 改进广义映射混沌序列的迭代次数是原序列的 p 倍, 在硬件实现上要比直接广义映射的结构复杂, 要增加抽样电路及中值生成环节, 但改进序列具有更好的保密性, 而且具有理想的平衡性, 更适合在多址通信中应用。图 6 和图 7 给出了把广义序列及改进的序列用作直扩序列的扩频信号频谱, 扩频因子 $\alpha = 1000$ 。

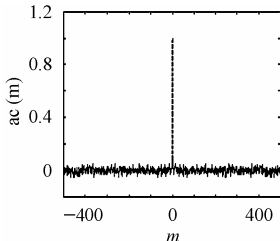


图4 改进序列的自相关图
Fig.4 Auto-correlation of the advanced sequences

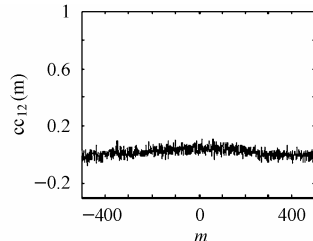


图5 改进序列的互相关图
Fig.5 Cross-correlation of the advanced sequences

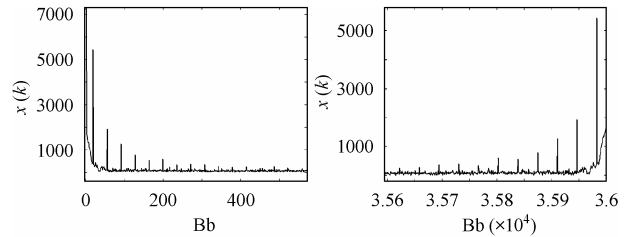


图 6 直接序列 Bb 的频谱

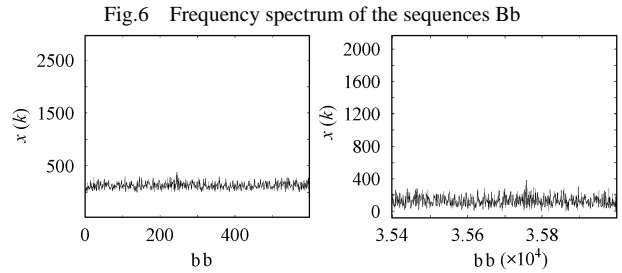


图 7 改进序列 bb 的频谱

Fig.7 Frequency spectrum of the advanced sequences bb

从图6中可以看出, 对于直接生成的广义序列作直扩序列 Bb , 其扩频信号的频谱在一个周期里有一些峰值, 而改进序列作直扩序列 bb 时, 从图7可以看出一个周期内频谱的比较平滑。这样用改进序列的保密性更好, 而且发射功率小。

6 结束语

本文的广义映射模型可以在一种结构下实现多个混沌映射, 所生成的混沌序列具有良好的相关特性。此混沌序列要比单一映射产生的混沌序列复杂, 可以有效延长序列的周期, 预测难度增加, 保密性更好。为了进一步提高序列的保密性, 并改善广义映射直接生成的混沌序列的平衡性, 提出了一种改进序列平衡性的方法。理论分析和计算机模拟证明, 对于改进的广义映射混沌序列, 不但具有良好的相关性, 而且具有理想的平衡性, 更适合作码分多址扩频序列用。

参考文献

- [1] 蔡国权, 宋国文等. logistic 映射混沌扩频序列的奇/偶相关特性分析. 电子学报, 1999, 27(11A): 128-130.
- [2] 蔡国权, 宋国文等. 基于 Chebyshev 映射的四相扩频序列. 电子学报, 1999, 27(8): 74-77.
- [3] 张家树, 肖先赐. 基于广义混沌映射切换的混沌同步保密通信. 物理学报, 2001, 50(11): 2121-2124.
- [4] 朱志良. 中间多比特量化混沌扩频序列及其性能分析. 东北大学学报, 2002, 23(8): 737-739.
- [5] 于舒娟. 二相混沌扩频序列相关性分析. 沈阳工业学院学报, 2001, 20(2): 84-89.
- [6] Zhang Hong Tao. Oversampled chaotic sequences with good security. *Journal of Circuits, Systems, and Computers*, 2002, 11(2): 173-185.

廖旋焕: 女, 1975 年生, 硕士, 研究方向为混沌同步在保密通信上的应用。

高金峰: 男, 1963 年生, 工学博士, 教授, 长期从事非线性系统理论与控制方面的教学和科研工作。