基于优选准则的混合混沌序列的生成

董文华 郭淑霞
(西北工业大学电子信息学院 西安 710072)

摘 要 针对传统的 m 序列、Gold 序列可用作扩频码的数量有限这一问题,提出了用混沌序列代替传统的 m 序列、Gold 序列的方法。针对单个低维混沌映射产生的混沌序列存在抗攻击能力差、密钥空间小、保密性不理想等缺点,依据优选结果将单个低维的改进型 Logistic 序列与 Chebyshev 序列组合产生了一种新的混合序列。仿真结果表明,新的混合混沌序列平衡性高、类随机、相关性好,且该混合混沌序列和 m 序列、Gold 序列的抗 AWGN 干扰和抗单频干扰的能力相近。

关键词 优选准则,混合混沌序列,抗干扰,蒙特卡罗
中图法分类号 TN918 **文献标识码** A

Generation of Mixed Chaotic Sequences Based on Optimization Criterion

DONG Wen-hua GUO Shu-xia
(School of Electronics and Information, Northwestern Polytechnical University, Xi'an 710072, China)

Abstract The number of traditional m sequence with and Gold sequence which can be used as spreading codes is limited. In order to solve this problem, using chaotic sequence instead of m sequence and Gold sequence was proposed. However, the chaotic sequence of single low-dimensional chaotic mapping has some shortcomings in terms of anti attack ability, key space and security. According to the optimization results, this paper presented a new mixed chaotic sequence by the combination of the single low-dimensional Logistic sequences and Chebyshev sequences. Results of performance analysis and simulation indicate that the new chaotic sequence does well in balance, random and correlation, and the anti-jamming ability of mixed chaotic sequences, m sequence and Gold sequence is similar.

Keywords Sequence optimized selection, Mixed chaotic sequences, Anti-jamming, Monte carlo

1 引言

直扩系统具有保密、抗干扰、多址等优良性能,因此被广泛地应用于导航、无人机数据链等领域[1]。在直扩系统中,扩频码的好坏与直扩系统的性能成正比,所以对扩频码的研究至关重要。传统的满足三值特性的 m 序列优选对很少,限制了 m 序列、Gold 序列可用作扩频码的数量[2],而混沌序列对初值很敏感,使其数量巨大。因此,很多学者已将注意力集中到用混沌序列代替传统 m 序列、Gold 序列等的研究上[3]。

由于单个低维混沌映射产生的混沌序列抗攻击能力差、密钥空间小、保密性不理想等[4,5]问题,作者依据混沌序列优选结果,将单个低维的改进型 Logistic 序列与 Chebyshev 序列组合产生了一种新的混合序列,并仿真分析了其统计特性和抗 AWGN 干扰、抗单频干扰的能力,该混合混沌序列不仅降低了扩频码被破解的可能性,还提高了直扩系统的抗干扰能力。

2 混沌序列的优选

2.1 混沌序列优选准则

在相同序列长度下,混沌序列对初值或分形参数极度敏感,可以得到近乎无数多个序列,然而并不是所有序列的性能都满足要求,因此必须对其进行优选才能获得性能良好的扩频码。

多址干扰和多径干扰是影响直扩系统性能好坏的决定因素。所以将抑制上述两种干扰作为序列优选的准则。对混沌序列优选的准则是:平衡性准则、自相关准则和互相关准则。

(1)平衡性准则:假如一定长度的混沌序列的平衡度 E 小于阈值,则该序列就是平衡的。满足平衡性条件的序列具有较好的载波抑制度。

(2)自相关准则:理想中扩频序列的自相关函数应是 δ 函数,但在实际中序列达不到要求。本文是以自相关函数旁瓣的最大值作为优选条件。满足自相关条件的序列抗多径干扰能力较强。

(3)互相关准则:理想中扩频序列的互相关函数是 0,实际是达不到的。本文是以互相关峰值作为优选条件。满足自相关条件的序列抗多址干扰能力较强。

2.2 混沌序列优选过程

对混沌序列进行优选,首先根据不同的初值产生 N 个长度为 M 的实值混沌序列。将 Gold 序列的平衡度、自相关旁瓣的最大值和互相关峰值作为优选准则的阈值[6]。图 1 所示

本文受国家自然科学基金项目(61571368),国防技术基础科研项目(2014607B006)资助。
董文华(1991-),女,硕士生,主要研究领域为电磁环境仿真、测控链路抗干扰方法,E-mail:1457090425@qq.com;郭淑霞(1965-),女,博士,副教授,主要研究领域为电子战、数据链、软件无线电等。

为混沌序列的优选流程图。混沌序列的优选过程如下：

(1)对 N 个混沌序列进行平衡性判定，得到满足要求的 N_1 个序列。若混沌序列的平衡度小于平衡性准则的阀值，则判定其自相关性；否则剔除此序列，并改变序列的初值，重复上述过程。

(2)对(1)中得到的 N_1 个混沌序列进行自相关性判定，得到满足要求的 N_2 个序列。若混沌序列的自相关旁瓣峰值小于自相关准则的阀值，则判定其互相关性；否则剔除此序列，并改变序列的初值，从(1)开始重复上述过程。

(3)对(2)中得到的 N_2 个混沌序列进行互相关性判定，得到满足要求的 N_3 个序列。若混沌序列的互相关峰值小于互相关准则的阀值，则该序列满足优选条件，并结束优选过程；否则剔除此序列，并改变序列的初值，从(1)开始重复上述过程，直到序列满足优选准则为止。

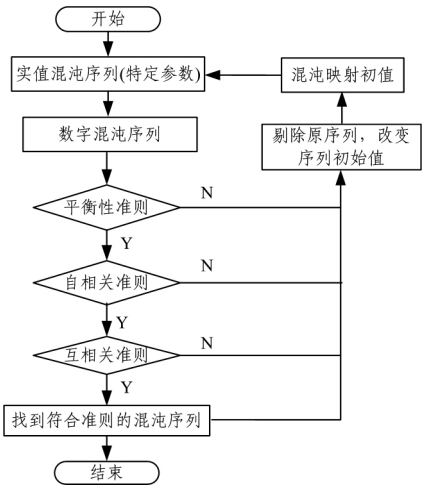

图 1　混沌序列的优选流程图

依据上述优选过程，选取序列长度 $N=255$ 的 Gold 码的平衡性与相关性作为判定标准。标准如下：1)平衡度 E 小于 0.01；2)自相关旁瓣最大值小于 0.15；3)互相关峰值小于 0.2[7]。

根据序列不同的初始值得到 6000 个长度为 255 的混沌序列，将这 6000 个混沌序列依次经过优选流程，得到满足标准的序列。选用 Logistic 序列的分形参数 $\mu=4$，Chebyshev 序列的分形参数 $\omega=20$，Tent 序列的分形参数 $a=0.4$，Hybrid 序列的分形参数 $b=0.5$，$\mu1=1.8$，$\mu2=2.0$。设置采样间隔 $l=0.00005$，将初值区间(0，0.3)设为搜索区域，这样产生了 6000 个待搜索的序列，筛选的结果如表 1 所列。

表 1　混沌序列筛选结果

映射函数	平衡性筛选 N_1	自相关性筛选 N_2	互相关性筛选 N_2
Chebyshev	938	443	72
Logistic	920	406	90
改进 Logistic	942	410	72
Tent	856	17	12
Hybrid	25	0	0

由表 1 可得出以下结论：Tent 序列与 Hybrid 序列的相关性相比其他 3 种序列都较差；*Logistic* 序列的统计特性很理想，但其均值不为 0。

3　混合混沌序列的生成及其特性分析

3.1　混合混沌序列生成

单个低维混沌映射迭代产生的序列数量多，不但没有周期性，而且频谱宽、类随机、相关性好[8-10]。然而，其存在抗攻击能力差、密钥空间小、保密性不理想等缺点。因此，本文采用统计性能比较好的改进型 Logistic 序列与 Chebyshev 序列进行组合，产生混合混沌序列。

改进型 Logistic 映射定义为：$x_{n+1}=1-2x_n^2$，其中 $x_0\in(-1,1)$。

ω 阶的 Chebyshev 映射定义为：$x_{n+1}=\cos(\omega\arccos x_n)$，$|x_n|\leqslant1$。$x_n$ 是当前时刻的状态，x_{n+1} 是下一时刻的状态。分形参数 $\omega\geqslant2$ 时，该映射具有遍历性和混沌性。

产生混合混沌序列的步骤如下：1)Chebyshev 映射迭代得到序列 f_1，将 f_1 当作改进型 Logistic 映射的初值，得到序列 f_3；2)改进型 Logistic 映射迭代得到序列 f_2，将 f_2 当作 Chebyshev 映射的初值，得到序列 f_4；3)将序列 f_3 和 f_4 量化后进行异或最终获得混合序列 f_5。图 2 所示为该混合混沌模型。

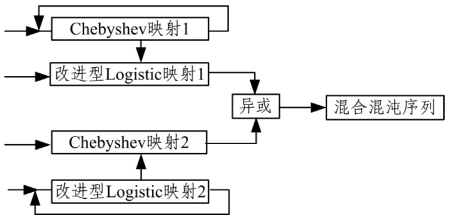

图 2　混合混沌模型

利用具有一定复杂度的映射结构产生的混沌扩频序列能够有效防止映射的参数被同步预测，这对混沌扩频系统的安全性是至关重要的。

3.2　混合混沌序列统计特性

(1)随机性分析

序列的随机性与信息的安全性成正比，因此分析序列的随机性是很有意义的。作者使用国际公认的 FIPS PUB 140-2 标准检测混合混沌序列的随机性。由 FIPS PUB 140-2 标准可知，选取长为 20000 的序列，可测试其单位、扑克、游程以及长游程。选取 5 组由不同初始值得到的序列进行测试，表 2 即其测试结果。

表 2　混合混沌序列 FIPS PUB 140-2 测试结果

序号	单位测试	扑克测试	游程测试
1	10028	12.1536	R1=2522，R2=1256，R3=632，R4=317，R5=174，R6+=140
2	10004	7.1744	R1=2556，R2=1191，R3=670，R4=294，R5=160，R6+=153
3	9895	28.8896	R1=2497，R2=1229，R3=601，R4=325，R5=135，R6+=171
4	9956	12.6912	R1=2485，R2=1234，R3=658，R4=292，R5=162，R6+=155
5	10024	8.5504	R1=2596，R2=1240，R3=591，R4=329，R5=158，R6+=156

由表 2 可知，5 组任意的二值伪随机序列完全通过了 FIPS PUB 140-2 标准规定的 4 项测试，则该混合混沌映射序列具有很好的随机性。

(2)平衡性分析

序列的不平衡会导致信息的载波泄露、传输的信息丢失以及误码率的增大。因此，分析序列的平衡性也是很有意义的。若文中产生的混合混沌序列中“1”和“−1”的数目分别是 M 和 N，则其平衡度 $E=(M-N)/T$[11]。其中 T 为序列的码元总数。

仿真分析文中生成的混合混沌序列的平衡性。若 $\omega=20$，由图 3 平衡性曲线可知，该序列平衡度 $E<0.02$，符合要求。

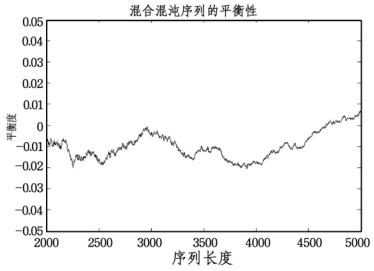

图 3　平衡性曲线

(3)相关性分析

序列的相关性影响了扩频系统的通信误码率。因此,其要求序列具有良好的相关特性。图 4 仿真了 $\omega=20$、初值是 0.32 时序列的自相关特性;图 5 是序列初值分别取 0.32000000、0.32000001 时的互相关特性。

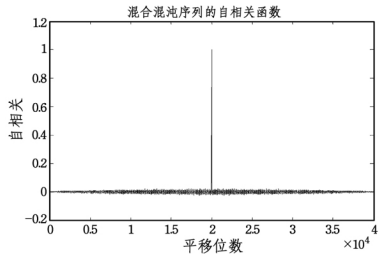

图 4　自相关特性

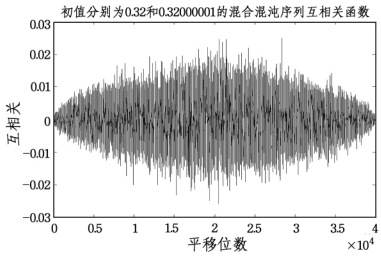

图 5　互相关特性

由图 4、图 5 的仿真结果可知,该混合序列的相关特性很好,能很好地解决扩频系统的同步问题。

4　混合混沌序列的抗干扰分析

采用蒙特卡罗的思想来仿真分析混合混沌序列的抗干扰能力,其基本原理是:首先利用产生的随机信息序列进行扩频调制,扩频码字是混合混沌码,经过 BPSK 调制后,送到加有高斯白噪声(AWGN)的信道中,在接收端与多路伪码进行相关,寻找最大相关值的支路,确定伪码序列,并根据其对信息序列解扩、解调,进而获得最终信号。最后将发送的信息和接收到的信息进行对比分析,计算出相对误码率。仿真思路如图 6 所示。下面主要仿真分析混合混沌序列的抗 AWGN 干扰和抗单频干扰能力。

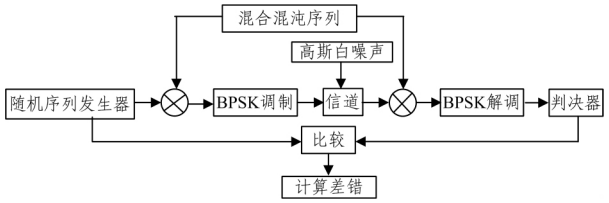

图 6　仿真思路图

采用 m 序列、Gold 序列的直扩系统和采用混合混沌序列的直扩系统的抗 AWGN 干扰和抗单频干扰能力相比结果分别如图 7 和图 8 所示。

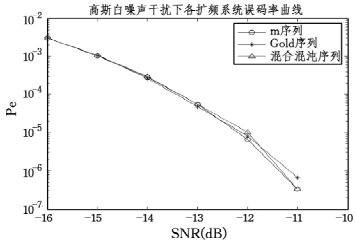

图 7　抗干扰性能(AWGN 干扰)

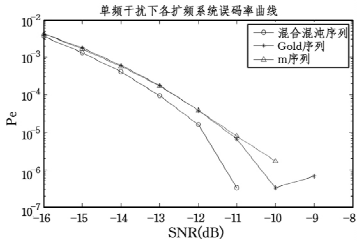

图 8　抗干扰性能(单频干扰)

由图 7、图 8 可知,混合混沌序列和 m 序列、Gold 序列的抗 AWGN 干扰和抗单频干扰的能力相近,但由于混合混沌序列的数量巨大且具有一定的复杂度,能够有效防止序列的参数被同步预测,因此该混合混沌序列适用于扩频系统。

结束语　文中依据平衡性准则、自相关准则和互相关准则对混沌序列进行优选,并依据优选结果将单个低维的改进型 Logistic 序列与 Chebyshev 序列组合产生了一种新的混合混沌序列。通过对混合混沌序列的统计特性及抗干扰性能仿真分析可知,该混合混沌序列平衡性高、类随机、相关性好,且该混合混沌序列和 m 序列、Gold 序列的抗 AWGN 干扰和抗单频干扰的能力相近。因此,该混合混沌序列不仅降低了扩频码被破解的可能性,还提高了直扩系统的抗干扰能力。

参 考 文 献

[1] 张严平,陆锐敏,马世旺. 一种混合混沌序列的研究[J]. 通信技术,2015,48(3):267-271

[2] 曾兴雯,刘乃安,孙献璞. 扩展频谱通信及其多址技术[M]. 西安:西安电子科技大学出版社,2004:90-110

[3] 王航,郭静波,王赞基. 混沌多进制直接序列扩频信号的盲解扩[J]. 清华大学学报(自然科学版),2009,49(1):14-16

[4] 李彩虹,李贻斌,赵磊,等. 一维 Logistic 映射混沌伪随机序列统计特性研究[J]. 计算机应用研究,2014,31(5):1403-1406

[5] 魏金成,魏巍. 改进型 Logistic-Map 混沌序列分析[J]. 电子设计工程,2011,19(4):20-23

[6] 刘联会,石军,石磊. 混沌扩频序列的优选算法及其系统性能研究[J]. 系统工程与电子技术,2004,26(12):1909-1911

[7] 张严平,陆锐敏. 一种改进的混沌扩频序列优选算法[J]. 计算机工程,2016,42(3):121-124

[8] Tohur K, Akio T. Pseudonoise sequences by chaotic nonlinear maps and their correlation properties[J]. IEICE Transactions on Communications, 1993, 76(8): 855-862

[9] Li T Y, Yorke J A. Period three implied chaos[J]. Springer New York, 2004, 82(82): 985-992

[10] Rao Ni-ni. A class of Chaotic spreading codes for A-CDMA system[J]. Journal of University of Electronic Science and Technology of China, 2000, 29(5): 465-468

[11] 胡健栋,郑朝辉,龙必起,等. 码分多址与个人通信[M]. 北京:人民邮电出版社,1996:153-170