一种新型的分段 Logistic 混沌扩频通信算法

张 薇[1] 谢红梅[1] 王保平[2]
(西北工业大学电子信息学院 西安 710129)[1] (西北工业大学无人机特种技术重点实验室 西安 710065)[2]

摘 要 混沌序列作为扩频系统中的扩频码,具有序列丰富、保密性好等特性。针对传统的 Logistic 混沌序列及其改进型在序列遍历性和随机性等方面不太理想的问题,提出了一种新型的分段 Logistic 混沌扩频通信算法。在分析了所提混沌序列的随机性、相关性、初值敏感性和 Lyapunov 指数的基础上,将其应用于扩频通信系统中。仿真结果表明:新序列较传统的 Logistic 混沌序列及其改进型作为扩频通信地址码,在误码率和信息保密特性方面有很大改善,从而证明了新算法的有效性。

关键词 分段 Logistic 序列,混沌,扩频通信
中图法分类号 TN914.42 **文献标识码** A

Novel Piecewise Logistic Chaotic Spread Spectrum Communication Algorithm

ZHANG Wei[1] XIE Hong-mei[1] WANG Bao-ping[2]
(School of Electronics and Information, Northwestern Polytechnical University, Xi'an 710129, China)[1]
(Science and Technology on UAV Laboratory, Northwestern Polytechnical University, Xi'an 710065, China)[2]

Abstract Chaotic sequence as spreading code in spread spectrum systems has the characteristics of rich sequences and good confidentiality. Traditional Logistic chaotic sequence as well as its modified sequence is not ideal in ergodicity and randomness of its sequence. To solve this problem, a new piecewise Logistic chaotic spread spectrum communication algorithm was proposed based on the analysis of the randomness, correlation, initial sensitivity and Lyapunoy exponents of the referred chaotic sequence, and applied to spread spectrum communication. The simulation results show that the algorithm greatly improves the error rate and confidentiality in the spread spectrum communication compared to the traditional logistic chaotic sequence and its modified sequence, which proves that the algorithm mentioned in this article is effective.

Keywords Piecewise Logistic sequence, Chaotic, Spread spectrum communication

1 引言

在扩频通信中,地址码的选取非常重要[1]。传统的扩频技术采用二值伪随机(PN)序列作为扩频和解扩序列。但由于序列码集中,地址码的个数有限,因此互相关函数存在大的尖峰,容易被破译,系统的保密性很差。用混沌序列代替一般的伪随机序列作为扩频系统的扩频序列,为选择扩频序列开辟了新途径[2]。

混沌序列是由确定性方程产生的,在方程参数和初始值确定时可重现混沌现象,并且混沌序列对方程参数和初始值极其敏感[3,4]。同时,它具有高斯白噪声的统计特征和序列的遍历性。其吸引子是非常复杂的分形结构,具有长期不可预测性。因此,混沌系统被广泛应用于保密通信[5-7]和数据安全[8,9]等众多科研领域中。

Logistic 混沌映射结构简单,性能良好,是目前应用较为广泛的一种混沌映射。为了更好地完善 Logistic 映射的性能,有学者在此基础上提出了一种改进型的 Logistic 映射[10]。与原映射相比,此改进型映射可以更早地进入混沌状态,而且相关特性更加理想。然而,这种改进型的 Logistic 映射在序列遍历性和随机性特性上仍然存在一些不足,为此本文提出了一种新型的分段 Logistic 映射,并对其性能进行了仿真分析和对比。

2 Logistic 映射和改进型 Logistic 映射

Logistic 映射定义为:

$$x_{n+1}=f(x_n)=\mu \cdot x_n \cdot (1-x_n) \tag{1}$$

式中,初始值 $x_0 \in (0,1)$,μ 为映射参数,决定了系统是否工作于混沌状态。这种混沌序列理论上的相关函数很理想,但均值不为零。文献[10]提出了另一种形式的改进型 Logistic 映射。其定义为:

$$x_{n+1}=f(x_n)=1-\gamma \cdot x_n^2 \tag{2}$$

式中,$x_0 \in (-1,1)$,$\gamma \in [0,2]$。与 Logistic 映射一样,γ 的变

到稿日期:2012-04-20 返修日期:2012-08-24 本文受 2012 年西北工业大学本科毕业设计(论文)重点扶持项目,武器装备预研基金(9140A25030411HK0339)资助。

张 薇(1990-),女,主要研究方向为扩频通信,E-mail:zhangwei19900410@163.com;谢红梅(1972-),女,博士,副教授,主要研究方向为数字图像处理、雷达信号处理和成像;王保平(1964-),男,博士后,副教授,主要研究方向为雷达成像、图像处理。

化决定系统的状态。

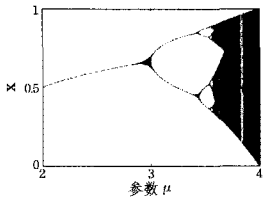


图 1　Logistic 映射分岔图

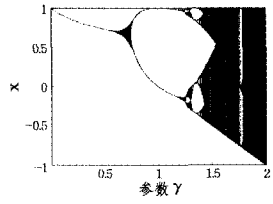


图 2　改进型 Logistic 映射分岔图

从图 1 可以看出，Logistic 映射只有在 $\mu=4$ 时，迭代结果才会映射到整个区间，称之为满映射状态。改进型 Logistic 映射的均值为零，序列的相关特性更加理想，但是图 2 表明，该映射也只有在 $\gamma=2$ 时才为满映射。这就导致在很大的参数范围内，序列迭代结果范围小，分布可能产生集中，不利于在保密通信和数据安全中对密码编制的随机性要求。为此，本文在改进型 Logistic 映射的基础上，提出一种新的定义分段 Logistic 映射。

3　分段 Logistic 映射

分段 Logistic 映射定义为：

$$x_{n+1}=f(x_n)=\begin{cases}1-4\cdot\gamma\cdot(x_n+0.5)^2, & -1\leqslant x_n<0\\ 4\cdot\gamma\cdot(x_n-0.5)^2-1, & 0\leqslant x_n\leqslant 1\end{cases} \tag{3}$$

式中，初始值 $x_0\in(-1,1)$，映射参数 γ 与序列的关系如图 3 所示。

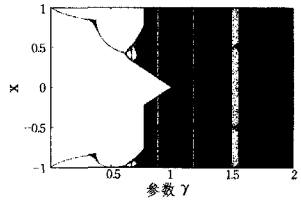


图 3　分段 Logistic 映射分岔图

对比图 3 和图 2 可以看出，这种分段 Logistic 映射比现有的改进型 Logistic 映射更快进入混沌状态。现有算法只在一个参数点是满映射，而分段 Logistic 映射在很大参数范围内都可以取到满映射，这就说明这种新算法比现有算法的遍历性更好，更适合应用在保密通信等领域。

在定义域内给定的任意初始值由式(3)迭代产生，将混沌映射的生成序列$\{a_1,a_2,\cdots,a_n\}$按式(4)转化：

$$b_i=\begin{cases}0, & -1\leqslant a_i<0\\ 1, & 0\leqslant a_i\leqslant 1\end{cases} \tag{4}$$

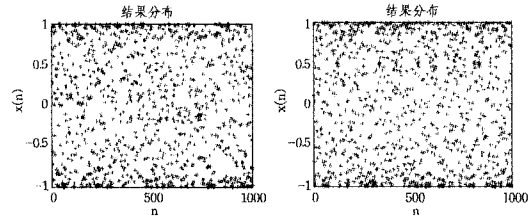
由此得到了二值序列$\{b_i\}$。将此二值序列$\{b_i\}$作为扩频通信系统中的扩频码对其性能进行进一步的分析。

4　实验仿真及分析

4.1　混沌序列特性分析

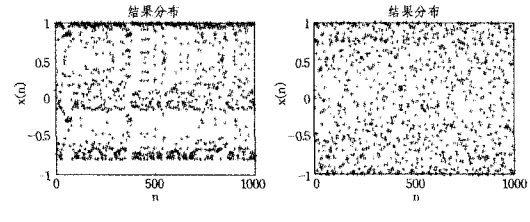
4.1.1　随机性

取 $\gamma=2$ 检验分段 Logistic 映射与现有的改进型 Logistic 映射生成序列的结果分布情况，如图 4(a)所示，两种映射的生成序列在其所对应的取值范围内均可看作是近似均匀的随机分布。取 $\gamma=1.8$ 再次检验，得到图 4(b)的结果，显然现有的改进型 Logistic 映射已不再是均匀的随机分布，而是形成一个带状区域，这就再次证明了现有算法在 $\gamma\neq 2$ 时，迭代结果分布集中，不利于保密通信。而分段 Logistic 映射很好地避免了这个问题。



改进型 Logistic 映射　　分段 Logistic 映射

(a)$\gamma=2$



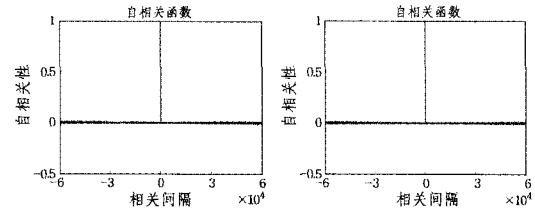
改进型 Logistic 映射　　分段 Logistic 映射

(b)$\gamma=1.8$

图 4　两种映射的生成序列分布

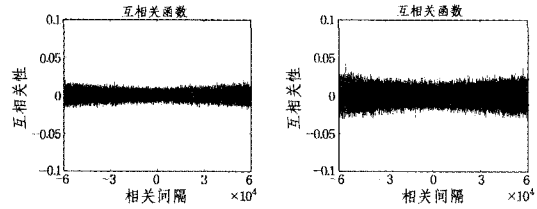
4.1.2　相关性

在扩频通信中最主要的性能就是自相关的旁瓣值、互相关系数及相关间隔为零时的自相关系数[11]。图 5 表明，改进型 Logistic 映射和分段 Logistic 映射的自相关特性是较为理想的 δ 函数，互相关性接近 0，即这两种映射具有很好的相关特性。



改进型 Logistic 映射　　分段 Logistic 映射

(a)自相关特性



改进型 Logistic 映射　　分段 Logistic 映射

(b)互相关特性

图 5　两种映射的相关特性

4.1.3　初值敏感度

以映射生成二值序列的初值发生微小变化后，采用所得到的新序列和原序列的位变化率 η 来衡量映射对初值的敏感程度，如表 1 所列。

为进一步研究两种序列的初值敏感度，采用混沌映射的分岔迭代次数作为另一种判断指标，即不同初始条件的两个序列，对应位差值大于阈值的最小迭代次数[12]。

表 1　两种映射的位变化率

变化前的初值	变化后的初值	改进型映射的 η	分段映射的 η
−0.8	−0.800001	0.4889	0.5025
−0.6	−0.600001	05066	0.4961
−0.4	−0.400001	0.4982	0.5042
−0.2	−0.200001	0.5087	0.5037
0.2	0.200001	0.5022	0.5001
0.4	0.400001	0.5004	0.4961
0.6	0.600001	0.4952	0.4979
0.8	0.800001	0.5029	0.5005

表 1 结果表明，尽管初值的变化率仅为 10^{-5}，两种映射的位变化率都接近 50%，对初始值都很敏感。从表 2 中可以看到，阈值一定时，分段 Logistic 映射的分岔迭代次数明显小于现有的改进型 Logistic 映射，即新算法的分岔速度比现有算法要快得多，说明在保密应用中这种分段 Logistic 映射会更快地进入混沌状态，从而使安全性大大提高。

表 2　两种映射的分岔迭代次数

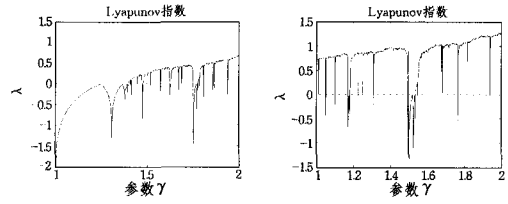
阈值	0.1	0.3	0.5	0.7	0.9
改进型映射	11.6412	13.3406	14.1725	14.5516	15.1751
分段映射	7.0417	7.9640	8.5201	8.7846	9.3103

4.1.4　Lyapunov 指数

Lyapunov 指数是衡量系统动力学特性的一个重要定量指标，它表征了系统在相空间中相邻轨道间收敛或发散的平均指数率。系统是否存在动力学混沌，可以从最大 Lyapunov 指数是否大于零直观地判断出来：一个正的 Lyapunov 指数，意味着在系统相空间中，无论初始两条轨线的间距多么小，其差别都会随着时间的演化而呈指数率增加，以致达到无法预测的结果，这就是混沌现象。指数越大，说明混沌特性越明显，混沌程度越高。若 Lyapunov 指数小于零，则意味着相邻点最终要靠拢合并成一点，这对应于稳定的不动点和周期运动。对于特定的混沌映射 $x_{n+1}=f(x_n)$，其 Lyapunov 指数 λ 定义为式(5)[13]：

$$\lambda=\lim_{N\to\infty}\frac{1}{N}\sum_{i=0}^{N-1}\ln f'(x_i) \tag{5}$$

下面分别计算现有的改进型 Logistic 映射和分段 Logistic 映射的 Lyapunov 指数。如图 6 所示，两种映射均具有稳定的混沌状态，同时可以看出分段 Logistic 映射要比现有的改进型 Logistic 映射更早地进入混沌状态，Lyapunov 指数也更大，这就说明这种新算法比现有算法的轨迹更不稳定，混沌度更大，预测难度更大，更安全。



改进型 Logistic 映射　　分段 Logistic 映射

图 6　两种映射的 Lyapunov 指数

4.2　扩频通信应用仿真

为进一步说明分段 Logistic 映射在实际应用中依然具有很好的性能，以下将采用扩频通信中的直接序列扩频(DDSS)方式[15]，分别用 Logistic 映射、改进型 Logistic 映射和分段 Logistic 映射生成的二值序列作为扩频码进行图像传输。其原理如图 7 所示，在扩频部分，首先将灰度图像二进制化，经 BPSK 调制后被混沌序列调制，产生扩频信号。在信号传输过程中采用高斯通道(设置信道的信噪比为 5dB)，扩频信号在通过此信道时会出现多径衰减，功率衰减，从而导致信噪比下降。在解扩部分，利用同步扩频码对扩频信号进行解扩，把宽带信号恢复到很窄的频带内，再用 BPSK 解调，从而恢复为基带信号，即原始的二进制信息，继而可以恢复出原始的灰度图像。

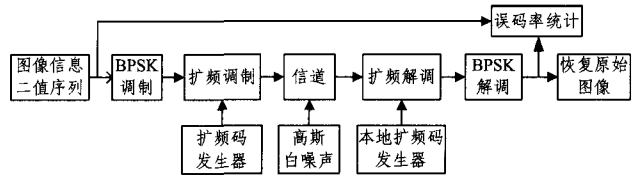


图 7　直接扩频原理图

通过图 8 的 MATLAB 模型仿真系统进行扩频通信，结果如图 9 所示，在相同的条件下，3 种序列都能较理想地恢复出原始图像，但显然新的分段 Logistic 映射比前两种恢复出来的图像更接近原始图像。

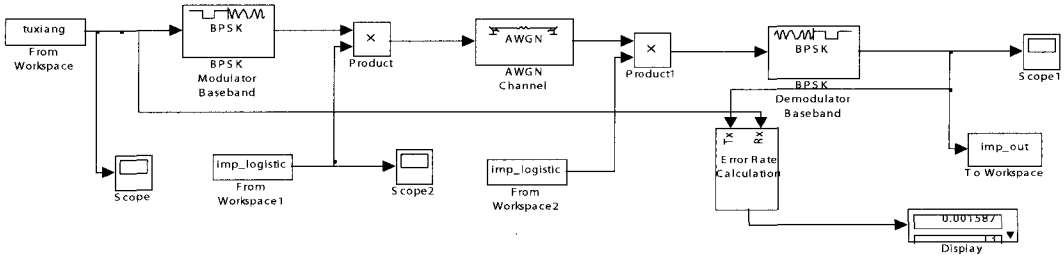


图 8　仿真系统

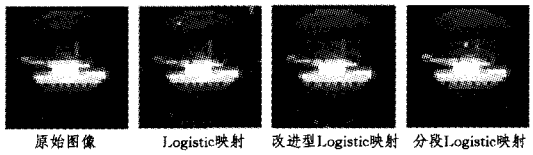


图 9　3 种扩频码恢复的图像

在图 8 的仿真系统中进一步计算恢复后的信息与原始信息的误码率，可以看出，Logistic 映射的误码率是 0.2808%，现有的改进型 Logistic 映射的误码率为 0.2197%，分段 Logistic 映射的误码率为 0.1587%，即平均传输 1000 个码字 3 种序列都只有 2 个左右错误码字；同时，分段 Logistic 映射比 Logistic 映射和现有的改进型 Logistic 映射的误码率分别降低了 43.383%和 27.765%，从而更好地保证了图像传输的完整性和可靠性。

另一方面，图像传输中如果信息被截获，在相同信噪比(5dB)下，接收端以与发射端 10^{-5} 的微小差异进行解扩，破译出来的结果如图 10 所示。

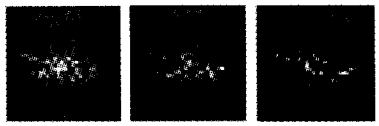


图 10　3 种扩频码被破译的图像

从图 10 中可以看到，在图像传输过程中信息被截获，3 种序列所恢复出来的图像都已经严重失真，而且很明显分段 Logistic 映射比前两种映射恢复出来的图像更加偏离真实图像。这就表明，这种分段 Logistic 映射比现有的改进型 Logistic 映射具有更好的安全性。

结束语　Logistic 映射是目前经常使用的一种混沌系统，具有较好的性能。在此基础上的改进型 Logistic 映射完善了均值和相关特性，使混沌序列能更好地应用于扩频通信中，但同时也存在一些不足。本文在改进型 Logistic 映射基础上提出一种新的分段 Logistic 映射，并与现有的改进型进行对比，其性能在很多方面都得到改进。将其用于扩频通信中也可以得到更优的结果。这些实验都表明，分段 Logistic 映射可以具有更加广泛的应用。

参 考 文 献

[1] 邱劲，王平，肖迪，等. 基于混沌映射的伪随机序列发生器 [J]. 计算机科学，2011，38(10)：81-83

[2] 廖旎焕，高金峰. 广义映射混沌扩频序列及其特性分析 [J]. 电子与信息学报，2006，28 (7)：1255-1257

[3] Mazzini G，Setti G，Rovatti R. Chaotic complex spreading sequences for asynchronous DS-CDMA Part2：Some theoretical performance bounds [J]. IEEE Transactions on Circuits and Systems Part1，1998，45(4)：496-506

[4] 杨吉云，廖晓峰，肖迪，等. 对一种基于 Logistic 映射的分组加密机制的分析和改进 [J]. 通信学报，2008，29(12)：86-90

[5] 郑世慧，张国艳，杨义先，等. 基于混沌的带密钥散列函数安全分析 [J]. 通信学报，2011，32(5)：146-152

[6] Heidari-Bateni G，Mcgillem C D. A chaotic direct-sequence spread-spectrum communication system [J]. IEEE Transactions on Communications，1994，42(2-4)：1524-1527

[7] Mazzini G，Setti G，Rovatti R. Chaotic complex spreading sequences for asynchronous DS-CDMA Part1：System modeling and results [J]. IEEE Transactions on Circuits and Systems Part1，1997，44(10)：937-947

[8] Mazzini G，Setti G，Rovatti R. Chaotic complex spreading sequences for asynchronous DS-CDMA Part2：Some theoretical performance bounds [J]. IEEE Transactions on Circuits and Systems Part1，1998，45(4)：496-506

[9] Parlitz U，Ergezinger S. Robust communication based on chaotic spreading sequences [J]. Physics Letters，1994，A188：146-150

[10] 王亥，胡健栋. 改进型 Logistic-Map 混沌扩频序列 [J]. 通信学报，1997，8(8)：71-77

[11] Sandoval-Morantes D，Munoz-Rodiguez D. Chaotic sequences for multiple access [J]. Electronics Letters，1998，34(3)：235-237

[12] 范九伦，张雪峰. 分段 Logistic 映射及其性能分析 [J]. 电子学报，2009，4(4)：720-725

[13] 赖建文，周世平，李国辉，等. 非正交的李雅普诺夫指数的计算方法 [J]. 物理学报，2000，49(12)：2328-2332

[14] 柳平，闫川，黄显高. 改进的基于 Logistic 映射混沌扩频序列的产生方法 [J]. 通信学报，2007，28(2)：134-140

[15] 徐远明，邵玉斌. MATLAB 仿真在通信与电子工程中的应用 [M]. 西安：西安电子科技大学出版社，2009

(上接第 32 页)

结束语　本文为异步休眠传感器网络设计了高效的 MAC 层广播协议。该协议能较好地应对广播报文的冲突，并且大幅降低广播能耗。为达到这两个目标，以随机变化的间隔多次重传广播数据，使得广播报文易于从冲突中区分，降低了广播报文的收发代价。我们在 NS-2 模拟环境中进行了深入的实验。结果验证，本协议在降低广播报文冲突、减小能耗方面有优越的性能。

参 考 文 献

[1] Demirkol I，Ersoy C，Alagoz F. MAC protocols for wireless sensor networks：a survey [J]. IEEE Communications Magazine，2006，44(4)：115-121

[2] MICAz motes[OL]. http://www.memsic.com

[3] Ye W，Heidemann J，Estrin D. Medium access control with coordinated adaptive sleeping for wireless sensor networks [J]. IEEE/ACM Transactions on Networking，2004，12(3)：493-506

[4] Ye W，Silva F，Heidemann J. Ultra-low duty cycle mac with scheduled channel polling[C]//Proceedings of the 4th International Conference on Embedded Networked Sensor Systems. 2006：321-334

[5] Polastre J，Hill J，Culler D. Versatile low power media access for wireless sensor networks[C]//Proceedings of the 2nd International Conference on Embedded Networked Sensor Systems. 2004：95-107

[6] Moon S，Kim T，Cha H. Enabling low power listening on IEEE 802.15.4-based sensor nodes[C]//Proceedings of IEEE Wireless Communications and Networking Conference. 2007：2305-2310

[7] Buettener M，Yee G，Anderson E，et al. X-MAC：a short preamble mac protocol for duty-cycled wireless sensor networks[C]//Proceedings of the 4th International Conference on Embedded Networked Sensor Systems. 2006：307-320

[8] Dutta P，Dawson-Haggerty S，Chen Y，et al. Design and evaluation of a versatile and efficient receiver-initiated link layer for low-power wireless[C]//Proceedings of the 8th International Conference on Embedded Networked Sensor Systems. 2010：1-14

[9] Römmer K. Time synchronization in ad hoc networks[C]//Proceedings of the 2nd ACM Interational Symposium on Mobile Ad Hoc Networking and Computing. 2001：173-182

[10] Sundararama B，Buy U，Kshemkalyani A D. Clock synchronization for wireless sensor networks：a survey[J]. Elsevier Ad Hoc Network Journal，2005，3(3)：281-323

[11] 赵强利，蒋艳凰，徐明. 无线传感器网络路由协议的分析与比较 [J]. 计算机科学，2009，36(2)：35-41

[12] McCanne S，Floyd S. ns Network Simulator[OL]. http://www.isi.edu/nsnam/ns/