

论文

一种混沌多相伪随机序列

胡汉平, 刘双红, 王祖喜, 吴晓刚

图像信息处理与智能控制教育部重点实验室 华中科技大学图像识别与人工智能研究所 武汉 430074

摘要:

提出了一种混沌多相伪随机序列生成方法, 推导出通过Logistic映射产生独立同分布多相序列的充分条件, 即根据混沌轨迹的概率密度分布把混沌吸引子划分为2n个区域, 对混沌轨迹进行采样间隔为n的采样, 对照轨道点所处位置与相应的序列元素之间的映射关系, 可以得到独立、均匀分布的2n相伪随机序列。数值统计分析支持以上研究结果并表明该序列具有较高的复杂度。此外文中给出了该序列生成的快速算法和一般表达式。该序列可用于信息安全、扩频通信等众多领域。

关键词: 多相序列;混沌;独立性

分类号:

65C; 94A

A Chaotic Poly phase Pseudorandom Sequence

HU Han-Ping, LIU Shuang-Hong, WANG Zu-Xi, Wu Xiao-Gang

Abstract:

A method based on Logistic map to generate poly phase (2n phases) sequence proposed in this paper. It gives the sufficient condition for this map to produce an independent and identically distributed (i.i.d) poly phase pseudo r andom (PN) sequence. The theoretical and numerical analyses show that the sequen ce also has a high complexity. It gives a fast algorithm to generate this sequence and general expression of the sequence in the paper too. The sequence can be used in fields such as information security and spread spectrum communication.

Keywords: Information security;Poly phase sequence;Chaos;Ind ependence

收稿日期 修回日期 网络版发布日期

DOI:

基金项目:

国家自然科学基金重大研究计划(90104029)、 “十五” 期间国家密码理论发展基金资助

通讯作者:

作者简介:

参考文献:

[1]Lasota A, Mackey M C. Chaos, Fractals and Noise. New York: Springer Verlag, 1994

[2]Matthews R A J. On the derivation of a “chaotic” encryption algorithm.Cryptologia,1989, 13:29-42

[3]Mitchell D E. Nonlinear Key Generators. Cryptologia, 1990,14:350-354

[4]Fukumasa H, Kohno R, Imai H. Design of pseudonoise sequences with good od d and even correlation

扩展功能

本文信息

▶ Supporting info

▶ PDF(360KB)

▶ [HTML全文]

▶ 参考文献

服务与反馈

▶ 把本文推荐给朋友

▶ 加入我的书架

▶ 加入引用管理器

▶ 引用本文

▶ Email Alert

▶ 文章反馈

▶ 浏览反馈信息

本文关键词相关文章

▶ 多相序列;混沌;独立性

本文作者相关文章

▶ 胡汉平

▶ 刘双红

▶ 王祖喜

▶ 吴晓刚

PubMed

▶ Article by Hu, H. B.

▶ Article by Liu, S. G.

▶ Article by Wang, J. C.

▶ Article by Tun, X. G.

[5]Kohda T, Tsuneda A. Statistics of chaotic binary sequences. IEEE Tran On Information Theory, 1997,43(1): 105-112

[6]Torhu Kohda, Akio Tsuneda. Pseudonoise sequences by chaotic nonlinear map s and their correlation properties. IEICE Commun, 1993,E76-B(8): 855-862

[7]Andreyev Y, Dmitriev A S, Kuminov D, Starkov S. Maps with stored informat ion in multiple access communications systems. NDES'97: Communication:185-190

[8]肖国镇, 梁传甲, 王育民. 伪随机序列及其应用. 北京: 国防工业出版社, 1985

[9]胡健栋, 郑朝晖, 龙必起, 李兴明. 码分多址与个人通信. 北京: 人民邮电出版社 1996

[10]凌聪, 孙松庚.用于CDMA的四相混沌扩频序列.通信学报,1998,19 (3):40-44

[11]Hammons R A, Kumar V P. On a recent 4 Phase sequence design for CDMA. IEICE Trans Commun, 1993,E76-B(8):804-813

[12]郝柏林.从抛物线谈起—混沌动力学引论. 上海: 上海科技教育出版社, 1993

[13]Gonzalez J A, Pino R. Chaotic and stochastic functions. Physica A, 2000 , 276:425-432

本刊中的类似文章

文章评论 (请注意:本站实行文责自负, 请不要发表与学术无关的内容!评论内容不代表本站观点.)

反馈人	<input type="text"/>	邮箱地址	<input type="text"/>
反馈标题	<input type="text"/>	验证码	<input type="text"/> 9205