基于线性反馈移位寄存器和组合猫映射的伪随机序列生成方法

肖旭韬, 张雪锋
(西安邮电大学 通信与信息工程学院, 西安 710061)

摘　要: 分析了线性反馈移位寄存器(LFSR)和猫映射的基本结构,给出了一种基于 LFSR 与猫映射的伪随机序列生成方法。该方法根据 LFSR 的计算结果产生相应的选择函数,通过选择函数确定当前迭代计算中猫映射的系数矩阵;应用选定的系数矩阵进行迭代计算产生相应的混沌序列,将其二值化后作为反馈值与 LFSR 的反馈值进行异或运算,运算结果作为 LFSR 的最终反馈值,实现对 LFSR 生成序列的随机扰动。通过实验对生成序列的性能进行了分析,结果表明,产生的混沌序列具有良好的随机性和安全性。

关键词: 线性反馈移位寄存器; 猫映射; 伪随机序列; 混沌; 随机性
中图分类号: TP311.56　　**文献标志码**: A　　**文章编号**: 1001-3695(2013)01-0161-04
doi:10.3969/j.issn.1001-3695.2013.01.041

Pseudo-random sequence generation method based on LFSR and combination cat map

XIAO Xu-tao, ZHANG Xue-feng
(*School of Communication & Information Engineering, Xi' an University of Posts & Telecommunications, Xi' an* 710061, *China*)

Abstract: This paper analyzed the basic structure of LFSR and cat map, and presented a pseudo-random sequence generating method based on LFSR and cat map. The presented method generated the corresponding selection function according to the calculating results of LFSR, determined the cat map's coefficient matrix in current iterative calculation by selection function adopting the selected map matrix and then to generate the corresponding chaotic sequence by iterative calculation. Binarized it as feedback value and LFSR's feedback value to conduct exclusive or operation, took the operation result as the final feedback value, these process achieved the random perturbation on LFSR generating sequence. It analyzed the generated pseudo-random sequence by experiments. The results show that the generated sequences have better characteristics of randomness and security.

Key words: linear feedback shift register(LFSR); cat map; pseudo-random sequence; chaos; randomness

0　引言

随着信息技术的飞速发展和普及,人们对信息安全问题日益关注。由于混沌良好的伪随机性、初值敏感性和遍历性等特点,同时具有确定的可再生性质[1],使得混沌保密技术已经被广泛应用到数据安全和保密通信等众多研究领域[2~4],其中基于混沌理论的伪随机序列生成技术成为重要的研究方向[5~7]。

流密码又称序列密码,是现代密码的一种重要加密技术。流密码具有安全性高、长度灵活可变、运算速度快、密文传输中没有差错或只有有限的错误传播等优点,目前已被广泛应用于信息加密、分布式计算、码分多址(CDMA)系统等领域。伪随机序列生成技术及其性能评价方法是实现流密码的关键技术,设计良好的伪随机序列发生器(pseudo-random number generator,PRNG)成为流密码领域的一个研究热点[8~10]。LFSR(线性反馈移位寄存器)是设计实现密钥流生成器的核心部件,其由移位寄存器和反馈函数构成,具有原理简单、计算速度快、便于硬件实现等优点。

目前,将 LFSR 和混沌理论相结合来设计生成伪随机序列的研究方面,已取得了一些成果。文献[11]设计了一种结合分段线性混沌映射和 LFSR 的流密码方案,加密过程采用自同步加密结构,应用分段线性混沌映射产生的序列与 LFSR 产生的 m 序列进行简单的异或运算,将所得结果应用于流密码,其不足是 LFSR 的短周期问题依然存在。文献[12]提出了一种基于 LFSR 和多个简单混沌系统相结合的伪随机序列生成方法。该方法通过 LFSR 产生选择函数对当前迭代计算的混沌系统进行选择,并将生成的序列进行二值化,再与 LFSR 的反馈值进行异或运算,实现对 LFSR 的随机扰动,但其在迭代计算时,需要对多个不同结构的混沌系统进行选择,计算过程复杂,不便于硬件实现。文献[13]给出了一种基于一维 Logistic 映射和二维 Henon 映射,用交错变参 Logistic 映射的混沌迭代值的汉明重量来控制 Henon 映射输出的迭代分量,克服了因计算机有限精度效应产生的混沌退化问题,但其增加了混沌映射的计算复杂度,使得对生成序列的理论分析更加困难,且不便于硬件实现。

收稿日期: 2012-06-04; **修回日期**: 2012-07-28

作者简介: 肖旭韬(1987-),男,硕士研究生,主要研究方向为随机序列分析(xxt_19@163.com);张雪锋(1975-),男,副教授,硕导,主要研究方向为随机序列分析、图像加密.

本文给出一种基于 LFSR 和组合猫映射的伪随机序列生成方法,该方法采用 LFSR 产生选择函数来确定猫映射的系数矩阵,通过循环迭代结构生成相应的伪随机序列。鉴于 LFSR 和组合猫映射相结合具有较大的密钥空间,采用 LFSR 产生选择函数来确定组合猫映射的系数矩阵,增加了密码分析攻击的难度。在本文方法的计算过程中,对迭代过程生成的伪随机序列进行二值化,将得到的二值序列与 LFSR 的反馈值进行异或运算,通过此种方式实现对 LFSR 的随机扰动,使得生成的序列具有良好的随机性和安全性。本方案的另一个优点是将一维混沌系统推广到二维空间,具体实现方式是利用组合猫映射替代了多个简单混沌系统,使得计算过程具有更高的效率,便于硬件实现。

1 猫映射与 LFSR

猫映射最早由 Arnold 引入[14],其二维映射形式可以表示为

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} \bmod 1 \tag{1}$$

其中:mod 1 表示只取 x 的小数部分,即 $x \bmod 1 = x - \lfloor x \rfloor$。因此$(x_n, y_n)$的相空间限制在单位正方形$[0,1] \times [0,1]$内。定义矩阵 $\boldsymbol{C} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix}$,可知行列式 $|\boldsymbol{C}| = 1$,因此,猫映射是一个二维保面积、可逆映射。

如图 1 所示,猫映射包括拉伸(乘以矩阵 $\boldsymbol{C}$,使 x、y 都变大)和折叠(取模,使 x、y 又折回单位矩形内)两个过程。猫映射系数矩阵 $\boldsymbol{C}$ 的特征值分别为 $\sigma_1 = \frac{3+\sqrt{5}}{2} > 1, \sigma_2 = \frac{3-\sqrt{5}}{2} < 1$,相应的 Lyapunov 指数 $\lambda_1 = \ln(\frac{3+\sqrt{5}}{2}) > 0, \lambda_2 = \ln(\frac{3-\sqrt{5}}{2}) < 0$,因此该系统是混沌的。

式(1)定义的猫映射可以推广为一般的二维可逆保面积方程:

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} \bmod N \tag{2}$$

式中:a、b、c、d 为正整数,矩阵 $\boldsymbol{C} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$,其保面积的性质要求

$$|\boldsymbol{C}| = ad - bc = 1 \tag{3}$$

反馈移位寄存器(feedback shift register),特别是线性反馈移位寄存器[6],是设计实现密钥流生成器的基本器件。LFSR 的基本构如图 2 所示,其中 $f(a_1, a_2, \cdots, a_n)$ 为反馈函数,当反馈函数为线性函数时,相应的反馈移位寄存器被称为线性反馈移位寄存器。

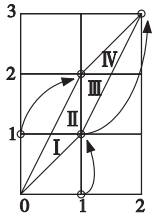


图1 猫映射示意图

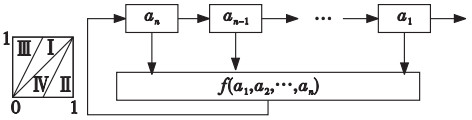


图2 反馈寄存器的基本结构

2 基本原理

基于 LFSR 与混沌系统生成伪随机序列的基本流程如图 3 所示。

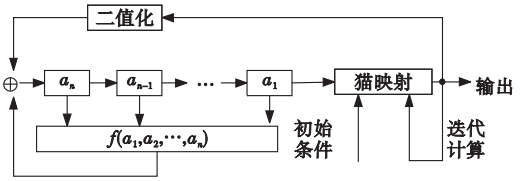


图3 伪随机序列生成的基本流程

伪随机序列的生成过程如下:

a)根据 LFSR 的计算结果产生相应的选择函数,通过选择函数确定当前迭代计算使用的组合猫映射的系数矩阵。

b)应用选择的系数矩阵进行迭代计算,产生相应的伪随机序列,将其作为伪随机序列输出。

c)将生成的伪随机序列输出的同时,将其二值化后作为反馈值与 LFSR 的反馈值进行异或运算,运算结果作为 LFSR 的最终反馈值。该过程实现对 LFSR 生成序列的随机扰动。

以上迭代计算过程中,反馈机制的二值化过程可以采用二值量化法来实现。对于混沌序列(x_i, y_i),$i = 1, 2, \cdots, N$,定义二值化结果为

$$y_i = \begin{cases} -1 & x_i > y_i \\ 1 & x_i \leqslant y_i \end{cases} \tag{4}$$

采用上述方法生成伪随机序列具有以下优点:

a)通过 LFSR 产生选择函数来确定猫映射系数矩阵的方式,增加了密码分析攻击的难度,使得生成的伪随机序列具有良好的安全性。

b)计算过程中,将二值化后的序列对 LFSR 进行随机扰动,使得生成的伪随机序列具有良好的随机性。

c)采用同一混沌系统的不同参数进行循环迭代计算能够保证该方法具有较大的密钥空间,并降低了计算过程的复杂度。

d)可以将组合猫映射扩展到多维空间,在不影响序列产生速率的前提下,扩大了密钥空间,提高了生成序列的安全性,且便于硬件实现。

3 性能分析

本节以 $f(D) = 1 + D^2 + D^3$ 为反馈函数的 4 阶 LFSR 来产生相应的选择函数,以系数矩阵为$\begin{bmatrix} 1 & a \\ b & ab+1 \end{bmatrix}$的猫映射作为循环迭代计算的混沌系统,对本文提出的伪随机序列生成方式进行性能分析。

3.1 相关性分析

设二值序列 b_n 的长度为 N,则该序列的自相关系数定义为[15]

$$ac(m) = \frac{1}{N} \sum_{i=1}^{N-m} b_i b_{i+m} \tag{5}$$

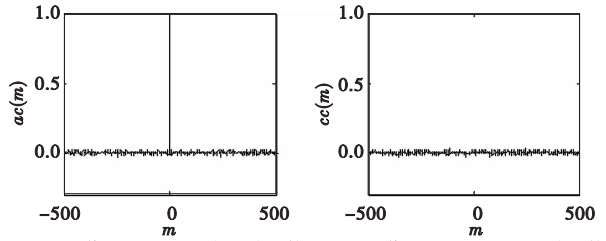
其中,m 为步长参数。自相关系数的值与步长 m 有关,当步长变化时,如果自相关系数变化越小,说明对应序列的随机性越好。

假设不同的两个二值序列 b_{1n} 和 b_{2n} 的长度均为 N,则相应

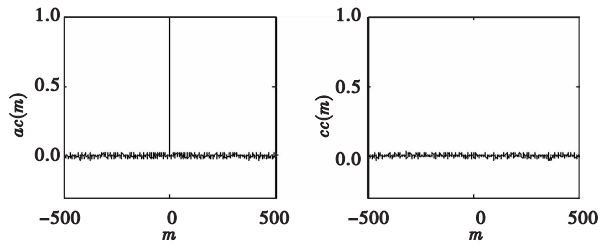
的互相关函数定义为

$$ac(m)=\begin{cases}\dfrac{1}{N}\sum_{i=1}^{N-m}b_{1i}b_{2(i+m)}\\ \dfrac{1}{N}\sum_{i=1}^{N-m}b_{1(i+m)}b_{2i}\end{cases}\tag{6}$$

互相关函数取值越接近 0,说明两个序列越互不相关,差异程度越大。自相关系数和互相关系数分析的实验结果如图 4 所示。



(a) 初值为(x_1,y_1)时的自相关函数　(b) 初值为(x_1,y_1)时的互相关函数



(a) 初值为(x_2,y_2)时的自相关函数　(b) 初值为(x_2,y_2)时的互相关函数

图4　不同初值相关性分析

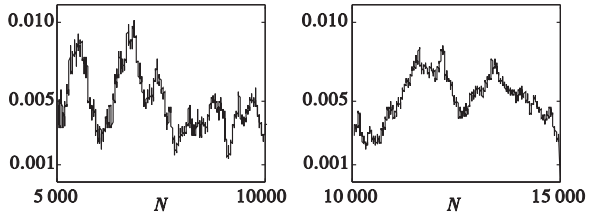
本文通过选择不同的初值进行了大量实验,结果表明,初值对产生的二值序列的相关性没有显著影响,几乎任意初值产生的伪随机序列均具有良好的相关性。这表明本文方法生成序列的随机性能良好。

3.2　平衡度分析

设扩频序列的长度为 N,序列中 −1 与 1 的个数分别为 P 和 Q,则该扩频序列的平衡度定义为[15]

$$E(N)=\frac{|P-Q|}{N}\tag{7}$$

平衡度的值越接近于零,说明序列中 −1 与 1 的个数越接近,随机性越好。图 5 给出本文方法生成序列的平衡度随序列长度变化的实验结果,其中(a)生成的伪随机序列长度从5 000 增加到 10 000,(b)生成的伪随机序列长度从 10 000 增加到 15 000。



(a) 序列长度从5 000到10 000的平衡度　(b) 序列长度从10 000到15 000的平衡度

图5　平衡度分析

图 5 的实验结果表明,应用本文方法产生的伪随机序列随着序列长度 N 的增加而逐步减小,具有良好的平衡度。

3.3　游程统计

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 1 的个数称为游程长度。随机序列中长度为 L 的游程大致占游程总数的$\frac{1}{2^L}$,且任意长度的 0 游程个数和 1 的游程个数相等[16]。在表 1 中统计了序列长度为 200 000 时,本文方法产生的伪随机序列中游程长度分别为 1 ~ 10 的游程数占游程总数的比值。

表 1　输出序列的游程统计

游程长度	0	1	0/1	测试值	理论值
1	24867	24793	1.0030	0.4985	0.5000
2	12477	12564	0.9931	0.2514	0.2500
3	6322	6178	1.0233	0.1255	0.1250
4	3062	3136	0.9764	0.0622	0.0625
5	1596	1540	1.0364	0.0315	0.0313
6	753	818	0.9205	0.0158	0.0156
7	392	415	0.9446	0.0081	0.0078
8	183	204	0.8971	0.0039	0.0039
9	109	96	1.1354	0.0021	0.0020
10	50	67	0.7463	0.0012	0.0010

从表 1 可以看出,不同长度的游程中,游程 0 和 1 的个数大致相等。本文方法产生的伪随机序列具有良好的游程特性。

3.4　初值敏感性分析

初值敏感性分析过程中,本文对混沌系统的初始条件进行微小变化,通过计算得到的两个伪随机序列的位变化率来评价系统的初值敏感性。位变化率定义如下[17]:

$$T=\frac{n'}{N}\tag{8}$$

其中:N 为序列长度,n' 为初始条件进行微小改变后生成的二值序列与原序列比较时,对应位置取值发生改变的位的个数。位变化率越接近 50%,说明该系统对于初始条件越敏感。

以下实验中的序列长度均为 $N=100000$。表 2 分别给出当反馈移位寄存器的初始状态和混沌系统的初始条件分别发生微小变化时,生成的二值序列的位变化率。结果表明,本文方法对线性反馈移位寄存器的初始状态和组合猫映射的初始条件均具有良好的敏感性。因为当初始值发生微小变化时,所生成的伪随机序列中均有约 50% 的位的取值发生了变化,很接近理想状态下对初始条件的敏感性要求。这里 S 表示反馈移位寄存器的初始状态,(X,Y) 表示组合猫映射的初始条件。

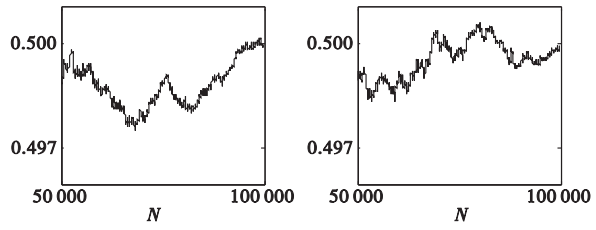
表 2　初值敏感性分析

初始条件	初始值	变化后的初始值	位变化率/%
S	$(1001)_2$	$(1001)_2$	49.98
(X,Y)	(0.4,0.2)	(0.3999999999,0.2000000000)	
S	$(1001)_2$	$(1001)_2$	49.80
(X,Y)	(0.4,0.2)	(0.4000000000,0.2000000001)	
S	$(1001)_2$	$(1001)_2$	50.01
(X,Y)	(0.4,0.2)	(0.3999999999,0.2000000001)	
S	$(1001)_2$	$(1001)_2$	50.33
(X,Y)	(0.4,0.2)	(0.4000000000,0.2000000000)	

根据表 2 的结果可知,当反馈寄存器的初始条件 S 或者组合猫映射的初始条件 (X,Y) 发生微小改变时,生成二值序列的位变化率均非常接近理想状态的 50%。

图 6 的实验结果表明,随着生成序列的长度增加,相应的位变化率也随着生成序列的长度产生变化,但是位变化率总体趋于 50%。说明应用本文所给方法生成的序列具有良好的初值敏感性。

分析本文方法产生的实值序列与猫映射产生的实值序列的分叉情况。相应的实验结果如图 7 和 8 所示,其中空心点表示猫映射生成的实值序列分布情况,实心点表示本文方法生成的实值序列分布情况。本文的方法中,猫映射系数矩阵的值分别取 $C_1=\begin{pmatrix}1 & a_1\\ b_1 & a_1b_1+1\end{pmatrix}$ 和 $C_2=\begin{pmatrix}1 & a_2\\ b_2 & a_2b_2+1\end{pmatrix}$。



(a) 初值为(x_1,y_1)时的位变化率 (b) 初值为(x_2,y_2)时的位变化率

图6 初值敏感性分析

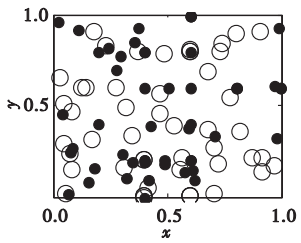


图7 本文方法（实心点）和系数矩阵取值为C_1的猫映射分叉情况

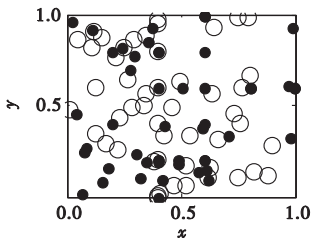


图8 本文方法（实心点）和系数矩阵取值为C_2的猫映射分叉情况

图 7 和 8 的实验结果表明，初始条件相同时，本文方法生成序列相比应用猫映射所产生的序列出现了明显的分叉，说明两种方法产生的序列并不相同。图 9 的实验结果表明，当初始条件发生微小变化时，应用本文方法生成的序列明显出现了分叉，说明本文的方法对初值具有良好的敏感性。

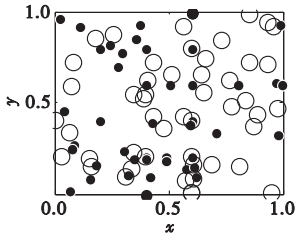


图9 本文初值敏感性分析

为了更好地研究混沌映射的初值敏感性问题，文献[17]提出了一种一维混沌序列初值敏感性量化评价指标——分叉迭代次数。该指标量化地评价了混沌系统初始条件微小改变对序列轨迹的影响程度。本文借鉴分叉迭代次数的定义，提出评价高维混沌序列初值敏感性的量化评价指标——距离迭代次数。

定义 1 距离迭代次数。设高维混沌系统为 $a_{n+1}=f(a_n)$，该映射对应两个不同的初始条件 a_0 和 b_0 产生的高维混沌序列分别为$\{a_1,a_2,\cdots\}$和$\{b_1,b_2,\cdots\}$，给定分叉判定阈值 δ，定义 $\Omega=\min\{i\mid D(a_i,b_i)>\delta\}$，则称 Ω 为混沌映射 $a_{n+1}=f(a_n)$对应初始条件为 a_0 和 b_0 时的距离迭代次数。

以下给出组合猫映射和本文所给出的方法对应不同分叉判定阈值所需要的平均迭代次数。在单位正方形[0,1]×[0,1]内取 100 000 个采样点，计算相邻点之间产生混沌序列所需的平均距离迭代次数。表 3 是相应的实验结果。

表 3 两种方法产生分叉所需迭代次数

方法	分叉判定阈值			
	0.2	0.4	0.6	0.8
组合猫映射	10.7268	11.3239	11.8909	13.6086
本文方法	6.7012	7.0888	7.9867	11.8828

根据表 3 的实验结果，对应相同的分叉判定阈值，组合猫映射所需的平均迭代次数明显大于本文方法所需的平均迭代次数，说明本文方法的分叉速度快于组合猫映射，从而保证了本文提出的方法在加密过程能够较快地进入稳定的混沌状态，保证了生成序列的安全性。

4 结束语

本文在混沌理论和 LFSR 的基础上，给出了一种 LFSR 和组合猫映射相结合的伪随机序列生成方法。该方法采用选择机制，循环迭代结构生成相应的伪随机序列，在每一轮迭代过程中都会对组合猫映射的系数矩阵进行选择，此种结构使得算法具有较大的密钥空间；通过生成的二值序列对 LFSR 进行随机扰动，使得生成序列具有良好的安全性和随机性；计算过程对同一混沌系统的不同参数进行循环迭代计算，降低了计算过程的复杂性，也便于硬件计算。仿真结果表明，应用本文方法产生的序列具有良好的性能。下一步将讨论多个移位寄存器与多个高维混沌系统的结合生成伪随机序列，并对其进行性能分析。

参考文献：

[1] MATTHEWS R. On the derivation of a chaotic encryption algorithm [J]. Cryptologia, 1989, 13(1): 29-42.

[2] PARKER A T, SHORT K M. Reconstructing the keystream from a chaotic encryption scheme [J]. IEEE Trans on Circuit and Systems Fundamental Theory and Applications, 2001, 48(5): 624-630.

[3] ALVAREZ G, MONTOYA F, ROMERA M, *et al*. Breaking two secure communication systems based on chaotic masking [J]. IEEE Trans on Circuits and Systems Ⅱ, 2004, 51(10): 505-506.

[4] ZHANG Han, WANG Xiu-feng, LI Zhao-hui, *et al*. A new image encryption algorithm based on chaos system [C]//Proc of International Conference on Robotics, Intelligent Systems and Signal Processing. [S.l.]: IEEE Press, 2003: 778-782.

[5] SINGH N, SINHA A. Optical image encryption using Hartley transform and logistic map [J]. Optics Communications, 2009, 282(6): 1104-1109.

[6] 张雪锋，范九伦. 基于混沌系统的伪随机序列生成方法[J]. 计算机工程与应用, 2010, 46(29): 80-82.

[7] 王福来. 基于复合符号混沌的伪随机数生成器及加密技术[J]. 物理学报, 2011, 60(11): 110-517.

[8] LI Na, QI Wen-feng. Symmetric Boolean functions depending on an odd number of variables with maximum algebraic immunity [J]. IEEE Trans on Information Theory, 2006, 52(5): 2271-2273.

[9] 任巧，戴紫彬，李伟，等. 基于流密码的可适配反馈移位寄存器指令[J]. 计算机工程, 2009, 35(4): 162-164.

[10] 高军涛，董丽华，胡予濮. 广义互缩生成器[J]. 计算机学报, 2006, 29(6): 936-943.

[11] BEHNIA S, AKHSHANI A, AKHAVAN A. A novel algorithm for image encryption based on mixture of chaotic maps [J]. Chaos, Solitons and Fractals, 2008, 35(2): 408-419.

[12] 张雪锋，范九伦. 基于线性反馈移位寄存器和混沌系统的伪随机序列生成方法[J]. 物理学报, 2010, 59(4): 2289-2297.

[13] 李孟婷，赵泽茂. 一种新的混沌伪随机序列生成方法[J]. 计算机应用研究, 2011, 28(1): 341-344.

[14] WEISSTEIN E W. Arnold's cat map [EB/OL]. (1999-12) [2005-12-30]. http://mathworld.woffram.com/ArnoldsatMap.html.

[15] 王兴元，王明军. 二维 Logistic 映射的混沌控制[J]. 物理学报, 2008, 57(2): 731-736.

[16] 陈争，曾以成，付志坚. 混沌背景中信号参数估计的新方法[J]. 物理学报, 2008, 57(1): 46-50.

[17] 范九伦，张雪锋. 分段 Logistic 混沌映射及其性能分析[J]. 电子学报, 2009, 37(4): 720-725.