分段 Logistic 混沌映射及其性能分析

范九伦[1],张雪锋[1,2]
(1. 西安电子科技大学电子工程学院,陕西西安 710071;2. 西安邮电学院信息与控制系,陕西西安 710061)

摘 要: 分析了具有逐段线性特性的 Tent 混沌映射和其推广形式:分段 Tent 混沌映射在计算机有限精度影响下的性能.在此基础上,根据 Logistic 混沌映射与 Tent 混沌映射之间具有的拓扑共轭关系,研究了 Logistic 混沌映射的推广形式:分段 Logistic 混沌映射,通过实验分析指出用类似于分段 Tent 混沌映射的方式来定义分段 Logistic 混沌映射是不可取的.本文构造了一个全新的分段 Logistic 混沌映射,通过实验对该映射产生的序列的随机性、初值敏感性等性质进行了研究.结果表明,本文定义的分段 Logistic 混沌映射产生的序列具有良好的随机性和初值敏感性.

关键词: 混沌; Tent 映射; Logsitic 映射; 分段; 随机性
中图分类号: TN914.42 **文献标识码**: A **文章编号**: 0372-2112 (2009) 04-0720-06

Piecewise Logistic Chaotic Map and Its Performance Analysis

FAN Jiu-lun[1], ZHANG Xue-feng[1,2]
(1. *School of Electronic Engineering, Xidian University, Shaanxi Xi'an 710071, China;*
2. *Department of Information and Control, Xi'an Institute of Posts and Telecommunications, Shaanxi Xi'an 710061, China*)

Abstract: For Tent map, which has piecewise-liner characteristic, and its expand form: piecewise Tent map, the performances under computer finite precision are analyzed. Based on the fact, considering the topologically conjugate relationship between Tent map and Logistic map, piecewise Logistic map, an expanded form of Logistic map is researched. It is pointed out that it is not a good way to define piecewise Logistic map using the similarly way to define piecewise Tent map. In this paper, we structure a bran-new definition of piecewise Logistic map, and study the sequence's properties generated by this chaos map, such as randomness and initial-value sensitivity. Simulation results show that the sequences generated by piecewise Logistic map is randomness and initial-value sensitivity.

Key words: chaos; Tent map; Logistic map; piecewise; randomness

1 引言

混沌是非线性确定系统由于内禀随机性而产生的外在复杂表现,是一种貌似随机的非随机现象.混沌系统表现为对初始值和系统参数的敏感性、白噪声的统计特性和混沌序列的遍历特性[1],其吸引子的维数是分维,有十分复杂的分形结构,具有不可预测性.由于混沌序列具有如此优良的密码学特性,基于混沌的保密技术已经被应用到数据安全和通信保密等众多研究领域[2~4].随着互联网的发展和广泛应用,对图像的安全保护受到人们的普遍关注.图像加密是图像保护技术之一,应用混沌系统进行图像加密是一个基本的方式,Logistic 混沌映射和 Tent 混沌映射是二个常见的用于图像加密的混沌映射.

文[5]首次给出了一种基于一维 Logistic 混沌映射和流密码技术的图像加密算法,该算法应用 Logistic 映射产生相应的伪随机序列,将得到的实数范围内的混沌序列进行简单的二值化,通过与图像灰度值进行异或运算,实现对图像的加密,这种加密思想后来得到广泛的应用.文[6]利用 Logistic 映射给出了一种混沌扩频序列生成方法,首先应用 Logistic 映射初始条件进行迭代计算,然后对每一个迭代点进行 L 比特的量化处理,通过截断操作得到新的扩频序列,该算法能够有效减少产生扩频序列的迭代次数,提高算法效率,而且可以生成任意长度的扩频序列.文[7]应用 Logistic 映射和猫映射给出了一种基于密码学中分组密码的交替结构图像加密算法,每一轮加密过程中,通过简单的密钥扩展产生两种子密钥,分别用于两个混沌映射的初始条件,该算法对密钥十分敏感,且对多种攻击手段都具有较好的免疫性.

Tent 混沌映射是一种具有逐段线性的混沌映射,文[8]对 Tent 混沌映射和 Logistic 混沌映射之间的关系进

收稿日期:2008-07-23;修回日期:2008-12-01
基金资助:国家自然科学基金(No. 60572133),陕西省自然科学研究计划项目(No. SJ08F24)

行了理论分析,得到 Tent 混沌映射和 Logistic 混沌映射满足拓扑共轭关系的结论,该结论为进一步分析这两种混沌映射之间的关系提供了理论基础. 文[9]给出了一种针对分段线性函数数字化混沌系统进行扰动的方案,该方案选择性地扩散数字化混沌系统的内部变量,以达到对整个系统的扰动,并以分段 Tent 混沌映射为例进行仿真实验,对生成的序列的性能进行了分析. 该方法被用来对分段线性映射进行随机扰动[10,11],改进使用分段线性映射产生的序列的随机性能,但是扰动过程会增加生成序列的计算量,导致算法效率的降低. 本文将指出,计算机有限精度问题会导致 Tent 混沌映射和分段 Tent 混沌映射产生的序列退化为 0 序列的现象.

鉴于 Tent 混沌映射与 Logistic 混沌映射之间存在的拓扑共轭关系,鉴于人们已经将 Tent 混沌映射扩展成分段 Tent 混沌映射,一个自然的想法是定义出与分段 Tent 混沌映射对应的分段 Logistic 混沌映射,本文的目的是给出一种合理的分段 Logistic 混沌映射的定义形式. 分段 Logistic 混沌映射是一种非线性映射,与文[9～11]提到的对分段线性函数加扰动的方法相比,分段 Logistic 混沌映射在生成混沌序列的过程中不需要增加相应的扰动过程,从而能够有效提高算法的效率. 作为一种应用,本文给出了 Logistic 混沌映射和分段 Logistic 混沌映射在图像加密中的应用.

2　Tent 混沌映射和 Logistic 混沌映射

Tent 混沌映射的定义为[11]:

$$x_{n+1}=g(x_n)=\begin{cases}\dfrac{x_n}{\alpha},0\le x_n<\alpha\\[2mm]\dfrac{1-x_n}{1-\alpha},\alpha\le x_n\le 1\end{cases}\qquad(1)$$

其中 $\alpha\in(0,1)$. 该映射具有均匀的分布函数,用该映射产生的混沌序列具有良好的统计性质. 常见的 Tent 混沌映射取参数 $\alpha=0.5$,相应的迭代公式为:

$$x_{n+1}=g(x_n)=\begin{cases}2x_n,0\le x_n<\dfrac{1}{2}\\[2mm]2(1-x_n),\dfrac{1}{2}\le x_n\le 1\end{cases}\qquad(2)$$

在公式(2)的基础上,相应的分段 Tent 混沌映射表示为[9]:

$$x_{n+1}=\begin{cases}4x_n,0\le x_n<\dfrac{1}{4}\\[2mm]2-4x_n,\dfrac{1}{4}\le x_n<\dfrac{1}{2}\\[2mm]4x_n-2,\dfrac{1}{2}\le x_n<\dfrac{3}{4}\\[2mm]4(1-x_n),\dfrac{3}{4}\le x_n\le 1\end{cases}\qquad(3)$$

公式(2)和(3)定义的 Tent 混沌映射和分段 Tent 混沌映射的函数曲线如图 1 所示.

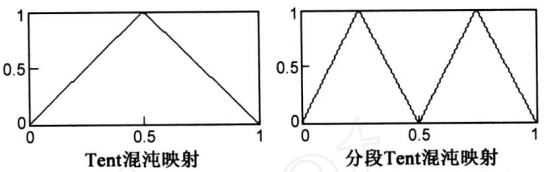

图1　Tent混沌映射与分段Tent混沌映射的函数曲线

以上定义的 Tent 混沌映射和分段 Tent 混沌映射在理论上能够产生具有良好随机性能的混沌序列. 但是用计算机实现以上迭代过程时,由于计算机的有限精度效应,产生的序列会退化为周期序列. 我们以公式(2)定义的 Tent 映射为例,给出相应的生成序列的退化速度与混沌系统初始条件之间的关系.

定理 1　对于 Tent 混沌映射,当 $\alpha=0.5$ 时,如果混沌系统的初始条件 x_0 在计算机中对应的二进制序列为 $x_0=\underbrace{(0.a_1a_2\cdots a_k000\cdots)_2}_{L\text{比特}}$,其中 $a_k=1$,则应用公式(2)的迭代过程至多经过 $k+1$ 次,计算的结果会变为 0[9].

定理 1 的结论表明,至多经过 $k+1$ 次迭代后,产生的序列必然为 0. 这种现象的出现源于计算机的有限精度效应和 Tent 混沌映射的逐段线性特点. 为了保证具有线性特性的混沌映射生成的混沌序列满足良好的随机性能,文[9]给出了一种在序列生成过程中增加扰动的解决方案,尽管该方案产生的序列具有良好的随机性能,但其缺点是生成混沌序列的过程复杂,降低了算法的执行效率.

Logistic 混沌映射由于其表达简单,随机性能良好,被广泛应用于混沌保密通信的各个领域. 该映射定义为:

$$a_{n+1}=f(a_n)=\mu\cdot a_n\cdot(1-a_n),\quad 0<a_n<1,\ n=1,2,\cdots\qquad(4)$$

其中 $3.569946\cdots\le\mu\le 4$. Logistic 混沌映射的输入和输出都分布在区间(0,1)上,当 $\mu=4$ 时,相应的 Logistic 映射定义为:

$$a_{n+1}=f(a_n)=4\cdot a_n\cdot(1-a_n),\quad 0<a_n<1,\ n=1,2,\cdots\qquad(5)$$

相比于线性关系的 Tent 混沌映射,Logistic 混沌映射是一种非线性映射. Logistic 混沌映射和 Tent 混沌映射之间存在拓扑共轭关系.

定义 1(同胚映射)　设 A 和 B 是两个拓扑空间,$f:A\to B$ 是一个连续映射,如果 f 是一一映射且 f 的逆映射连续,则称 f 为同胚映射. 如果拓扑空间 A 和 B 之间存在同胚映射,则称这两个空间是同胚的.

定义 2(拓扑共轭)　设 A 和 B 是两个拓扑空间,

$f:A\to A$, $g:B\to B$, 分别是空间 A 和 B 上的变换, 如果存在 $h:B\to A$ 是一个同胚映射, 满足 $f\cdot h=h\cdot g$, 则称变换 f 和 g 是拓扑共轭的.

定理 2 公式(2)中的映射 g 和公式(5)中的映射 f 是拓扑共轭的[8].

3 分段 Logistic 混沌映射

公式(2)定义的 Tent 混沌映射有相应的扩展: 分段 Tent 混沌映射, 分段 Tent 混沌映射保留了 Tent 混沌映射的混沌特性. 既然 Logistic 混沌映射和 Tent 混沌映射之间具有拓扑共轭关系, 因此有必要研究分段 Logistic 混沌映射. 根据分段 Tent 混沌映射的定义形式, 一个自然的想法是将分段 Logistic 混沌映射定义为:

$$a_{n+1}=\begin{cases}4\cdot\mu\cdot a_n\cdot(0.5-a_n), & 0\le a_n<0.5\\ 4\cdot\mu\cdot(a_n-0.5)\cdot(1-a_n), & 0.5\le a_n\le 1\end{cases}\tag{6}$$

其中 $3.5699456\cdots\le\mu\le 4$, $a_0\in(0,1)$. 当 $\mu=4$ 时, 定义的分段 Logistic 混沌映射的函数曲线如图 2 所示.

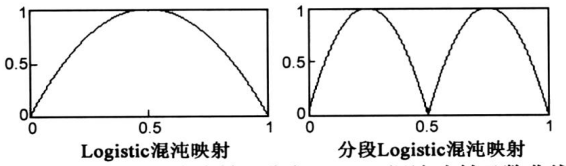

图2 Logistic混沌映射和分段Logistic混沌映射函数曲线

为了验证这种定义方式是否合理, 下面给出实验测试的结果. 图 3 给出了当 $\mu=4$, 生成序列长度为 10000 时, Logistic 混沌映射和分段 Logistic 混沌映射的序列取值分布情况.

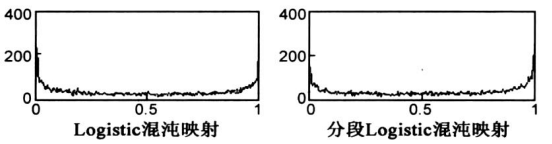

图3 两种映射生成序列分布情况

图 3 的实验结果表明, Logistic 混沌映射生成序列在(0,1)之间具有对称分布的特点, 而公式(6)定义的分段 Logistic 混沌映射生成序列在(0,1)之间分布的对称性较差.

为了进一步对以上两种映射的性能进行比较, 我们首先将生成的混沌序列转化成二值序列$\{a_1,a_2,\cdots,a_n\}$, 然后对相应的二值序列的随机性作进一步的比较分析. 序列$\{a_1,a_2,\cdots,a_n\}$对应的二值序列$\{b_1,b_2,\cdots,b_n\}$的取值如下:

$$b_i=\begin{cases}0, & 0\le a_i<0.5\\ 1, & 0.5\le a_i\le 1\end{cases},\quad i=1,2,\cdots,n$$

以下对得到的二值序列的随机性进行一系列检验.

3.1 频数检验

频数检验能够保证二值序列中 0 和 1 的个数大致相等, 这也是二值序列具有随机性的必要条件. 计算[12]:

$$\chi_1^2=\frac{(n_1-n_0)^2}{n^2}\tag{7}$$

其中 n_1 为二值序列中的 1 个数, n_0 为二值序列中的 0 个数, 与 1 自由度的 χ^2 分布比较, 对应 5 %的显著性水平, χ_1^2 的值为 3.84, 即只要得到的 χ_1^2 值不大于 3.84, 则认为二值序列具有较好的随机性.

实验结果表明, 公式(6)定义的分段 Logistic 混沌映射生成的序列虽然能够通过频数检验, 但是 χ_1^2 的取值明显大于 Logistic 混沌映射生成序列的 χ_1^2 值, 说明以上定义的分段 Logistic 混沌映射生成序列的随机性比 Logistic 混沌映射生成的序列随机性差.

表 1 两种序列频数检验结果

初始条件	Logistic 混沌映射			分段 Logistic 混沌映射		
	n_0	n_1	χ_1^2	n_0	n_1	χ_1^2
0.1	5083	4917	$2.7556e$-004	4344	5656	0.0172
0.2	4999	5001	$4.0000e$-008	4325	5675	0.0182
0.3	4982	5018	$1.2960e$-005	4325	5675	0.0182
0.4	5035	4965	$4.9000e$-005	4289	5711	0.0202

3.2 平衡度分析

设二值序列的长度为 N, 序列中 1 与 0 的个数分别为 P 和 Q, 则该二值序列的平衡度定义为[13]:

$$E(N)=\frac{|P-Q|}{N}\tag{8}$$

平衡度的值越小, 说明序列中 1 与 0 的个数越接近, 随机性越好. 以下给出 Logistic 混沌映射和公式(6)定义的分段 Logistic 混沌映射对不同初始条件生成序列的平衡度分布情况实验结果, 其中序列长度为 10000.

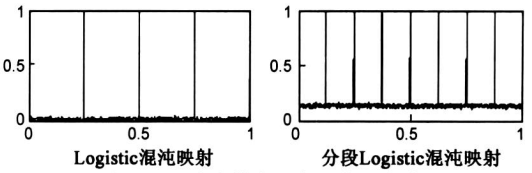

图4 两种映射生成序列的平衡度

根据实验结果可知, Logistic 混沌映射生成序列的平衡度曲线接近 0, 说明生成序列的平衡度取值接近 0, 序列具有良好的随机性; 而分段 Logistic 混沌映射生成序列的平衡度曲线离 0 较远, 说明生成序列的平衡度要大于 0. 这意味着公式(6)定义的分段 Logistic 混沌映射生成的序列的随机性比 Logistic 混沌映射生成的序列随机性差.

上述实验结果表明, 按公式(6)定义的分段 Logistic 混沌映射生成的序列尽管具有随机分布的特点, 但生成序列的随机性较差. 因此有必要重新考虑分段 Logistic 混沌映射的定义方式. 下面给出一种可行的表达式,

分段 Logistic 混沌映射定义为:

$$a_{n+1}=\begin{cases}4\cdot\mu\cdot a_n\cdot(0.5-a_n), & 0\le a_n<0.5\\ 1-4\cdot\mu\cdot(a_n-0.5)\cdot(1-a_n), & 0.5\le a_n\le 1\end{cases} \tag{9}$$

其中 $3.569946\cdots\le\mu\le 4$, $a_0\in(0,1)$. Logistic 混沌映射和分段 Logistic 混沌映射的函数曲线如图 6 所示,其中 $\mu=4$.

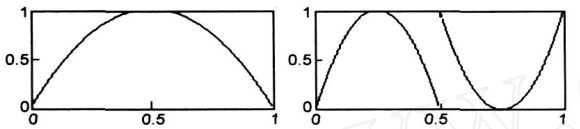

图5　两种映射的函数曲线

4　分段 Logistic 混沌映射性能分析

接下来对 Logistic 混沌映射和公式(9)定义的分段 Logistic 混沌映射生成的序列的随机性进行实验比较. 以下对这两种映射生成序列的分布情况进行实验分析,其中 $\mu=4$,生成序列长度为 10000.

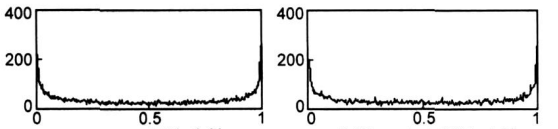

图6　两种映射生成序列分布情况

图 6 给出了两种映射产生序列取值的分布情况,实验结果表明,这两种映射生成的序列在(0,1)之间分布情况相同,均具有对称分布的特点.

4.1　随机性分析

(1)频数检验:我们对 Logistic 混沌映射和公式(9)定义的分段 Logistic 混沌映射生成的序列进行频数检验,相应的实验结果如下:

表 2　两种序列频数检验结果

初始条件	Logistic 混沌映射			分段 Logistic 混沌映射		
	n_0	n_1	χ_1^2	n_0	n_1	χ_1^2
0.1	5083	4917	2.7556e-004	5056	4944	1.2544e-004
0.2	4999	5001	4.0000e-008	5009	4991	3.2400e-006
0.3	4982	5018	1.2960e-005	5009	4991	3.2400e-006
0.4	5035	4965	4.9000e-005	4998	5002	1.6000e-007

实验结果表明,公式(9)定义的分段 Logistic 混沌映射生成的序列不仅能够通过频数检验,而且 χ_1^2 的取值与 Logistic 映射生成序列的 χ_1^2 值属于同数量级,说明公式(9)定义的分段 Logistic 混沌映射生成序列与 Logistic 混沌映射生成序列的频数检验结果等效.

(2)随机性分布

以下我们给出 Logistic 混沌映射和分段 Logistic 混沌映射分布情况的实验结果. 其中混沌系统的初始条件为 $a_0=0.34$,生成序列长度为 1000.

通过实验结果可以看出,当 $\mu=4$ 时,两种映射产生的混沌序列在(0,1)上满足近似均匀的随机分布,当 $\mu=3.7$ 时,两种映射产生的混沌序列虽然仍然满足随机分布的特点,但是 Logistic 混沌映射生成的序列分布在(0,1)之间的一个带状区域,而公式(9)定义的分段 Logistic 混沌映射生成的序列则保留了在(0,1)上满足近似均匀的随机分布的特性.

4.2　自相关性分析

设二值序列的长度为 N,则该二值序列的自相关系数定义为[13]:

$$ac(m)=\frac{1}{N}\cdot\sum_{i=1}^{N-m}b_i\cdot b_{i+m} \tag{10}$$

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,说明对应二值序列的随机性越好.

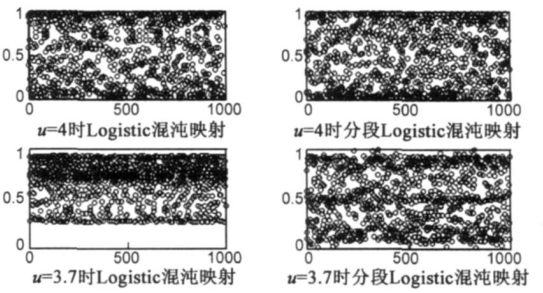

图7　两种映射产生序列分布情况

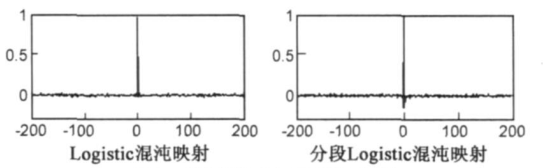

图8　扩频序列自相关性分析

实验结果表明,当步长参数 $m\neq 0$ 时,两种映射产生的二值序列的自相关系数接近 0,说明应用这两种映射产生的二值序列均具有良好的自相关性.

4.3　平衡度分析

以下给出 Logistic 混沌映射和公式(9)定义的分段 Logistic 混沌映射在不同初始条件下生成序列的平衡度分布情况的实验结果,其中混沌系统初始条件从 0 变化到 1,产生的序列长度为 10000.

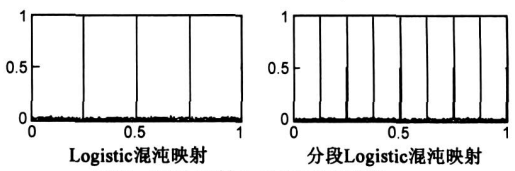

图9　两种映射生成序列平衡度

实验结果表明,应用两种映射产生的二值序列均具有良好的平衡度,说明这两种映射产生的二值序列均具有等效的平衡度.

4.4　初值敏感性分析

初值敏感性分析过程中,我们对混沌系统的初始条件进行微小变化,通过统计产生的二值序列中相应位置上的 1 和 0 的值的变化情况,计算相应的序列位变化率. 位变化率定义如下:

$$T = \frac{n'}{n}$$

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. 以下给出了当初始条件发生微小变化时所生成的两个混沌序列的位变化率.

表 3 两种映射初值敏感性比较

混沌系统初始条件	0.1	0.2	0.3	0.4
变化后的初始条件	0.100001	0.200001	0.300001	0.400001
Logistic 映射位变化率	0.5038	0.5000	0.4965	0.5014
分段 Logistic 映射位变化率	0.5010	0.4998	0.5004	0.4996

根据表 3 的结果可知,两种映射对于初始条件的微小改变,生成序列的位变化率接近 50 %,说明这两种映射具有良好的初值敏感性.

为了对 Logistic 混沌映射和分段 Logistic 混沌映射的初值敏感性进行进一步的对比分析,我们给出一种混沌映射初值敏感性判断指标 ——混沌映射分叉迭代次数.

定义 3(分叉迭代次数):设混沌系统为 $a_{n+1} = f(a_n)$,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 $\Omega = \min\{i \mid |a_i - b_i| > \delta\}$,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 时的分叉迭代次数.

以下给出 Logistic 混沌映射和分段 Logistic 混沌映射的对应不同分叉判定阈值所需要的平均迭代次数,我们在(0,1)区间取 10000 个采样点,计算相邻点之间产生混沌序列所需的平均分叉迭代次数,表 4 是相应的实验结果.

表 4 两种映射产生分叉所需迭代次数

分叉判断阈值	0.2	0.4	0.6	0.8
Logistic 混沌映射迭代次数	11.7014	13.0154	14.1030	18.4466
分段 Logistic 混沌映射迭代次数	7.1248	8.0536	9.5272	14.1706

通过表 4 的实验结果可知,对应相同的分叉判定阈值,Logistic 混沌映射所需的平均迭代次数明显大于分段 Logistic 混沌映射所需的平均迭代次数,说明分段 Logistic 混沌映射的分叉速度快于 Logistic 混沌映射,从而保证了分段 Logistic 混沌映射在加密过程能够较快地进入稳定的混沌状态.

4.5 Lyapunov 指数

为了定量地刻画混沌系统相邻的两点经过循环迭代过程产生分离的快慢,人们引入 Lyapunov 指数来表示在多次迭代所引起的相邻离散点之间以指数形式的分离或靠拢情况. 对应混沌系统 $x_{n+1} = f(x_n)$ 的 Lyapunov 指数定义如下[14]:

$$\lambda = \lim_{n\to\infty} \frac{1}{n} \sum_{i=1}^{n-1} \ln \left| \frac{\mathrm{d}f}{\mathrm{d}x} \right|_{x = x_i} \tag{11}$$

Lyapunov 指数小于 0 意味着经过混沌映射的迭代运算,相邻点最终要靠拢合并成一点,这时混沌系统对应稳定的不动点和周期运动;Lyapunov 指数大于 0 意味着相邻点经过混沌映射的迭代计算最终要分离,此时混沌系统对应的轨迹产生局部不稳定. Lyapunov 指数大于 0 可以作为判断序列是否为混沌序列的一个依据.

以下我们基于文[14]给出的混沌系统 Lyapunov 指数计算方法对 Logistic 混沌映射和公式(9)定义的分段 Logistic 混沌映射的 Lyapunov 指数进行计算. 相应的实验结果如下.

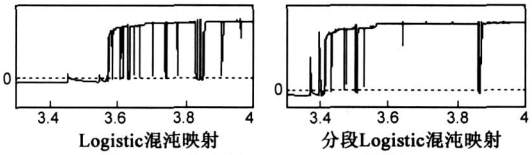

图10 两种映射的Lyapunov指数

根据图 10 的实验结果可知,Logistic 混沌映射和分段 Logistic 混沌映射在 $3.569946\cdots \le \mu \le 4$ 均具有稳定的混沌状态,而且分段 Logistic 混沌映射的 Lyapunov 指数取值大于 0 的状态比 Logistic 混沌映射的 Lyapunov 指数大于 0 的状态要稳定,这与表 4 的实验结果一致,说明了本文构造的分段 Logistic 混沌系统的运动轨迹更加不稳定,其相邻轨道分离得更快,因此对该序列的分析预测就更加困难.

5 结论

本文根据 Logistic 混沌映射与 Tent 混沌映射之间具有的拓扑共轭关系,结合分段 Tent 混沌映射给出了一种分段 Logistic 混沌映射的定义形式. 与分段 Tent 混沌映射相比,由于分段 Logistic 混沌映射的非线性性质,采用分段 Logistic 混沌映射生成混沌序列时不需要进行扰动运算,保证了生成算法具有更好的效率和安全性. 通过实验分析,表明本文定义的分段 Logistic 混沌映射的性能更加优于 Logistic 混沌映射. Logistic 混沌映射是一个被经常使用的混沌映射,这意味着本文给出的分段 Logistic 混沌映射会具有广泛的应用前景.

参考文献:

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

[2] Andrew T, Parker, Kevin M, Short. Reconstructing the keystream from a chaotic encryption scheme[J]. IEEE transactions on circuits and systems-I 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 transactions on circuits and systems-II, 2004, 51(10): 505 - 506.

[4] Zhang Han, Wang Xiu Feng, et al. A new image encryption algorithm based on chaos system[A]. International conference on robotics, Intelligent systems and signtal processing[C]. Changsha, China. 2003: 778 - 782.

[5] T Habutsu, Y Nishio, I Sasase, et al. A secret cryptosystem by iterating a chaotic map[A]. Advances in Cryptology EURCRYPT '91[C]. Berlin: Springer-Verlag. 1991: 127 - 140.

[6] 柳平,闫川,黄高显. 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.
LIU Ping, et al. Optimized method of generating the spread-spectrum sequences based on Logistic-map[J]. Journal on Communications, 2007, 28(2): 134 - 140. (in Chinese)

[7] 张翌维,王育民,沈绪榜. 基于混沌映射的一种交替结构图像加密算法[J]. 中国科学(E 辑:信息科学). 2007, 37(2): 183 - 190.
ZHANG Yu-wei, et al. An alternation structure image encryption algorithm based on chaotic map[J]. SCIENCE IN CHINA (Serise E). 2007, 37(2): 183 - 190. (in Chinese)

[8] 单梁,强浩,李军,王执铨. 基于 Tent 映射的混沌优化算法[J]. 控制与决策, 2005, 20(2): 179 - 182.
SHAN Liang, et al. Chaotic optimization algorithm based on Tent map[J]. Control and Decision. 2005, 20(2): 179 - 182. (in Chinese)

[9] 刘镔,张永强,刘粉林. 一种新的数字化混沌扰动方案[J]. 计算机科学, 2005, 32(4): 71 - 74.
LIU Bin, et al. A new scheme on perturbing digital chaotic systems[J]. Computer Science, 2005, 32(4): 71 - 74. (in Chinese)

[10] 刘光杰,单梁,戴跃伟,孙金生,王执铨. 基于混沌神经网络的单向 Hash 函数[J]. 物理学报, 2006, 55(11): 5688 - 5693.
LIU Guang-Jie, et al. One-way Hash function based on chaotic neural network[J]. ACTA PHYSICA SINICA. 2006, 55(11): 5688 - 5693. (in Chinese)

[11] 刘建东,付秀丽. 基于耦合帐篷映射的时空混沌单向 Hash 函数构造[J]. 通信学报, 2007, 28(6): 30 - 38.
LIU Jian-dong, et al. Spatiotemporal chaotic one-way Hash function construction based on coupled tent maps[J]. Journal on Communications, 2007, 28(6): 30 - 38. (in Chinese)

[12] Goce Jakimoski, Ljupco Kocare. Chaos and Cryptography-PART Ⅱ: Block Encryption Based on Chaotic Maps[J/OL]. http://rfic.ucsd.edu/chaos/papers.Html, 2000.

[13] 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.
LIAO Ni-huan, et al. The chaotic spreading sequences generated by the extended chaotic map and tis performance analysis[J]. Journal of Electronics & Information Technology, 2006, 28(7): 1255 - 1257. (in Chinese)

[14] 赖建文,周世平,李国辉,徐得名. 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.
LAI Jian-ping, et al. A method for computing Lyapunov exponents spectra without reorthogonalization[J]. Acta Physica Sinica, 2000, 49(12): 2328 - 2332. (in Chinese)

作者简介:

范九伦　男, 1964 年生, 陕西省西安市人, 博士后, 教授, 博士生导师. 主要研究方向为模糊集理论、模糊信息处理、模式识别与图像处理、信息安全.
E-mail: jiulunf@xiyou.edu.cn

张雪锋　男, 1975 年生, 陕西省户县人, 博士研究生, 副教授. 研究方向为信息安全、数字图像保护技术.
E-mail: zhangxuefeng3@163.com