信息加密的混沌流密码受参数变化影响的实验研究*

林土胜[1], 徐亚国[2]
(1. 华南理工大学电子与信息学院, 广东 广州 510641;
2. 广州市公共安全技术研究所, 广东 广州 510030)

摘 要: 近年来利用混沌特性在互联网中进行信息加密得到了较多的应用研究。混沌参数的不同取值直接影响混沌映射所产生流密码的复杂性。以广泛采用的 Logistic 映射、Henon 映射及其复合映射作为实验对象, 分析不同参数取值时混沌映射所产生的流密码的随机特性、自相关特性、互相关特性、平衡性及游程的变化, 为工程实际应用提供参数选择的参考。

关键词: 信息加密; Logistic 映射; Henon 映射; 混沌流密码
中图分类号: TN914.2 文献标识码: A 文章编号: 0529-6579 (2004) S2-0101-04

混沌是一种很普遍的现象, 混沌现象无处不在, 但却是一种很复杂的概念, 至今仍未有一种公认的严格的定义。通常来说, 对于一个确定性的非线性系统, 若表现出“有界”、“非周期性”和“敏感初条件”三特性, 则认为处于混沌状态。混沌信号的非周期性、连续宽带频谱、类似噪声的特性, 使之具有天然的隐蔽性; 对初始条件高度敏感、高度复杂度等特性, 使之具有长期不可预测性, 十分适合于信息加密。传统密码学的信息加密与基于混沌密码学的混沌加密相比, 前者有 100 多年历史, 技术成熟, 而后者兴起仅十来年; 前者理论体系完整和门类齐全, 而后者属开创初期和实践阶段; 前者加密技术基础是以数学方法为主并基于计算复杂性, 而后者以物理方法为主, 基于利用混沌系统的复杂性和混沌特性; 但在保密性和抗破译能力方面, 后者比起前者来则更为优越[1]。因为理论上传统密码学把明文变成密文, 其关系是固定不变的, 而混沌系统的加密形式是随机的、不定的、甚至是无穷多的, 每次都不一样, 无律可循, 保密的随机变化过程极其深奥。图 1 是组合混沌映射对图文进行加密/解密的一个例子。

目前在混沌序列密码的研究中, 大部分采用差分方程的迭代运算来产生具有非周期性和伪随机性特性的密钥序列[2,3]。即利用混沌映射产生流密码。不同的混沌映射参数将决定映射流密码复杂度的优劣。本文以被广泛地采用的 Logistic 映射与 Henon 映射为研究对象, 通过 Matlab 实验仿真[4,5] 来观察相应映射的随机特性、自相关特性、互相关特性、平衡性及游程的变化, 研究参数变化对流密码复杂度的影响情况, 为实际工程应用提供参数选择的参考。

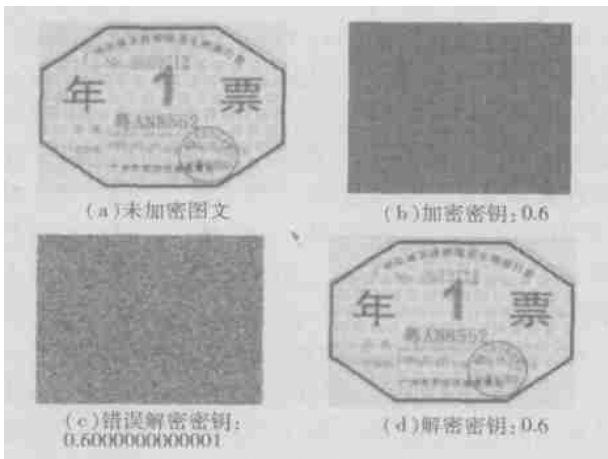

图 1 车辆通行票据的加密/解密

Fig. 1 Encryption & decryption for traffic tickets

1 Logistic 映射受参数变化的影响

Logistic 映射是一种简单的一维混沌映射, 采用如下形式:

$$\chi_{n+1} = 1 - \mu\chi_n^2$$
$$\mu \in (0, 2) \qquad \chi \in [-1, 1] \qquad (1)$$

当 $\mu \in [1.5437, 2)$, 式 (1) 所示的 Logistic 映射是混沌的。下面仿真这一取值范围。

* 收稿日期: 2004-09-11
基金项目: 广州市科技局应用基础研究 (2002J1-C0341)
作者简介: 林土胜 (1945 年生), 男, 教授; E-mail: eetshlin@scut.edu.cn

1.1 不同 μ 值下的伪随机特性

限于版幅，只显示 μ 的取值区间两端的仿真结果，以下类同。(设 $\mu=a$，纵坐标为区间范围 x，横坐标为迭代次数 N)(见图2)。

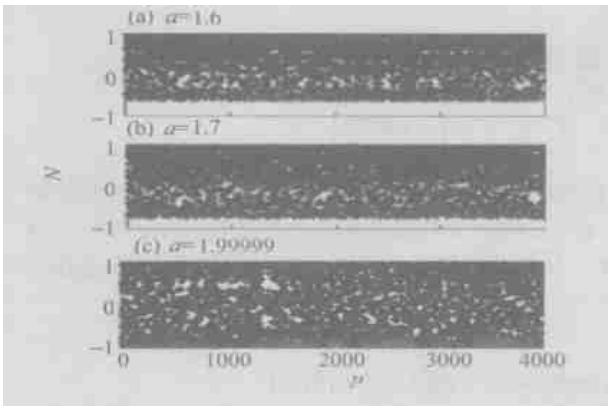

图2 不同 μ 值下的 Logistic 混沌序列

Fig. 2 Logistic chaotic sequences with value μ

从仿真图可以看到当 μ 的值取 [1.5437, 2) 时，产生分布在 [1, −1] 的混沌序列的情况。当 $\mu=1.6$ 时，明显看到序列在“1”侧分布密集，“−1”侧出现空白，序列在 [−1, 1] 区间内分布不均匀。当 $\mu=1.7$ 时，序列分布逐趋均匀，但是也不理想。随着 μ 逐渐趋向于2时，产生的 x 序列越来越近似于随机分布。当 μ 的值很接近2时(如图2中 $\mu=1.99999$ 时)，混沌序列的值很均匀的分布在整个 [−1, 1] 区间，非常接近随机分布的序列。

1.2 不同 μ 值下的相关性比较

具有很好伪随机特性的混沌序列应该在分布上体现出随机性，即每一个序列值与自己的相关系数是1，与其它序列值相关系数是0。这样的序列所形成的流密码将具有很好的平衡性和很强的复杂度。图3仿真了不同参数下 Logistic 映射产生的序列其自相关性与互相关性的差异(设 $\mu=a$, $N=8\,000$)。

图3中 m(未标出)为相关间隔，理想情况下自相关曲线应该是 $m=0$ 时，$R_{xx}=1$ 的冲击函数；互相关曲线近似为高斯白噪声。图中得出的结论是，当 μ 值趋向于2时，Logistic 映射自相关曲线接近冲击函数，即每个序列值只和自己相关，与其他序列值的相关系数为0，互相关特性曲线接近于白噪声，这意味着随着 μ 值接近2，Logistic 映射序列相关性明显变好。

1.3 平衡性及游程分析

在实际应用中常常需要对混沌映射进行编码，而最简单的编码方式就是正1负1码，保密通信常常

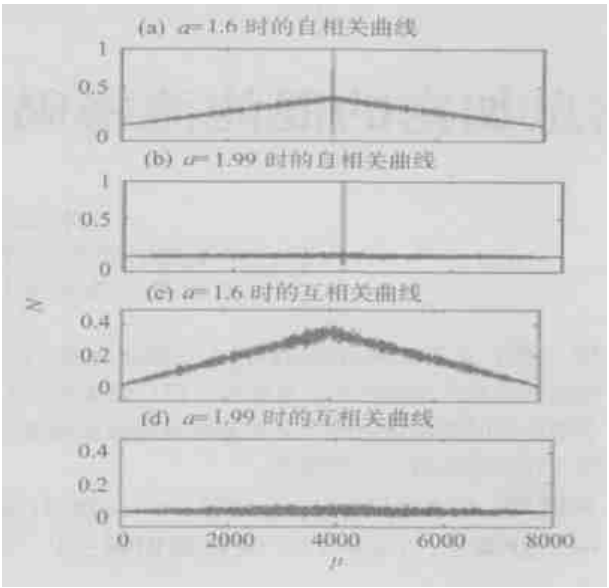

图3 不同参数下 Logistic 映射序列的相关性

Fig. 3 The correlativity of Logistic mapping

要求流密码有很好的平衡性，在正1负1码中平衡性序列中“1”码元数目应与“−1”相当，不能过多也不能过少。此外，理想伪随机码对游程的要求是，1/2的游程长度为1，1/4的游程长度为2，1/2n的游程长度为n。表1用最简单的编码方式比较了不同参数取值时 Logistic 映射流密码平衡性能与游程性能。

表1 混沌二进制序列平衡性比较($N=4096$)

Tab. 1 The balance of binary chaotic sequences

μ	1的个数	比率/%	−1的个数	比率/%
1.60	3055	74.58	1041	25.42
1.70	2977	72.68	1119	27.32
1.80	2479	60.52	1612	39.48
1.99	2139	52.22	1957	47.78

在平衡性比较中可以看到当 $\mu=1.6$ 时−1, 1的分布很不均衡。随着 μ 值接近2，−1码同1码所占比例逐渐接近50%。当 $\mu=1.99$ 时，仿真结果已经非常接近理想值。

表2 混沌二进制序列游程性能比较($N=4096$)

Tab. 2 The run of binary chaotic sequences

μ	游程1	比率/%	游程2	比率/%	游程3	比率/%	总游程
1.60	1562	72.28	0	0	273	12.63	2161
1.70	1496	67.66	268	12.12	186	8.41	2211
1.80	1435	57.42	831	33.25	83	3.32	2499
1.99	1160	51.77	573	25.57	285	12.72	2241

从表2的仿真数据可以明显看出，μ 接近2时，游程性能也越来越接近理想值。当 μ 的值很接近

2(1.99) 时, Logistic 映射产生的流密码与随机数列性能十分接近。在平衡性与游程角度看, μ 的值越接近 2, 序列的伪随机特性越好。

2　Henon 映射受参数变化的影响

为了实际应用算法的需要, 把二维 Henon 映射转化为如下的形式:

$$\chi_{n+2} = 1 + b\chi_n - \alpha\chi_{n+1}^2$$
$$b = 0.3 \qquad 1.07 \leqslant a \leqslant 1.4 \tag{2}$$

2.1　不同参数值下的伪随机特性

图4 中可看出 a 值在 [1.07, 1.40] 上取值时, Henon 序列的分布图变化明显。当 a 在 1.07附近时, [－1.5, 1.5] 中分布为几个不均匀的间隔(－1.5 段未示出)。随着 a 值增加, 序列值的分布逐渐均匀, 1.20时最为均匀。其后 a 增加到某个数值时(如 a = 1.27), 序列值出现反复的交替, 整个序列失去了伪随机性, 流密码呈现规律性, 不能在实际中应用。接着当 a 逐渐接近 1.40时, 序列的分布又渐渐类似于随机序列。当 a = 1.40时, 序列在[－1.5, 1.5] 上分布最为均匀。

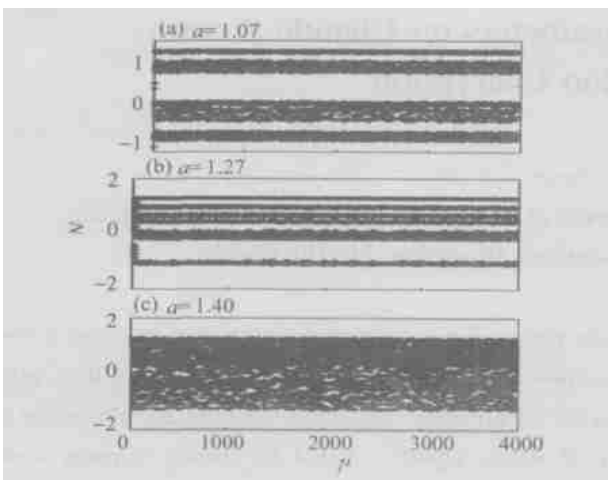

图 4　不同参数取值时 Henon 映射序列

Fig. 4　Henon sequences in varied parameters

2.2　不同 a 值下的相关性比较

从图 5 可看到 a 在[1.07, 1.40] 中取值较低时, Henon 映射产生的序列值之间有很强的相关性, 同一参数下不同初值序列之间的相关性也很强。这种流密码显然性能不好。同样, 当 a 的取值在 1.24 到 1.30 范围时, 序列的性能也很差, 不适于应用。当 a 取另外的一些值时, 序列的伪随机性增强。可看到 a = 1.40 时, 自相关特性曲线更接近为冲击响应, 互相关特性曲线更接近于白带噪声信号, 表明此时产生的流密码具有较好的相关特性, 但仍应采取相应措施, 去掉序列初值以得到更理想的流密码。

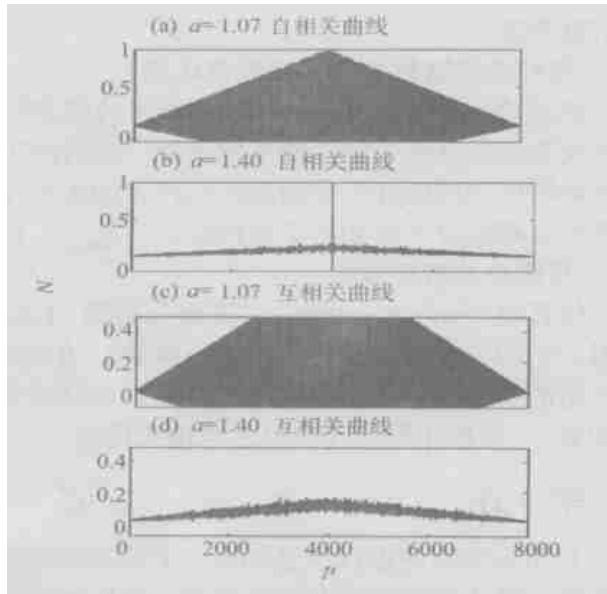

图 5　不同参数下 Henon 映射的相关特性曲线

Fig. 5　The correlativity of Henon mapping

2.3　平衡性及游程分析

并不是所有[1.07, 1.40] 之间的参数取值都具有很好的随机性, 仿真结果表明 a = 1.40 时序列的平衡性最好, 其中 1 和－1 的个数比率分别为 69.46%和 30.54%, 比其余参数的比率要高; 游程性能方面 a = 1.33 时序列性能较好(限于版幅, 其余结果从略), 尽管 a = 1.40 时游程性能稍逊, 但在其它分析中它的表现优异。

3　单一与组合混沌映射的伪随机特性比较

3.1　组合混沌映射

在实际应用中可采用去初值法, 取模非线性运算法和过采样处理法加强流密码的复杂度。也可以采用几种混沌映射组合的方法, 增强流密码的伪随机特性和复杂度。产生混沌映射复合序列的过采样处理方法表示为:

$$X_{n+1} = f(x_n) \qquad (x \in I) \tag{3}$$
$$X_{N+1} = f(f\cdots(f(x_n))) = f^{(p)}(x_n) \tag{4}$$

式(4) 称为过采样混沌映射(oversampled chaotic mapping)[6]。对混沌映射采用过采样技术, 可以使混沌映射产生的流密码分布更加随机化, 提高保密通信的质量。p 也可作为一个密钥参数。如果将(3) 设置成混沌映射, 而参数 p 由另一个混沌序列所决定, 就可以实现两个混沌映射的复合。式(3) 取 Logistic 映射, p 由另一个 Logistic 映射产生的序列值决定, p 的值也具有很好的伪随机性, 这就使最终产生的过采样序列拥有更好的随机特性, 提高了流密

码的复杂度。

3.2 两种混沌映射组合的相关性比较

仿真结果表明,采用映射组合产生的流密码其自相关特性与互相关特性明显优于单一映射产生的流密码特性,究其原因,是因为迭代产生的序列经过过采样处理后分布更加趋于随机化。

3.3 平衡性及游程分析

仿真统计值($N=4096$)和游程分析表明,组合映射产生的流密码平衡性优于单一映射。两类映射所产生的二进制流密码均与理想随机二进制数列极为相似,二者相比则组合映射性能稍为优越。

4 结 论

利用混沌特性进行信息加密,不同的混沌映射参数决定混沌流密码复杂度的优劣。对广为采用的一维Logistic和二维Henon混沌映射进行参数范围实验仿真的研究表明,在混沌区间内选择合适的参数,能使产生的混沌序列的自相关特性接近冲击响应函数,互相关特性接近白噪声;组合混沌映射比单一混沌映射产生的混沌序列具有更优良的随机性和复杂度。参数变化影响的实验研究为工程实际应用提供了参数选择的方向和取值依据。

参考文献:

[1] 赵耿,方锦清.现代信息安全与混沌保密通信应用研究的进展[J].物理学进展,2003,23(2):212-255.

[2] 王工一.混沌序列流密码[EB/OL].http://www.ahcit.com/200203/03.doc,2002-03-15

[3] 王相生,甘俊人.一种基于混沌的序列密码生成方法[J].计算机学报,2002,25(4):351-356.

[4] 陈桂明,等.应用MATLAB语言处理数字信号与数字图像[M].北京:科学出版社,2000.

[5] 清源计算机工作室.MATLAB高级应用-图形及影像处理[M].北京:机械工业出版社,2000.

[6] ZHANG H T, GUO J C, WANG H Y, et al. Oversampled chaotic map binary sequences: definition, performance and realization. The 2000 IEEE Asia-pacific conference on circuit and system[C]. Tianjin, 2000: 618-621.

Experimental Study of Different Parameters on Chaotic Stream Ciphers for Information Encryption

LIN Tu-sheng[1], *XU Ya-guo*[2]

(1. Electronics & Information College, South China University of Technology, Guangzhou 510641, China;
2. Research Institute of Public Security of Guangzhou, Guangzhou 510030, China)

Abstract: Information encryption based on the features of chaos are getting more applications in internet in recent years. Chaotic mappings are sensitive to the change of parameters, the complexity of stream ciphers would depend on their value of parameters. Logistic-mapping and Henon-mapping were taken as experimental objects to analyze the properties of randomness, auto-correlation, cross-correlation, balance and run of stream ciphers created by chaotic mapping under different parameters on the system, the conclusion will be a help to select chaotic parameters in engineering practice.

Key words: information encryption; logistic mapping; Henon mapping; chaotic stream cipher