第33卷 第10期 计 算 机 工 程 2007年5月
Vol.33 No.10 Computer Engineering May 2007
·安全技术· 文章编号：1000—3428(2007)10—0164—02 文献标识码：A 中图分类号：TP309

基于Logistic映射的混沌流密码设计

王化丰[1]，张桂香[2]，邵 勇[3]
(1. 大连理工大学电信学院，大连 116023；2. 齐齐哈尔大学计算中心，齐齐哈尔 161005；3. 北京工业大学软件工程学院，北京 100022)

摘 要：混沌系统特有的一些优良属性较适合流密码的设计，比如混沌迭代序列对初始条件和控制参数的敏感性、伪随机性、混和性和确定性等。该文以Logistic映射为例说明了其主要特性和初值敏感性，并重点图示了在字节输出方式下和比特输出方式下，其离散分布和均匀分布的差异和改善。

关键词：流密码；伪随机性；混沌；Logistic

Design of Chaotic Stream Cipher Based on Logistic Mapping

WANG Huafeng[1], ZHANG Guixiang[2], SHAO Yong[3]
(1. School of Electronics and Information, Dalian University of Technology, Dalian 116023; 2. Computer Center, Qiqihar University, Qiqihar 161005; 3. School of Software Engineering, Bejing University of Technology, Beijing 100022)

【Abstract】Some particular attributes of chaos system are more suitable for stream cipher design, such as the sensitivity to initial conditions and control parameters, pseudo randomness, mixing and exactness, etc. Taking Logistic mapping as example, this paper shows out its primary characteristics, illustrates the difference and improvement of the discrete distribution and uniform distribution under conditions of the standard byte output method and the improved bit output method.

【Key words】Stream cipher; Pseudo randomness; Chaos; Logistic

1 概述

序列密码也叫流密码，是相对分组密码而言的一个密码学分支，1949年Shannon证明了只有一次一密的密码体制才是绝对安全的，对流密码的发展研究提供了有力支持。通过密码序列来加密明文序列，其核心技术就是伪随机数序列发生算法，常用的方法有线性反馈移位寄存器法(LFSR)，非线性反馈移位寄存器法(NLFSR)，有限自动机法和线性同余法等。如今，流密码技术已经广泛地应用于移动通信、数字电视、流媒体数字广播和其他数据通信业务领域。

混沌理论是一门研究奇异函数和奇异图形的数学理论，和分形几何有着密切的联系，它们协同成为研究自然界有序和无序间规律的科学。混沌是一种确定性系统中出现的类似随机的过程，1963年首先由气象学家Lorenz在流体热对流的简化模型计算中观察到，1974年物理学家Feigenbaum发现了普适常数，1975年李天岩和Yoke发表的“Period Three Implies Chaos”使用了“混沌”(Chaos)这个术语。

随着现代密码学的不断发展，许多非线性系统的特性研究与应用逐渐被关注，其中混沌系统在网络通信和信息安全领域中的应用更是研究的对象。混沌系统特有的一些优良特性很适合于密码学领域的应用，比如混沌迭代序列对初始条件和控制参数的敏感性、难预测性、伪随机性、遍历性、混和性和确定性等。1989年Robert Matthews在Logistic映射的变形基础上给出了用于加密的伪随机序列生成函数[1]，其后混沌密码学及混沌密码分析等便相继发展起来。混沌流密码的研究主要是基于混沌系统伪随机数发生器的(PRNG)相关算法的研究，大部分技术都是采用从各种混沌系统生成的伪随机数序列来抽取特定比特流作为密钥流来掩盖明文的，也有的是利用了混沌映射区间划分把迭代次数来作为输出密文的。混沌流密码系统的设计可以采用不同的混沌映射，如一维Logistic映射、二维He'non映射、三维Lorenz映射、逐段线性混沌映射[2]、逐段非线性混沌映射等，还可以基于逆混沌系统或时空混沌的耦合映像网格等。

一个完整的混沌流密码系统设计和分析包括混沌映射系统的复合设计、数值测试分析、初值敏感性分析、离散分布和均匀分布性分析、周期性分析[3]、系统自相关性和互相关性分析、线性复杂度分析等诸多方面。这里仅以一维Logistic映射的部分特性为例，对其初值敏感性及离散分布和均匀分布性进行解析，其它更深入的分析方法和结果请参考文献[4,5]。

2 混沌流密码设计

2.1 Logistic映射的主要特性

一维Logistic映射是一个简单的混沌映射，20世纪50年代，有好几位生态学家就利用过这个简单的差分方程，来描述种群的变化：

$$X_{n+1} = \mu * X_n * (1 - X_n) \qquad \mu \in [0,4] \quad X \in [0,1]$$

式中，X_n表示当年的种群数，X_{n+1}便是下年的种群数，μ为增长参数。显然这个方程只有一个二次项非线性部分。可以利用Logistic映射的混沌区产生伪随机性很好的伪随机数序列，理论上讲，在混沌区的伪随机序列可以是无周期的，但是，数值在计算机中表示的位数是有限的，所以有限位精度数值的迭代运算是有周期的。Logistic映射的控制参数μ应该介于[0，4]之间，初始条件的X初值X_0应该介于[0，1]之间。为了观察这个迭代过程输出的数值序列的分布情况和局部细

作者简介：王化丰(1971－)，男，硕士、讲师，主研方向：密码学，网络安全和电子商务等；张桂香，讲师；邵 勇，硕士、讲师
收稿日期：2006-06-26 **E-mail：**wanghuaf@dlut.edu.cn

节，首先选取 X_0=0.5，μ 值遍历于[0,4]之间，迭代 512 次；其次再选取 X_0=0.5，μ 分别取[3,4]范围，再迭代 388 次，如图 1，其中横轴表示 μ 的取值范围，纵轴表示 X 的取值范围。

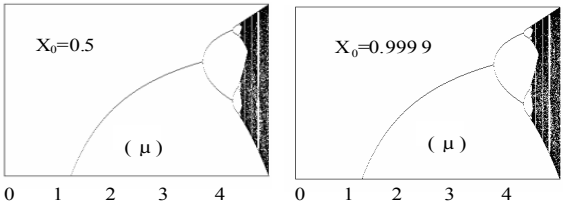


图 1 初值 X_0=0.5 和 X_0=0.999 9 时 Logistic 映射迭代(抛弃前 512 次迭代数)

从图 1 中可以看出，在 μ 取值很接近 4 的时候，X 的取值趋向于分散在整个(0,1)范围内。这说明当 μ 取值在 4 附近的时候，X 伪随机数序列的取值区间范围较大，μ 的这个取值范围比较适合于用来产生较好的伪随机数序列。再结合图 2，还有其它的一些迭代图，研究者们进一步得出如下结论：

(1)当 μ >=3 时，X 值一分为二，对应周期为 2 的解，随着参数进一步增加，周期数不断加倍，X 迭代值周而复始地在有限个周期轨道之间重复，从而进入 2n(n=1,2,3,…) 的倍周期分岔(Bifurcation)区，进而进入多片混沌区。

(2)当 μ=4 时，X 取值进入单片混沌区，周期为任意整数的解都存在，且不稳定。当 μ 逐渐小于 4 时，出现混沌区的倒分岔行为。

(3)混沌区有些空白的窗口，最大的窗口是周期 3 窗口。 它出现在 μ=3.828 的地方。周期 3 窗口附近还有 7,9,…等周期窗口， 在混沌的 2 带区则有 2×3,2×5,2×7…等周期窗口；在 2^n 带区中有 2^n ×3,2^n ×5,2^n ×7…等周期窗口。

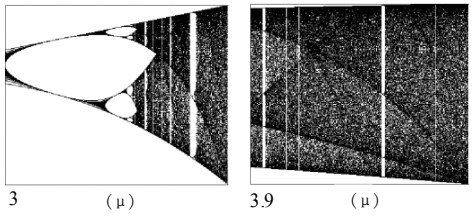


图 2 初值 X_0=0.5，μ 取[3,4]和[3.9,4]范围时的迭代(无抛弃数)

2.2 对初值与控参的敏感性

如果 μ 的取值定下来，讨论 X 的初值选取对迭代序列的影响。考虑不同的迭代初值对以后的生成结果有什么影响，从而保证不同的用户能够通过不同的初值参数产生不同的伪随机数序列。当初值选取差别很大的时候，显然运算结果将会有很大差别的，但是如果 X 的初值选取得很接近的时候，比如 X_0 分别选取 0.1+DBL_EPSILON(2.2204460492503131e-016)和 0.1，它们的初值相差微小，当 μ 选取 4，分别进行 150 次迭代运算，两个序列差值的图形(就是用第一个序列某一次运算的迭代值减去另一个序列相同运算次数产生的迭代值)如图 3 所示。

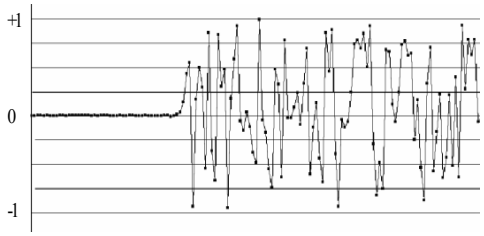


图 3 固定 μ 值，初值 X 有微小差别时，两个迭代序列的差值

其中横轴表示迭代次数，纵轴表示 2 个序列迭代值之间的差值。可以形象地看出，两个伪随机数序列最初相差很小，迭代值非常接近，但是随着迭代次数增加，差距逐渐变大，然后变得越来越毫无规律。同理，对于固定 X 值而让 μ 值有一个微小差异，混沌迭代序列差值的特性和上面的结果非常类似。因此，当应用 Logistic 一维映射来产生伪随机数序列的时候，任意的 μ 或 X 初值的微小差异，都会导致一定次数迭代运算以后的结果产生很大差别，特别是当使用的两套 μ 参数和 X 初值均不相同的时候，生成的两个序列之间很难寻找到明显的相关性。可以认为用这种方法产生的混沌伪随机数序列具备有较好的伪随机性。

2.3 离散分布和密度分布

伪随机数序列在取值范围内的分布特征也是一个衡量其伪随机性时要考虑的方面。看一下一维 Logistic 映射生成的伪随机序列的离散分布和密度分布，迭代次数为 100 000 次，输出是双精度浮点数取整后的字节输出值，参数 μ=0.4，初值 X=0.1，结果如图 4 所示。

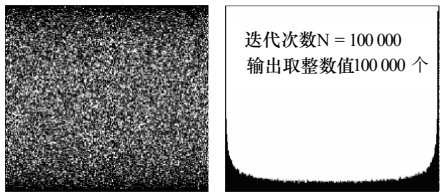


图 4 字节输出方式的离散分布和密度分布(X_0=0.1, μ=4)

由图 4 可以看出 Logistic 映射的迭代序列在完全混沌区的离散分布和密度分布并不是均匀的，可以考虑采用按比特输出的如下 2 种改进的方法：

(1)如果 Logistic 映射迭代序列整数化后的奇偶性分布是均匀的，则可以采用每次根据迭代值整数化后的奇偶性来输出 0 或 1 比特的方法来产生伪随机数序列，公式如下：

$$P_{n+1}=\begin{cases}0, \mathrm{int}(X_{n+1}) \bmod(2)=0\\ 1, \mathrm{int}(X_{n+1}) \bmod(2)=1\end{cases},\quad X_{n+1}=4X_n(1-X_n)$$

(2)如果 Logistic 映射迭代序列关于 X=0.5 的分布是对称的，则可以采用每次根据迭代值是否大于或小于 0.5 域值来输出 0 或 1 比特的方法来产生伪随机数序列，公式如下：

$$P_{n+1}=\begin{cases}0, X_{n+1}\geq 0.5\\ 1, X_{n+1}<0.5\end{cases},\quad X_{n+1}=4X_n(1-X_n)$$

采用方法(2)的结果如图 5 所示。其中，迭代运算 160 000 次，输出 10 000 个 16 比特整数。从图 5 可以看出这种改进的伪随机数序列生成方法至少应该有相对较好的离散分布和密度分布。方法(1)的迭代结果同方法(2)相近，这里不再作图说明，可以在上述两个方法基础上继续改进，以期达到更好的效果。

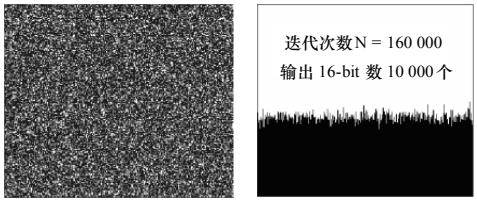


图 5 比特输出方式的离散分布和密度分布(X_0=0.1,μ=4)

3 结论

混沌系统的类密码学特性，比如初值和控参敏感性、伪随机性、确定性等使得基于混沌系统的密码设计成为近十几年来密码学新研究领域的热点之一，已经有了不少的进展和研究积累。通过调整 Logistic 映射的迭代输出方式，可以改

(下转第 168 页)

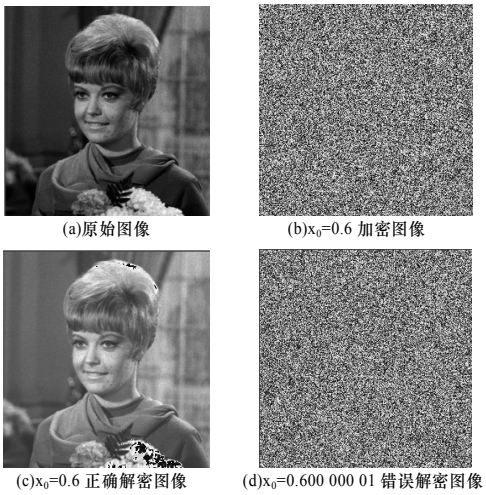
不论从视觉效果，还是从图像置乱程度来看，改进猫映射均优先于传统猫映射。

表 1 两种猫映射加密图像的相关系数比较

	原始图像	传统猫映射加密图像	改进猫映射加密图像
水平方向	0.960 5	0.398 2	0.186 8
垂直方向	0.948 3	0.072 4	0.096 9
对角线方向	0.923 9	0.035 2	0.010 5

6 实验结果及其分析

在 VC++6.0 编程环境下利用本文提出的基于改进的混沌猫映射和扩散函数相结合的加密算法对一幅灰度图像进行了加密和解密试验，设置密钥分别为：a=20，b=40，m=5，n=8，u=11，v=5，f=50，x_0=0.6，u=2,t=1。图像加密解密效果如图 2 所示。



(a)原始图像　(b)x_0=0.6 加密图像

(c)x_0=0.6 正确解密图像　(d)x_0=0.600 000 01 错误解密图像

图 2 图像的加密和解密结果

混沌序列对初始值非常敏感，即使初始值有微小的变化也会得到完全不同的解密结果(图 2(d))，如初始值(密匙)x_0=0.600 000 01，u=2.0 时，就无法对图像进行正确解密。

本文从原始图像和加密图像中各选取了 1 000 对像素点来测试其各自在水平方向、垂直方向和对角线方向的相关性，测试结果如表 2 所示。

表 2 本算法加密图像的相关系数比较

	原始图像	本算法加密图像
水平方向	0.960 5	0.008 6
垂直方向	0.948 3	0.044 6
对角线方向	0.923 9	0.007 3

由表 2 可见，利用本算法加密后的图像在水平方向、垂直方向和对角线方向的相关系数都有明显的降低，充分证明了本算法可以有效的抵抗统计攻击。

7 结论

针对传统的猫映射加密图像无法改变原始图像直方图的缺陷，提出了一种利用改进的混沌猫映射和扩散函数相结合来对数字图像进行置乱加密的算法。该算法具有很好的加密/解密效果和安全性，如图 2(c)中解密的密码 x_0=0.600 000 01，与正确的密码 x_0=0.6 只相差 0.000 000 1，就无法对图像进行正确解密，且改进的猫映射与传统的猫映射相比，密钥空间增大了 5 倍。该算法同时在空间域和色度域对图像进行加密，基本上都采用整数运算和位运算，具有加密速度快、运算简单的特点。

参考文献

1 丁　玮, 齐东旭. 数字图像变换及信息隐藏与伪装技术[J]. 计算机学报, 1998, 21(9): 838-843.

2 Qi Dongxu, Zou Jinacheng, Han Xiaoyou. A New Class of Scrambling Transformation and Its Application in the Image Information Covering[J]. Sciences in China, 2000, 43(3): 304-312.

3 Ding Wei, Yan Weiqi, Qi Dongxu. Digital Image Watermarking Based on Discrete Wavelet Transform[J]. Computer Science and Technology, 2002, 17(2): 129-139.

4 Chen Guanrong, Mao Yaobin, Chui C K. A Symmetric Image Encryption Scheme Based on 3D Chaotic Cat Maps[J]. Chaos, Solitons and Fractals, 2004, 21(3): 749-61.

5 Lian Shiguo, Sun Jinsheng, Wang Zhiquan. Security Analysis of a Chaos-based Image Encryption Algorithm[J]. Physica A, 2005, 351(2-4): 645-661.

6 张小华, 刘　芳, 焦李成. 一种基于混沌序列的图像加密技术[J]. 中国图像图形学报, 2003, 8(4): 374-378.

(上接第 165 页)

善原来伪随机序列数值分布不平衡这一缺点，其它方面的改善还要结合更多的其它办法。

造成混沌流密码系统不够安全的重要原因之一就是数字化混沌系统的动力学特性退化问题。由于计算机生成的混沌系统都是在有限数值精度下运算模拟出来的拟混沌轨道的周期是有限的，这给混沌流密码系统的安全应用带来了很大的隐患，因此必须特别注意和采取适当的措施加以避免。目前，除了采用更高的计算精度和复合多个相同或不同的混沌系统外，还可以采用对混沌系统施加伪随机微小扰动等方法来加大混沌系统迭代序列的周期。

参考文献

1 Robert A, Matthews J. On the Derivation of a Chaotic Encryption Algorithm[J]. Cryptologia, 1989, 13(1): 29-42.

2 Shujun L, Xuanqin M, Yuanlong C. Pseudo-random Bit Generator Based on Couple Chaotic Systems and Its Applications in Stream-cipher Cryptography[C]//Proceedings of the Progress in Cryptology——the 2nd International Conference on Cryptology, India. 2001: 316-329.

3 Shihong W, Weirong L, Huaping L, et al. Periodicity of Chaotic Trajectories in Realizations of Finite Computer Precisions and Its Implication in Chaos Communications[J]. International Journal of Modern Physics B, 2004, 18 (17-19): 2617-2622.

4 Kocarev L, Jakimoski G. Pseudorandom Bits Generated by Chaotic Maps[J]. IEEE Transactions on Circuits and Systems- I: Fundamental Theory and Applications, 2003, 50(1):123-126.

5 Álvarez G, Montoya F, Romera M, et al. Cryptanalyzing an Improved Security Modulated Chaotic Encryption Scheme Using Ciphertext Absolute Value[J]. Chaos, Solitons and Fractals, 2005, 23(5).