一种基于 Hénon 映射和 m-序列的混沌序列密码算法研究

韦鹏程[1] 张 伟[1,2] 杨华千[1,2]

(重庆教育学院计算机与现代教育技术系 重庆400067)[1]

(重庆大学计算机科学与工程学院 重庆400044)[2]

摘 要 在详细分析二维 Hénon 映射的混沌和密码学特性的基础上,结合收缩式发生器,提出一种基于 m-序列和 Hénon 混沌序列的混合混沌序列密码算法。同时对该系统的安全性能进行了深入分析,理论和实验结果表明:在有限精度实现下,该方法可以有效提高混沌系统的复杂性和周期性,并且算法安全性高、运算速度快,适于在 Internet 上对多媒体信息的保密传输。

关键词 序列密码,线性移位反馈寄存器,m-序列,混沌,混合混沌序列

A Novel Chaotic Stream Cryptographic Algorithm Based on Hénon Map and m-Sequences

WEI Peng-Cheng[1] ZHANG Wei[1,2] YANG Hua-Qian[1,2]

(Department of Computer and Modern Education Technology, Chongqing Education College, Chongqing 400067)[1]

(Department of Computer Science and Engineering, Chongqing University, Chongqing 400044)[2]

Abstract The chaotic and cryptographic properties of the 2-D Hénon map are analyzed firstly. By using the Shrinking Generator, a novel mixed chaotic cryptographic algorithm based on combining Hénon map sequences and m-sequences has been proposed in this paper. At the same time, the authors made in-depth analysis of the security performances of the system. The theoretic and simulation show that the new approach not only allows us to improve the complexity and the period of the chaotic system under the finite-precision circumstances but has high security and encrypting speed, thus it is suitable for practical use in the multimedia secure transmission over the Internet.

Keywords Stream cipher, LFSR, M-sequences, Chaos, Mixed chaotic sequences

1 引言

混沌(Chaos)是一种复杂的非线性动力学行为,混沌系统所具有的对初值敏感性,混沌轨道的伪随机性、遍历性和不可预测等自然特性,可以提供数量众多、非相关、伪随机而又确定可再生的混沌序列,使其在保密通信和密码学领域的应用越来越广泛,研究越来越深入,取得了大量的成果[1~4]。由于混沌系统的优良特性主要体现在轨道上,其实数值自然形成一个序列,因此,混沌系统被大量应用于序列密码的设计中。混沌序列应用于密码的研究是从1989年提出后发展起来的。十多年来,存在的主要问题是[6,7]:混沌序列的生成器总是在有限精度器件实现的,使得任何混沌序列最终是周期的,因此,有限精度效应是混沌序列从理论走向应用的主要障碍;现有的混沌序列的研究对于所生成序列的周期,伪随机性,复杂性等的估计不是建立在(连续状态空间)统计分析上,就是通过实验给出,故难于保证其每个实现序列的周期性,伪随机性,复杂性都足够高,因而不能使人放心地采用它来加密。

本文在详细分析二维混沌系统 Hénon 映射的基础上,提出一种新颖的基于 Hénon 映射和线性反馈移位寄存器(Linear Feedback Shift Register, LFSR)为结构的混合混沌系统,结合收缩式发生器,由此设计出混合混沌的序列密码算法,并从理论和数字实验两方面对其安全性进行了评估、分析。

2 混沌系统及其特性分析

本文应用混沌理论中非常经典的 Hénon 映射作为密钥流生成函数,主要是基于两个方面的原因:一是理论上对其混沌行为的研究比较深入,二是它具有很好的密码学特性。

2.1 Hénon 映射及其特性

Hénon 映射的方程为:

$$\begin{cases} x_{n+1} = -px_n^2 + y_n + 1 \\ y_{n+1} = qx_n \end{cases} \tag{1}$$

它是一个二维的非线性混沌系统,具有很多优良特性,在非线性研究领域,对 Hénon 映射的混沌特性的研究比较深入[8,9]。本文只对其混沌行为和密码学特性进行分析。当1.050 $< p <$ 1.085, $q = 0.3$时,其部分分岔图及 $p = 1.4$, $q = 0.3$,迭代4000次的混沌吸引子如图1所示。

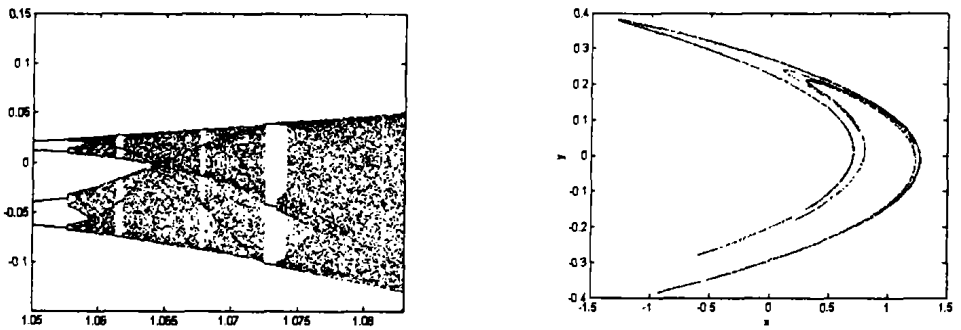


图1 Hénon 映射的分岔图和混沌吸引子

2.2 密码学特性

Hénon 映射在保密通信、混沌密码中的应用比较多[8~10]，下面我们对它的密码学特性进行定性分析。

1) Hénon 映射的一大特点是对初始值有极其敏感的依赖性。因此通过改变 Hénon 映射参数及其初始值便可以得到数量巨大的平移相异的混沌序列，即混沌序列的码量大，混沌序列的这一优点很适合于密码系统的密钥流生成函数。图2为初值仅相差10^{-4}初值迭代100次的 x 轨道图。

2)Hénon 映射具有优良的伪随机性，其轨道的演化是非周期、不收敛的，具有很好的随机性及不可预测性。我们取初值 $x=0.20, y=0.10$(作为密钥 k 的一部分)，对映射进行迭代。取序列长度 $N=5000$，相关间隔 $M=1000$，对其混沌实值序列按如下公式计算相关函数 $R_x(m)$：

$$R_x(m)=\frac{1}{N-m}\sum_{n=1}^{N-m}X_nY_{n+m}\quad m=0,1,\cdots,M$$

$$=\frac{1}{N-|m|}\sum_{n=|m|}^{N}X_nY_{n+m}\quad m=-1,-2,\cdots,-M \tag{2}$$

当取 $Y=X$ 时，其非周期自相关如图3，改变初值为 $x_0=0.2001, y=0.1001$时两个混沌序列的互相关特性如图4。可见其具有很好的密码学所需要的相关特性。

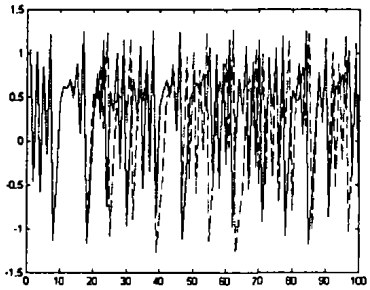


图2 混沌轨道对初值敏感性

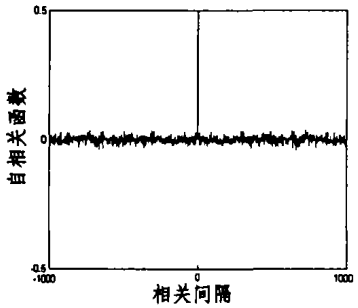


图3 自相关特性

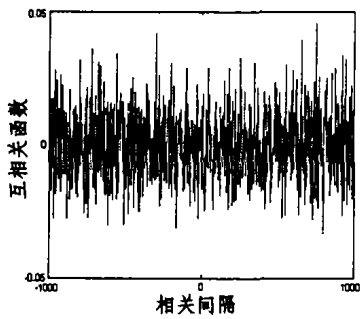


图4 互相关特性

2.3 随机二进制序列的产生

从混沌系统中提取随机二进制序列的方法比较多[8]，为提高系统的安全性，我们希望提取的方法是单向的、不可逆的，所得到的序列是随机的、最好还是统计独立且同分布的。本文采用以下方法：

首先将 Hénon 映射轨道的实数值 x(或者 y)写为：

$$|x|=0.B_1(x)B_2(x)\cdots B_i(x)\cdots, B_i(x)\in\{0,1\} \tag{3}$$

其第 i 个比特 $B_i(x)$可表示为：

$$B_i(x)=\sum_{r=1}^{2^i-1}(-1)^{r-1}\Theta_{(r/2^i)}(x) \tag{4}$$

其中 $\Theta_t(x)$是阈值函数，定义为：

$$\Theta_t(x)=\begin{cases}0 & |x|<t\\ 1 & |x|\geqslant t\end{cases} \tag{5}$$

根据 Kohda 的证明，序列$\{B_i(x_n(x))\}_{n=0}^{\infty}$($n$ 为迭代次数)确实是独立同分布的随机二进制序列。

3 混合混沌系统的设计和实现

文[11,12]详细介绍收缩密钥流生成器和自收缩密钥流生成器的设计和性能分析，并且也指出了两类密钥流生成器的等价性，但随后文[13,14]中出现了这两类生成器的一些攻击方法，这些方法表明，收缩式密钥流生成器和自收缩式密钥流生成器都是不安全的。我们已经详细地讨论了 Hénon 映射的性质，结合文[12,13]我们给出具体的混合混沌系统设计与实现，并进行相应的仿真实验。

3.1 混合混沌系统结构设计

混合混沌密钥流生成器的结构图见图5。图5中，x_n 和 y_n 是 Hénon 映射按2.3节方法提取随机二进制序列，$LFSR_1$和 $LFSR_2$是两个线性反馈移位寄存器。

3.2 算法描述

在混沌密码系统中，Hénon 映射的初值 x_0、y_0和两个线性反馈移位寄存器初态 $m_0^{(1)}, m_0^{(2)}$作为加密系统的密钥，为获得较好的随机效果，混沌系统的暂态过程即初始的 N_0次迭代不予使用。加密过程如下：

(1) 输入：两个线性反馈移位寄存器 LFSR1和 LFSR2的初态 $m_0^{(1)}, m_0^{(2)}$；Hénon 映射两个初值 x_0、y_0和控制参数 p、q；

(2)线性反馈移位寄存器 $LFSR_1$产生序列为$\{m_i^{(1)}\}$；

(3)线性反馈移位寄存器 $LFSR_2$产生序列为$\{m_i^{(2)}\}$；

(4)给定初始值 x_0和 y_0，Hénon 映射产生数字混沌序列为 $x_i^{(1)}$ 和 $y_i^{(2)}$；

(5)作运算 $s_i^{(1)}=m_i^{(1)}\oplus x_i^{(1)}, s_i^{(2)}=m^{(2)}\oplus y_i^{(2)}$；

(6)若 $s_i^{(1)}=1$；则置 $k_i=s_i^{(2)}$；若 $s_i^{(1)}=0$；则删去 $s_i^{(2)}$；

(7)输出：混合混沌序列$\{k_i|i=1,2,\cdots\}$；

(8)加密：得到的序列$\{k_i|i=1,2,\cdots\}$与明文$\{p_i|i=1,2,\cdots\}$进行异或运算得$\{c_i|i=1,2,\cdots\}$，即：$c_i=k_i\oplus p_i$。

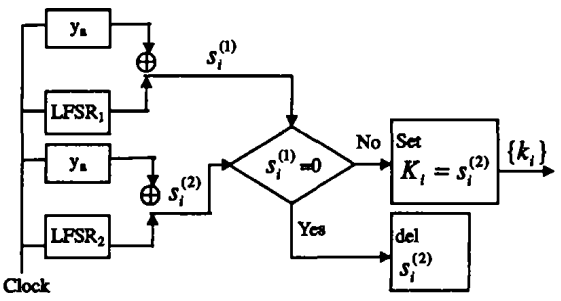


图5 混合混沌密钥流生成器

混沌系统和两个 LFSR 通过时钟控制，使它们同时开始启动。两个子系统输出的序列$\{s_i^{(1)}\}$和$s_i^{(2)}$也是通过时钟来保持同步，从而用一个序列来选择另一个序列。解密过程与加密相同。

4 模拟仿真及分析

本节主要利用计算机仿真实验来研究混合混沌加密系统的性能，我们对如下明文进行加密实验：

明文采用文[15]中给出的明文：Cryptologyist the science of overt secret writing (cryptography), of its authorized decryption (cryptanalysis), and of the rules which are in turn intended to make that unauthorized decryption more difficult (encryption security)；

系统中，Hénon 映射 $p=1.4, q=0.3, x_0=0.2345, y_0=0.1234$；$LFSR_1$的反馈多项式为：$P_1(x)=x^9+x^4+1$，其初始态为1010110011；$LFSR_2$的反馈多项式：$p_2(x)=x^{11}+x^2+1$，其初始态为10011100101。

4.1 密文分布分析

密文分布是一个密码系统最重要的特性之一，它将直接影响到密码系统的安全。一个分布不均匀密文，往往是密码分析者进行唯密文攻击的首选入口[16]。为更清晰地描述这一特性，我们使用二维图形来表达。在图6和图7中，横轴代表信息中字符出现的序号，纵轴代表对应字符的 ASCII 码值(范围0～255)。从明文和密文的图形来看，明文的码值比较集中，而根据本文所提算法所得到的密文在整个密文空间的分布都非常均匀。图8和图9分别为加密前后字符的统计分布图。也就是说，通过扩散、扰乱等作用后，密文中不包含明文的任何信息(包括明文的统计概率信息)。这正是我们想要达到的加密效果。

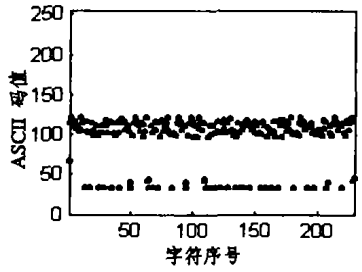


图6 明文

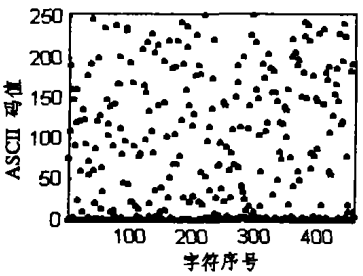


图7 密文

4.2 混乱与扩散性能分析

混乱与扩散是设计密码的两条基本指导原则。扩散是将每一位明文的影响尽可能地作用到较多的输出密文位中去，同时，还要尽量使得每一位密钥的影响也尽可能迅速地扩展到较多的密文位中去。其目的是有效隐藏明文的统计特性，这也就是混沌系统的初始条件敏感依赖性。混乱，是指密文和明文之间的统计特性的关系尽可能复杂化，这也就是混沌映射通过迭代，将初始域扩散到整个相空间。为说明本文所提算法的混乱与扩散特性，我们分别将明文初始值及控制参数作小的改变，通过分析改变前后所得密文的统计分布图情况来说明算法的扩散与混乱特性。控制参数的微小扰动，即 $p=1.4+1/2^{32}$，(误差为10^{-10}数量级)，其它参数不变；初始值的微小改变，即 $x_0=0.2345+1/2^{32}$，(误差为10^{-10}数量级)，其它参数不变。实验结果见图10和图11。同样地，解密时则需要使用与加密时完全相同的密钥，否则将不能正确得到原文。比如在解密时初值为 $x_0=0.2345+1/2^{32}$(误差为10^{-10}数量级)，其它参数不变，则从密文恢复出的内容见图12，与原文完全不同，此时解密失败。

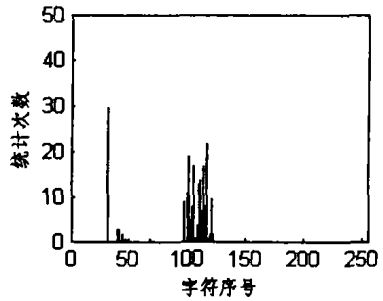


图8 明文字符统计图

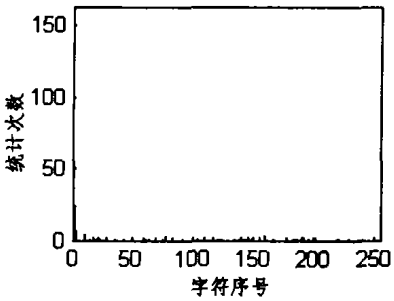


图9 密文字符统计图

4.3 周期性

从理想上说，混沌系统所产生的序列周期是无限长的，但是在实际应用中，计算机或数字电路的有限字长恶化序列的各项性能，从而使任何混沌序列都具有周期性。因此，如何克服有限精度效应使混沌应用于密码和保密通信系统是一个关键性问题。Gernak[17]采用可编程组合电路对混沌映射的系统变量或参数随机扰动来增大周期，周红[7]等人提出 m-序列的扰动来实现有限精度混沌系统。本文提出的混沌系统和传统序列密码相结合的方法，可以证明有如下定理[6]：

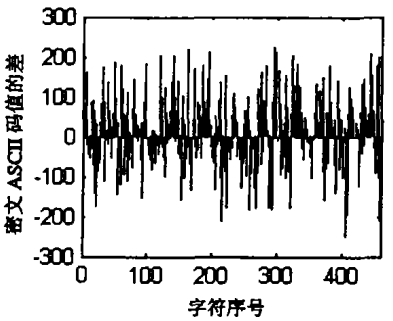
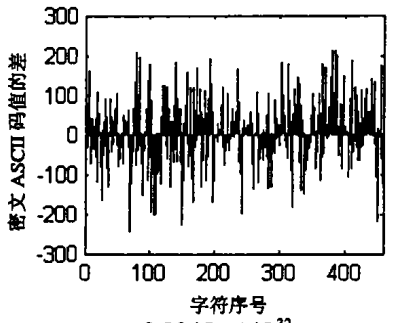


图10 密文对控制参数的敏感性

定理1 图5所示的混合混沌系统中，设 m-序列的周期为 T 和混沌序列的周期为 Q，并且，$Q \neq T$，则混合混沌序列的周期 P 是 m-序列周期 T 和混沌序列周期 Q 的最小公倍数。即 $P=[Q.T]$，其中 $1 \leqslant Q \leqslant Q_t$，$Q_t$ 混沌迭代函数的状态总数。



$x_0 = 0.2345 + 1/2^{32}$

图11 密文对初始值的敏感性

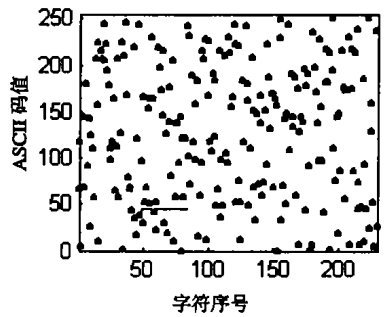


图12 参数微小失配时恢复出的明文

显然，混合混沌序列的周期不好确定，但我们知道随着时间精度的增大，混沌序列的周期也随之增大。因此，有两个因素影响图5输出序列的周期：实现精度和 LFSR 的级数。要想增大图5周期所采取的措施或是提高实现精度，或是增大 LFSR 的级数，一般高精度的实现系统必然以高成本为代价，因此要想进一步获得更大周期的混合混沌序列，可用较低精度的实现系统通过增大 LFSR 的级数来增大周期，且其周期随 LFSR 的级数增大呈指数递增。从定理1可以看出，对子系统的序列的周期取了两次最小公倍数，因此，最终输出的混合混沌序列将是非常的大，如果遇到子系统输出的序列的周期值为素数的时候，最终输出的混合混沌序列的周期的增大效果更明显。因此，虽说在有限的精度实现条件下，所有的序列会出现周期，但在增大混沌序列的周期方面，本文提出的混合混沌方法效果更明显，实现也比较简单，所用 LFSR 的级数也比较小。

4.4 抵抗密码分析的能力

因为混沌序列是由确定性的方程产生，理论上可通过相空间重构的方法预测，典型的混沌时间序列，如 Logistic、Kent、Tent、Lozi、Hénon、和 Lorenz 混沌时间序列已被成功预测，即使耦合的二维 Logistic 超混沌系统也被文[18]成功预测。但是对于混合混沌系统，由于把混沌序列和 m-序列以异或形成混合混沌序列，用一个混合混沌序列随机的选择另一个混合混沌序列作为系统的最后输出序列，这可以抵抗通过相空间重构的方法预测混沌时间序列。

结论 本文结合收缩式发生器，提出了 Hénon 映射产生的混沌序列和 m-序列相结合的混合混沌序列密码，给出了系统实现原理和算法描述，对混沌序列进行理论分析和计算机仿真，同时对该系统的产生安全性能进行了分析，如密文分布特性、扩散扰乱特性、周期性和抗密码学分析等。结果表明，混合混沌序列随机性好，周期极大，在较低精度下序列的相关性能好，且并不要求 LFSR 的级数很高，这大大降低了实现了成本，因此无论从实用角度还是从序列的性能方面来说，都不失为一种优良的伪随机序列。

参 考 文 献

1 Baptista M S. Cryptography with chaos. Physics Letters A, 1998, 240: 50～55

2 Wong K W. A fast chaotic cryptographic scheme with dynamic look-up table. Physics Letters A, 2002, 298: 238～245

3 Palacios A, Juarez H. Communication through chaotic map systems. Physics Letters A, 2002, 298: 35～41

4 Masuda N, Aihara K. Cryptosystems With Discretized Chaotic Maps. IEEE Trans. on CAS- I , 2002, 49(1): 28

5 Frey D R. Chaotic digital encoding an approach to secure communication. IEEE Trans. on circuits and systems (II), 1993, 40(10): 660～666

6 饶妮妮. 一类混合混沌序列及其性能分析. 电子科技大学学报, 2001, 20(2): 115～119

7 周红. 有限精度混沌系统的 m 序列扰动实现. 电子学报, 1997, 25(7): 95～97

8 Jridrich J. Image Encrytion Based on Chaotic Maps[J]. In: Systems, Man and Cybernetic, 1997, 'Computational Cybernetics and Simulation', 1997 IEEE Intl. Conf. on, Vol. 2, 1997

9 Erdmann D, Murphy S. Henon Stream Cipher. Electronics Letters 23rd, 1992, 28(9)

10 Kohda T, Tsuneda A. Statistics of Chaotic Binary Sequences. IEEE Trans. Inform. Theory, 1997, 43(1): 104～110

11 Coppersmith D, Kawczys H, Mansour Y. The Shrinking Generator. Advances in Cryptology -Crypto'93, Springer-Verlag, 1994. 22～39

12 Meler W, Staffetbach O. The Self-Shrinking Generator. Advances in Cryptology Eruocrypt'94, Spring-Verlag, 1995. 205～214

13 张道法, 陈伟东. 关于对 Shrinking Generator 及 Self-shrinking Generator 的熵漏分析. 通信学报, 1996, 17(4): 15～20

14 Golic J. Intrinsic Statistical Weakness of Key-stream Generator. Advances in Cryptology Eurocrypt'94, Spronger-Verlag, 1995. 91～103

15 Alvarez E, Fernández A, García P, et al. New approach to chaotic encryption. Phys. Lett. A, 1999, 263 (4-6): 373～375

16 吴世忠, 等. 应用密码学[M]. 机械工业出版社, 2000

17 Gernak J. Digital generators of chaos. Phys. Lett. A, 1996, 214: 151～160

18 Jako Z, Kis G. Application of noise reduction to chaotic communication systems. IEEE Trans. on CAS-I FTAA, 2001, 47(12): 1720～1725