一种新的混沌伪随机序列生成方式

罗启彬 张 健
(中国工程物理研究院电子工程研究所 绵阳 621900)

摘 要 利用构造的 Hybrid 混沌映射，通过周期性改变混沌迭代初值来产生混沌伪随机序列。理论和统计分析可知，该混沌序列的各项特性均满足伪随机序列的要求，产生方法简单，具有较高的安全性和保密性，是一类很有应用前景的伪随机加密序列。

关键词 混沌序列, 加密, Lyapunov 指数，自相关
中图分类号：TN918 **文献标识码**：A **文章编号**：1009-5896(2006)07-1262-04

A New Approach to Generate Chaotic Pseudo-random Sequence

Luo Qi-bin Zhang Jian
(*Institute of Electronic Engineering, CAEP, Mianyang* 621900，*China*)

Abstract This paper proposes hybrid mapping to generate chaotic sequence, by altering initial value periodically. The results show that the properties of the hybrid chaotic sequence are good，and the sequence generator can be easily realized. It is a class of promising pseudo-random sequence in practical applications.

Key words Chaotic sequence, Encryption, Lyapunov exponent, Auto-correlation

1 引言

混沌序列是一种性能优良的伪随机序列，其来源丰富，生成方法简单。通过映射函数、生成规则以及初始条件便能确定一个几乎无法破译的加密序列。因此，混沌加密受到越来越多的关注，近年来被广泛应用于保密通信领域[1-4]。

将混沌理论应用于流密码是 1989 年由Matthews[5]最先提出。迄今为止，利用混沌映射产生随机序列的理论研究很多。但是，混沌序列发生器总是用有限精度来实现，其特性由于有限精度效应会与理论结果大相径庭。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。文献[6]用m序列与产生的混沌序列“异或”来克服有限精度的影响，但由于微扰是随机的，不易产生，而且系统分布以及相关性能取决于附加的m序列而不是混沌系统本身。文献[7]通过构造变参数复合混沌系统来实现有限精度混沌系统。本文利用构造的分段非线性Hybrid映射，通过周期性地改变混沌迭代初值的办法来产生混沌序列，克服了序列有限精度效应的影响。计算机数值实验表明所产生的混沌序列的各项特性均较好，产生方法简单，具有较高的安全性，是一类很有应用前景的伪随机加密序列。

本文第 2 节给出了混沌随机序列发生器的产生过程，在此基础上讨论了混沌系统的扰动问题；第 4 节通过计算机仿真来验证所产生的混沌伪随机序列的性质；最后是结论。

2004-11-22 收到，2005-08-08 改回
中国工程物理研究院科学技术基金面上资助课题(20050429)

2 序列产生

由于 Logistic 映射和 Tent 映射的复杂度都不高，由此产生的混沌加密序列的安全性能都不是非常理想。本文把两者相结合，构造出一种新的混沌迭代映射——Hybrid 映射：

$$x_{k+1}= f(x_k)=\begin{cases} b\,(1-u_1\,x_k^2), & -1<x_k\le 0 \\ 1-u_2\,x_k, & 0<x_k<1 \end{cases} \tag{1}$$

该映射不但继承了 Logistic 映射和 Tent 映射容易产生的特点，而且还能增加混沌系统的安全性。

当初值x_0=0.82，u_1=1.8，u_2=2.0， b=0.85 时，此映射处于混沌态，产生的混沌序列如图 1 所示，其中横轴是迭代次数k，纵轴是经不断迭代得到的混沌状态空间变量$x(k)$。图 1(a)为初值等于 0.82 的Hybrid混沌映射时序图，图 1(b)为Hybrid映射对迭代初值高度敏感性的示意图(初值相差 10^{-15})。

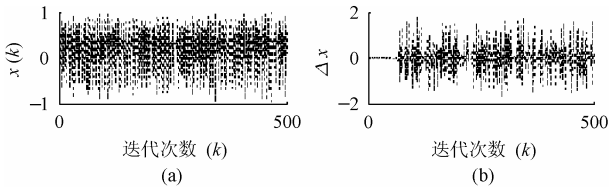

图 1 (a) Hybrid mapping 的随机特性
(b) Hybrid mapping 对初值的敏感特性
Fig.1 (a) Randomicity of Hybrid mapping
(b) Sensitivity of Hybrid mapping

把生成的实值混沌随机序列$\{x_k\}$转化为二进制随机序列$\{S_k\}$，按如下方法实施：

第 1 步 用l位无符号定点小数来表示实数$|x_k|$，即$|x_k|$ =

$0.b_{l-1}b_{l-2}\cdots b_1b_0$，式中$|x_k|$用$l$位二进制数$b_i$表示，$i$ =0,1 ,…, l–2, l–1，b_i的取值为 0 或 1。l越大，则表示的数据精度越高。

第 2 步　对小数化后的随机序列$\{x_k\}$，统一取其第i位b_i(b_i的取值为 0 或 1)二进制数组成一个新的序列$\{b_i\}$。

第 3 步　为了进一步增加算法的随机性，提高序列的抗破译能力，使得对初始条件的攻击无效，加密时截掉序列的初始段部分和结尾部分。假设序列$\{b_i\}$的长度为L，任取截点N_1，N_2(即预迭代次数)，满足 1< N_1< N_2< L。

通过以上处理，得到所需要的二进制随机序列$\{S_k\}_{k=N_1}^{N_2}$，该序列的长度为(N_2−N_1+1)。与单一的Logistic映射或Tent映射相比，本文提出的Hybrid映射，其序列产生算法更加复杂，输出序列也更随机和不可预测，极大地增强了系统的保密性。本算法的保密性不但依赖于混沌系统的参数，而且还依赖于保密系统的初始值和“预迭代次数”等参数。这样，加密系统的密钥可包括迭代参数：b ，u_1， u_2，迭代初值x_0，量化比特位置i及预迭代次数N_1，N_2，即加密密钥为 {b u_1 u_2 x_0 i N_1 N_2}，使得密码分析更加困难。

3　混沌序列的有限精度实现

由于实际计算中存在的有限精度效应，混沌序列在迭代过程中必将退化为周期序列，而且生成的序列的密码特性和周期也难以度量。为了获得周期足够长的密钥流序列，可用不同的初始值x_{0j} (j=1,2 ,…, M)分别对Hybrid映射进行迭代，如取x_{0j}=sin(2πjt), j=1,2 ,…, M, $M\in Z^+$，得到M组不同的混沌伪随机序列；然后对结果进行非线性组合，可获得周期至少为M×N的序列，其中N是序列$\{S_k\}$的周期。

4　混沌伪随机序列的特性分析

4.1　Lyapunov 指数估计

利用 Lagrange 中值定理，可以推得 Lyapunov 指数计算式为

$$\lambda=\lim_{N\to\infty}\frac{1}{N}\sum_{k=2}^{N-1}\ln\left|\frac{x_{k+1}-x_k}{x_k-x_{k-1}}\right| \tag{2}$$

通过计算可得所产生的 Hybrid 序列的 Lyapunov 指数 λ =1.18142，这要比单纯的 Logistic 混沌映射的 Lyspunov 指数 λ≤0.7 大。可见，与 Logistic 映射系统相比，本文构造的 Hybrid 混沌系统的运动轨道更加不稳定，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。

4.2　初值敏感性

任取两个Hybrid混沌映射的迭代初始值(相差仅 10^{-15})，大约经 60 次迭代后，两个序列变得完全不同，说明该Hybrid混沌系统依然保持了类似Logistic混沌映射的初值高度敏感特性，如图 1(a)所示。正因为混沌序列对初始值非常敏感，即使密钥值有微小的变化也会得到完全不同的解密结果，所以说该混沌序列适合于加解密系统。

4.3　PN序列检验[8,9]

首先用Golomb提出的 3 个随机性公设来检验本文产生的混沌二进制序列$\{S_k\}$的特性。

取迭代初值x_0=0.82，参数u_1=1.8，u_2=2.0， b=0.85，迭代次数N =10000, 按第 2 节所述的序列生成方法，得一长度为 8192 的二进制随机序列$\{S_k\}$。

通过统计，该二进制混沌序列$\{S_k\}$中‘0’的个数N_0=4081，‘1’的个数N_1=4111，N_0/N_1=0.9927。

理论上二进制伪混沌序列的 0-1 比计算公式为

$$r_{01}=\lim_{L\to\infty}\frac{N_0(J)}{N_1(J)}=\frac{1-\int_0^L\int_0^L T_n(x,y)P(x,y)\mathrm{d}x\mathrm{d}y}{\int_0^L\int_0^L T_n(x,y)P(x,y)\mathrm{d}x\mathrm{d}y}=1 \tag{3}$$

其中$N_0(J)$和$N_1(J)$分别表示$\{S_k\}_{L=\infty}^{J}$中‘0’和‘1’的个数。

由此可以得出该二进制混沌序列$\{S_k\}$有均衡的 0-1 比，满足Golomb伪随机假设的第 1 条件。

对该二进制混沌序列$\{S_k\}$进行游程统计，结果见表 1 所示。

表 1　二进制随机序列$\{S_k\}$的游程统计分析表

Tab.1 The runpath analysis of sequence$\{S_k\}$

	N_0	N_1	N_0/ N_1	占总游程的比例(实验)(%)	占总游程的比例(理论)(%)
游程长为 1	4081	4111	0.9927	49.81	50.00
游程长为 2	1999	2030	0.9852	24.40	25.00
游程长为 3	991	1035	0.9575	12.10	12.50
游程长为 4	497	504	0.9861	6.07	6.25
游程长为 5	244	251	0.9721	2.98	3.125

从表 1 中可以看出该方法生成的二进制混沌序列$\{S_k\}$中长度为L的‘0’串和‘1’串个数大致相等，且占整个二进制序列总游程个数的 1/2^L，满足Golomb伪随机假设的第 2 条件。

序列的自相关及互相关性检验：

序列的均值：

$$s_{\mathrm{mean}}=\lim_{N\to\infty}\frac{1}{N}\sum_{i=0}^{N-1}s_i \tag{4}$$

其自相关函数：

$$R(m)=\lim_{N\to\infty}\frac{1}{N}\sum_{i=0}^{N-1}(s_i-s_{\mathrm{mean}})(s_{i+m}-s_{\mathrm{mean}}) \tag{5}$$

互相关函数：

$$C(m)=\lim_{N\to\infty}\frac{1}{N}\sum_{i=0}^{N-1}(s_i-s_{\mathrm{mean}})(s'_{i+m}-s_{\mathrm{mean}}) \tag{6}$$

其中$\{S_k\}$和$\{S'_k\}$为不同初值的两个二进制混沌序列。

图 2 是二进制序列的自相关和互相关特性图，可以看出此二进制序列$\{S_k\}$具有类似δ-like的性质，有尖锐的自相关和良好的互相关特性，满足Golomb伪随机性假设的第 3 个条件。因此，Hybrid 映射通过上述方法产生的二进制序列$\{S_k\}$的确为PN序列。

由于受有限精度效应的影响，Logistic 映射产生的二进制混沌序列会出现短周期的行为(在 16 位有效计算精度条件下)，其自相关函数会出现等间隔的峰值，不再为 δ-函数(如图 3 所示)。而本文提出的 Hybrid 映射，通过上述方法产生的二进制序列的相关性能接近理论结果。

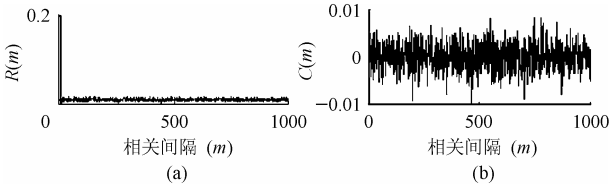

图 2（a）序列$\{S_n\}$的自相关特性（b）序列$\{S_n\}$的互相关特性

Fig.2 (a) Auto-correlation properties of $\{S_n\}$
(b) Cross-correlation properties of $\{S_n\}$

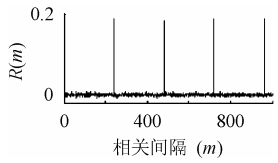

图 3 有限精度下 Logistic 映射的自相关特性

Fig.3 Auto-correlation properties of Logistic mapping under finite precision

4.4 序列密码的局部随机性统计检验

任何一种密钥序列如果要在密码体制中用于加密，除必须很像随机序列外，还需对序列的各个段落进行统计性检验，这是密钥序列设计中所必须的。

首先定义检验的显著性水平α=5%，并假定伪随机序列$\{S_k\}$的长度为N，其中‘0’和‘1’的个数分别为N_0，N_1。

(1) 频率检验 利用 $\chi^2=(N_0-N_1)^2/N$，可算得 χ^2=0. 117，低于显著性水平 5%所对应的 χ^2 值(3.95)，说明该方法产生的伪随机序列中‘0’和‘1’的个数大致相同。

(2)序列检验 序列检验用来判定转移概率是否合理，即出现相同和相异的相邻元素的概率大致相等。设N_{00}，N_{01}，N_{10}，N_{11}分别表示‘00’，‘01’，‘10’，‘11’出现的次数，统计结果表明序列检验的以下 3 个关系式均成立：

$$N_{00}+N_{01}=N_0-1 \tag{7}$$

$$N_{10}+N_{11}=N_1-1 \tag{8}$$

$$N_{00}+N_{01}+N_{10}+N_{11}=N-1 \tag{9}$$

并且利用戈德关系式可得

$$\frac{4}{N-1}\sum_{i=0}^{1}\sum_{j=0}^{1}(N_{ij})^2-\frac{2}{N}\sum_{i=0}^{1}(N_i)^2+1\approx 4.33 \tag{10}$$

而 2 自由度的 χ^2 分布在 5%的显著性水平下对应的值为 5.99，所以序列检验也能通过。

(3)扑克检验 将所产生的二进制序列$\{S_k\}$分成大小为 8 的分组，然后计算长度为 8 的每一种分组出现的频率。设这些频率分别是f_1，f_2,…,f_{255}。通过计算可得

$$F=\sum_{i=0}^{2^m-1}f_i=\sum_{i=0}^{255}f_i=8159 \tag{11}$$

于是有

$$\chi^2=\frac{2^m}{F}\sum_{i=0}^{2^m-1}(f_i)^2-F=231.89 \tag{12}$$

与对应的 5%显著性水平的扑克检验值(为 241.7)相当。

统计结果与理论分析表明，采用本文提出的方法产生的混沌序列完全能通过随机性检验，具有优良的伪随机性能及相关特性；而且与单一的 Logistic 映射或 Tent 映射相比，系统复杂度更高，运动轨道更加不稳定，输出序列也更随机和不可预测，因此对该序列的分析预测就更加困难。加上利用周期性的扰动迭代初值来克服有限精度的影响，使得密钥序列分布在 $M\times N$ 个混沌轨道上(相应密钥空间扩大了 M 倍)，破坏了混沌密钥轨道的相关性。这样即使密码分析者得到连续的密文序列，并利用构造函数向后进行迭代得到 M 个序列值，但由于得到的密文序列值在不同的混沌轨道中，此后的值与明文无关。因此本文产生的混沌序列加密系统能够抵抗频谱分析和搜索攻击。

5 结束语

本文所设计的伪随机密钥流产生算法是利用周期性的扰动迭代初值来产生混沌序列，不但扩展了序列的周期，增加了有限精度实现时输出伪随机序列的长度，而且能使产生的序列更加混乱和不可预测，相应地增强了系统的安全性，克服了 Logistic 映射加密易于攻击的缺点。由于系统设计时所采用的预迭代次数控制方法以及有限精度实现时的非线性处理有效地克服了攻击者对系统状态的预测；而其自身良好的统计特性有效地克服了对系统的统计攻击；仿真结果显示该混沌序列的各项特性均满足伪随机序列的要求，具有较高的安全性和保密性，是一类很有应用前景的伪随机加密序列。

参 考 文 献

[1] Frey D R. Chaotic digital encoding: An approach to secure communication. *IEEE Trans.on Circuits and Systems*, 1993, 40(10): 660−666.

[2] Toni Stojanovski, Liupc čo Kocarev. Chaos-based random number generators—part I: analysis [J]. *IEEE Trans.on Circuits Syst.-I*, 2001, 48(3): 281−288.

[3] Toni Stojanovski, Johnny Pihi, Liupc čo Kocarev. Chaos-based

random number generators—part II: practical realization [J]. *IEEE Trans.on Circuits Syst.-I*, 2001, 48(3): 382−385.

[4] 王育民. 混沌密码序列实用化问题. 西安电子科技大学学报, 1997, 24(4): 560−562.

[5] Robert Matthews. On the derivation of a “chaotic” encryption algorithm.*Cryptologia*,1989, 13(1): 29−42.

[6] 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): 95−101.

[7] 张巍, 李德华. 一种新的混沌序列生成方式. 华中科技大学学报, 2001, 29(11): 64−66.

[8] 丁存生, 肖国镇. 流密码学及其应用. 北京: 国防工业出版社, 1994: 251−254.

[9] 张凤仙. 通信保密技术. 北京: 国防工业出版社, 2003: 34−39.

罗启彬： 男，1972 年生，博士，工程师，主要研究方向为混沌保密通信、纠错编码等.

张　健： 男，1968 年生，博士生导师，研究员，主要研究方向为非线性理论、软件无线电等.