一类混合混沌序列及其特性分析*

饶妮妮**

(电子科技大学自动化系 成都 610054)

【摘要】提出将 Logistic 混沌序列与 m 序列以异或方式结合形成一类混合混沌序列的方法．用理论与统计分析相结合的方法对该混合混沌序列的周期、平衡性、相关性及线性复杂度等特性进行了系统分析．分析结果表明：该混合混沌序列的各项特性均较好，产生方法简单，可用数字电路实现，是一类很有应用前景的伪随机序列．

关 键 词 Logistic 映射； m 序列； 混合混沌序列； 周期； 伪随机特性

中图分类号 TN919

在许多应用系统，如密码、扩/跳频通信等系统中，都要用到伪随机序列[1,2]。伪随机序列特性的好坏对系统性能有直接的影响。寻求好的伪随机序列一直是密码、扩/跳频通信等领域的学者们需要解决的难题。混沌现象一经发现，它的类随机性就十分引人注目，迄今为止，利用混沌映射产生随机序列的理论研究已很成熟[3~6]。然而，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[7]。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。将混沌系统与移位寄存器序列混合，可以克服有限精度效应对混沌系统的影响，从而改善混沌序列特性。本文提出将 Logistic 混沌序列与 m 序列以异或方式结合形成一类混合混沌序列。对这类混合混沌序列的周期、平衡性、相关性以及线性复杂度等特性进行了系统分析，为混合混沌序列的应用开辟了一条途径。

1 混合混沌序列的产生

本文的混合混沌序列产生方法如图1所示。该方法是混沌序列发生器和 m 序列发生器以异或方式结合，属于混合混沌系统。m 序列具有良好的伪随机特性，其特性的理论分析已很成熟，且产生方法也十分简单。用 m 序列发生器与混沌序列发生器的结合无疑会简化分析。目前，产生混沌序列的方法很多，例如，Logistic 映射、Tent 映射、Chebyshev 映射以及分段线性映射等[8]。其中，Logistic 映射算法简单，对其研究也最为透彻。因此，图1中的混沌序列选用 logistic 映射产生。Logistic 映射的算法如下

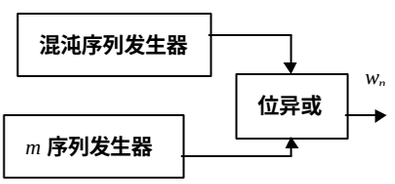

图1 混合混沌序列产生方框图

$$a_{t+1}=1-2a_t^2 \qquad a_t \in I=[-1,1] \tag{1}$$

由式(1)产生的混沌序列是数值在 I 上遍历且具有均匀的不变分布函数 $f(a)$=0.5的实数序列[9]。对实数序列进行量化，得到0-1二进制混沌序列 $\{b_n(t)\}\big|_{t=1}^{\infty}$。不同的量化函数对混沌二进制序列的自相关、互相关和平衡性产生的影响不同。现有多种量化方法，为了便于硬件实现，本文选用的量化方法是：将实值 $\{a_t\}$ 的绝对值的有效值用 m 比特来表示为 $|a_t|=0.b_1(a_t)b_2(a_t)\cdots b_n(a_t)\cdots b_m(a_t)$，其中 $b_n(a_t)\in(0,1)$。取每一个实数值 $\{a_t, t=1,2,\cdots,\infty\}$ 的第 n 比特，便得到二进制混沌序列 $\{b_n(t)\}\big|_{t=1}^{\infty}$。

2000年12月8日收稿
* 国防科研基金资助项目
** 女 37岁 硕士 副教授

将二进制混沌序列 $\{b_n(t)\}_{t=1}^{\infty}$ 与 m 序列按位异或运算即可得到混合混沌序列 $\{w_n, n=1,2,\cdots\}$。可见，混合混沌序列的产生方法十分简单。

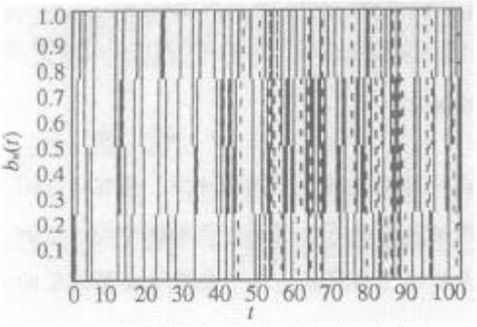

图2 混合混沌系统的初值敏感性

2 混合混沌序列的特性

2.1 初值敏感性

Logistic 混沌系统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 Logistic 混沌系统的参数及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用于加/解密系统、扩/跳频系统。本文用统计分析的方法对混合混沌序列的初值敏感性进行了研究，结果如图2所示。

在图2的混合混沌序列中，取两个 Logistic 混沌映射的初值仅相差 10^{-14}，m 序列的级数 $L=42$，任意选取初值。经大约43次迭代后，混合混沌序列一分为二，成为两个平移相异的序列，说明混合混沌系统仍然保持了 Logistic 混沌映射的初值敏感性，即混合混沌序列的数量仍然巨大。

2.2 周 期

定理 1 图1所示混合混沌系统中，设 m 序列的周期为 T 和混沌序列的周期为 Q，并且 $Q \nmid T$，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 $1 \leqslant Q \leqslant Q_S$，$Q_S$ 为混沌迭代函数的状态总数。

证明 系统输出周期 p 是 m 序列周期 T 和混沌序列周期 Q 的最小公倍数，即 $p=[Q, T]$。在二元域上异或运算就是相加运算。由于 m 序列的运行状态与混沌序列的运行状态独立，且 m 序列的状态数与混沌序列的状态数不等，所以包括状态数为 Q 的混沌序列和状态数为 T 的 m 序列的全系统，从某一初始状态起又回到该初始状态经历的状态数只可能是 Q 和 T 的最小公倍数。若 Q 和 T 互素，则图1系统输出序列的周期 $p=QT$。

根据混沌现象的产生机理知，理论上 Logistic 混沌序列是非周期的。由于任何混沌序列只能用有限精度设备来生成，所以混沌序列的状态数实质都是有限的。设 Q 代表 Logistic 混沌序列在某个初值下的有限状态数(即周期)，受有限精度效应的影响，混沌系统可能出现不动点现象，即 Q 的最小值可为1，若设混沌序列的最大状态数为 Q_S，则在不同的初值条件下，$1 \leqslant Q \leqslant Q_S$。 证毕

大量仿真实验也证实了定理1的正确性。尽管难以控制混沌序列的周期，但可以通过选择 m 序列的周期来满足实际应用中对序列周期的要求。显然，图1所示混合混沌系统有效地克服了混沌系统因有限精度效应而产生的短周期行为，使混合混沌系统可用数字化的方法实现。

2.3 平衡性

定理 2 在图1的混合混沌系统中，若混合混沌序列为0-1的二元序列，则在 m 序列的一个周期 T 内，混合混沌序列中0-1出现次数均值的差不大于1。

证明 设 m 序列的级数为 L，则周期为 2^L-1。在一个周期内 m 序列中“0”的个数为 $2^{L-1}-1$ 个，“1”的个数为 2^{L-1} 个。又设混合混沌序列中，出现“1”的概率为 $p(1)$；出现“0”的概率为 $p(0)$，且 $p(1)+p(0)=1$。因此，在一个 m 序列的周期 T 中“1”出现次数的均值为

$$num(1)=(2^{L-1}-1)p(1)+2^{L-1}p(0)=2^{L-1}-p(1)$$

“0”出现次数的均值为

$$num(0)=(2^{L-1}-1)p(0)+2^{L-1}p(1)=2^{L-1}-p(0)$$

两者之差为

$$\Delta num=|num(1)-num(0)|=|p(0)-p(1)|<1$$ 证毕

定理 3　在图1所示的混合混沌系统中，若混合混沌序列为0-1的二元序列，则在 m 序列的一个周期 T 内，“00”、“01”、“10”、“11” 出现次数(二维均匀性)任意两者均值的差不大于1。

证明　设 m 序列的级数为 L，则周期为 2^L-1。由 m 序列的广义平衡性知，在一个周期内，“00” 的个数为 $2^{L-2}-1$ 次，“01”、“10”、“11” 的个数为 2^{L-2} 次。又设混合混沌序列中，出现 “00” 的概率为 $p(00)$ 次；出现 “01” 的概率为 $p(01)$；出现 “10” 的概率为 $p(10)$；出现 “11” 的概率为 $p(11)$，且 $p(00)+p(01)+p(10)+p(11)=1$。因此，在一个 m 序列的周期 T 中，“00” 出现次数的均值为 $num(00)=(2^{L-2}-1)p(00)+2^{L-2}(p(01)+p(10)+p(11))=2^{L-2}-p(00)$。同理，“01”、“10”、“11” 出现次数的均值分别为

$$num(01)=(2^{L-2}-1)p(01)+2^{L-2}(p(00)+p(10)+p(11))=2^{L-2}-p(01)$$
$$num(10)=(2^{L-2}-1)p(10)+2^{L-2}(p(00)+p(01)+p(11))=2^{L-2}-p(10)$$
$$num(11)=(2^{L-2}-1)p(11)+2^{L-2}(p(00)+p(01)+p(10))=2^{L-2}-p(11)$$

所以任意两者之差

$$\Delta num=|num(i)-num(j)|=|p(i)-p(j)|<1$$

其中　$i,j=00,01,10,11$，$i\neq j$。　　证毕

定理2、3从理论上确保了混合混沌序列有好的平衡性。对500组(每组混沌映射和 m 序列的初值不同)长度为1 024 bit 的混合混沌序列进行 $c^2(0.05)$ 测试，通过率为 99% ，理论分析与统计分析吻合。

2.4　相关特性

2.4.1　周期自相关和周期互相关

伪随机序列 $\{x_t\}$ 的周期相关函数定义为

$$q(t)=\lim_{N\to\infty}\frac{\sum_{t=1}^{N}x_t x'_{t+t}}{\sum_{t=1}^{N}x_t x_t}\qquad t=0,1,2,\cdots \tag{2}$$

式中　N 为序列长度；t 为移位长度。当 $\{x_t\}$ 和 $\{x'_t\}$ 为同一序列时，$q(t)$ 代表自相关，通常用 $q_a(t)$ 表示；当 $\{x_t\}$ 与 $\{x'_t\}$ 不是同一序列时，$q(t)$ 代表互相关，通常用 $q_c(t)$ 表示。

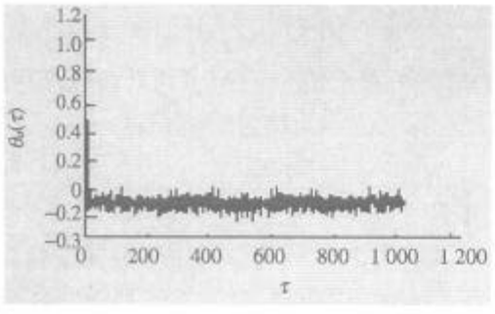

图3　混合混沌序列的自相关函数

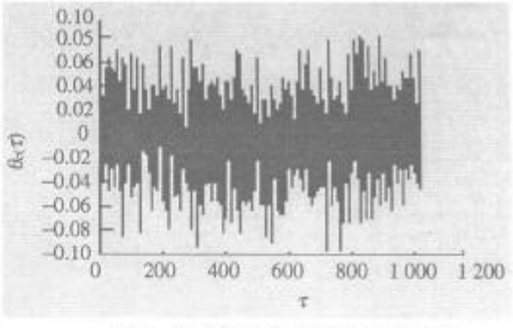

图4　混合混沌序列的互相关函数

在密码学、扩/跳频通信等应用领域中，要求伪随机序列具有 d -like 的自相关和为零的互相关。m 序列具有十分理想的周期自相关函数，但具有好的互相关特性的 m 序列数量较少。Logistic 映射产生的混沌序列则具有理想的自相关和互相关[9]。目前，研究混合混沌序列周期相关特性的有效方法是随机选择一些序列作为样本进行大量统计计算。1000组长度为1. 024 bit 的混合混沌序列周期自、互相关函数的均值分别如图3、4所示。由图3和图4知，混合混沌序列具有近似 d -like 的自相关函数，归一化最大旁瓣值仅为0.09，而单纯的混沌序列在同等序列长度下，归一化周期自相关最大旁瓣值不低于0.1[6]；混合混沌序列也具有近似为零的互相关函数，其归一化最大互关值为0.08，

单纯的混沌序列在同等序列长度下，归一化周期互相关最大值不低于0.09[6]。

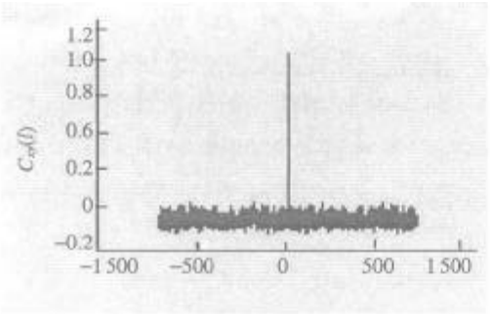

图5 混合混沌序列的部分自相关函数

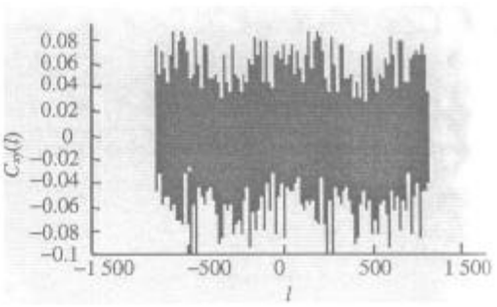

图6 混合混沌序列的部分互相关函数

2.4.2 部分自相关和部分互相关

许多应用领域除要求伪随机序列有较理想的周期相关特性外，还要求序列有较好的部分相关特性。部分相关函数定义为

$$C_{xy}(l)=\begin{cases}\sum_{i=0}^{N-1-l} x_i y_{i+l} & 0\leqslant l\leqslant N-1\\ \sum_{i=0}^{N-1+l} x_{i-l} y_i & 1-N\leqslant l\leqslant 0\\ 0 & |l|>N\end{cases} \tag{3}$$

式中 N 为序列长度；l 为移位长度。 同理，若$\{x_t\}$和$\{y_t\}$为同一序列时，$C_{xy}(l)$代表部分自相关；若$\{x_t\}$和$\{y_t\}$为不同序列时，$C_{xy}(l)$则代表部分互相关。

500组长度 $N=1\ 024$ bit 的混合混沌序列的统计部分自相关和部分互相关函数如图5、6所示。由图可知，混合混沌序列有较理想的部分自相关，其最大旁瓣值仅为0.09；同时具有较理想的部分互相关，互相关最大值为0.09。

2.5 线性复杂度

从理论上获得混合混沌序列线性复杂度的表达式尚有困难。用 Massey 算法进行统计分析的结果如图7所示。可见，混合混沌序列具有较理想的线性复杂度曲线，即 $LC\approx N/2$(N 为序列长度)。

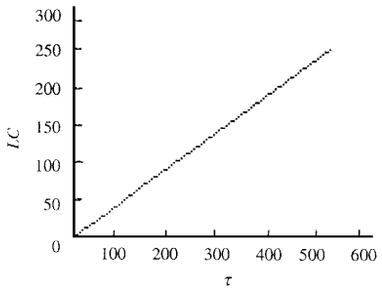

图7 混合混沌序列的线性复杂度曲线

3 结 论

将 Logistic 离散混沌映射产生的混沌序列与 m 序列以异或方式结合得到的混合混沌序列能综合 Logistic 混沌序列和 m 序列的优点，克服两者的缺点。该序列周期长并且可控、序列数量大(对初值敏感)、平衡性好、具有近似 d -like 的自相关和近似为零的互相关以及较理想的部分相关特性，且线性复杂度高。其产生方法也十分简单，并能克服有限精度效应，因而可用数字电路实现，是一类很有应用前景的伪随机序列。

参 考 文 献

1 Rao Nini. The study of the spreading codes combined multiple access and encryption for A-CDMA system. Journal of University of Electronic Science and Technology of China, 1999, 28 (5):451~454[饶妮妮. A-CDMA 系统多址与保密结合的扩频码研究. 电子科技大学学报, 1999, 28 (5):451~454]

2 Rao Nini, Gong Yanhuan. Analysis of KM $\overline{M}$ dock controlled sequence properties. Journal of University of Electronic Science and Technology of China, 1994, 23(4):363~369 [饶妮妮，龚耀寰. $KM\overline{M}$ 钟控序列特性分析. 电子科技大学学报. 1994, 23(4):363~369]

3 Kohda Tohur, Tsuneda Akio. Pseudonoise sequences by chaotic nonlinear maps and their correlation Properties. IEICE Trans Commun, 1993, E97－B (8): 855~862

4 凌　聪, 孙松庚. Logistic 映射跳频序列. 电子学报，1997, 25(10): 107~110

5 Li T Y, York J A. Period three implied chaos. Amer Math Monthly , 1975, 12(82): 985~992

6 Rao Nini. A class of Chaotic spreading codes for A-CDMA system. Journal of University of Electronic Science and Technology of China, 2000, 29(5): 465~468 [饶妮妮. 一种适于作 A-CDMA 系统扩频码的混沌序列. 电子科技大学学报, 2000, 29(5): 465~468]

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 胡健栋. 码分多址与个人通信. 北京: 人民邮电出版社, 1996

9 王　亥, 胡健栋. 改进型 Logistic-Map 混沌扩频序列. 通信学报，1997(8): 71~77

Property Analysis of a Class of Mixed Chaotic Sequences

Rao Nini

(Dept. of Automation, UEST of China　Chengdu　610054)

Abstract　A class of mixed chaotic sequence, which is produced by combining logistic sequence and *m* sequence in the form of exclusive-OR, is presented in this paper. The period, balance, correlation and linear complexity for a class of mixed chaotic sequences are analyzed systematically. The results show that the properties of the mixed chaotic sequence are good, and the sequence generator can be easily realized by the use of digital circuits. It is a class of promising pseudo-random sequence in practical applications.

Key words　logistic mapping; *m* sequence; mixed chaotic sequence; period; pseudo-random property