

一类数字混沌系统的有限精度实现

Implementation of a Class of Digital Chaotic Systems with Finite Precision

王宏霞 虞厥邦

(电子科技大学光电子技术系570实验室 成都610054)

Abstract This paper presents a method to implement digital chaotic systems with finite precision via composing LFSR sequences. The period and correlation are studied under different order of LFSR. An application of information security is an example for this approach.

Keywords Finite precision effect, Chaotic sequence, Correlation function

1 引言

混沌现象作为一种随机现象在20世纪60年代首先被气象学家 Lorenz 发现^[1],此后用非线性差分方程映射产生的混沌数字序列在物理学、密码学以及信息安全等领域的应用都有大量报导,混沌的应用研究已受到广大学者的重视。混沌由于对初始条件的极端敏感性而具有高度的随机性,可作为产生密钥流的伪随机序列发生器,优点是统计性能好、实现简单且码源丰富。理想的混沌系统其状态是无限不重复的,但作工程实现时,计算机或数字电路的有限字长效应恶化了序列的各项性能,如文[2]指出的短周期行为难以避免。文[3]认为计算精度、所采用的机器甚至语言类型都可能影响有限精度混沌系统的最终结果,精度越高,开销越大,因此有限精度混沌系统的数字实现研究具有重要意义。Gernak^[4]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^[5]等人提出用 m 序列的扰动来实现有限精度混沌系统,并指出混沌序列所需要达到的周期越大,则 m 序列的阶数也越大;扰动下的自相关函数周期峰在 m 序列的周期的整数倍的位置出现,到底是多少倍,目前还未见报导。因此,加扰后的混沌序列的周期和 m 序列的周期的精确关系式不好确定。本文采用合成线性反馈移位寄存器(LFSR)码序列来实现有限精度 Logistic 映射数字混沌序列,并分析了其自相关性能,以及所需达到的数字混沌序列周期与 LFSR 码序列周期的精确关系,从而为 LFSR 级数的选择提供了依据,最后给出了在信息安全上的应用。

2 数字混沌序列的有限字长效应

我们采用如下 Logistic 映射来产生混沌序列:

$$x_{n+1} = f(x_n) = 1 - 2x_n^2 \quad x \in [-1, 1] \quad (1)$$

将式(1)产生的实值混沌序列变换成 GF(2)域中的二进制序列:

$$a_n = (\text{sgn}(x_n) + 1) / 2 \quad n = 0, 1, 2, \dots, N-1 \quad (2)$$

其中 $\text{sgn}(\cdot)$ 是符号函数, N 为序列周期。

文[6]证明了 Logistic 映射的测度熵为1,从而它产生的二进制序列 a_n 为 Bernoulli 序列,其自相关函数为 δ 函数。当混沌系统的实现精度 $L < \infty$ 时,即在有限字长条件下,产生的二进制数字混沌序列会出现短周期行为,其自相关函数会出现等间隔的旁峰。我们在8位精度条件下,初值为0.735时,对 Logistic 混沌映射进行了仿真,得到的二进制数字混沌序列为10100010110001101110110100100101001……,可见迭代不久便出现了周期。图1和图2分别是在8位精度和16位精度条件下的二进制混沌序列的自相关函数值,从图中可看出自相关函数不再为 δ 函数,而出现了周期峰,实现精度越高,周期峰的间隔越大,而峰值减小,这说明在有限精度条件下实现数字混沌系统,序列的性质会与其理论结果有很大的差距。现在我们把混沌序列的实现精度提高到32位,得到的数字混沌序列的自相关函数值如图3所示,可以看出随着混沌序列实现精度的提高,其自相关性能越来越接近理论结果。

3 有限精度实现数字混沌系统的方法

由第2节的分析可知,提高精度,可以改善混沌序列的性能,精度越高,序列的相关性和安全性越接近于理想序列,但同时也加大了电路的硬件复杂度和成本。在有限的精度条件下,为了使输出的二进制混沌序列自相关性能接近于理论结果,在这一节提出了解决有限精度实现数字混沌序列的方法。图3是有限精度数字

混沌系统实现的框图, M_0 是 LFSR 的初态, $M_0 = (m_{01}, m_{02}, \dots, m_{0n})$, n 为 LFSR 的级数, m_i 为 LFSR 的最大周期输出, 即 m 序列, L 为混沌系统的实现精度, x_0 为

其初始值, 有限精度实现条件下的混沌系统经过式(2)的二进制化处理, 得到的数字混沌序列 a_i 和 m_i 作异或运算, 从而输出二进制序列 k_i 。

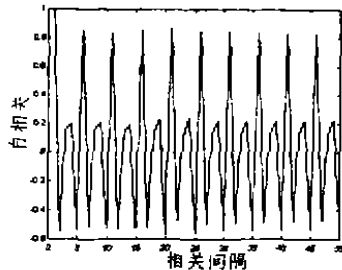


图1 8位精度数字混沌序列的自相关

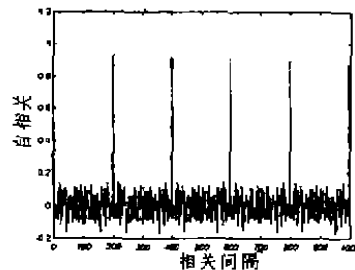


图2 16位精度数字混沌序列的自相关

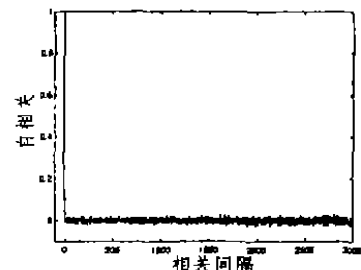


图3 32位精度数字混沌序列的自相关

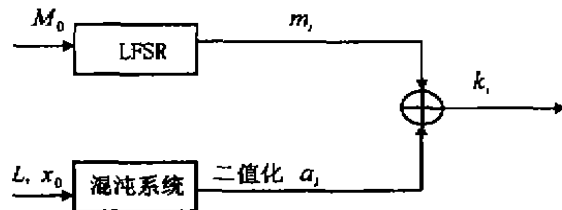


图4 有限精度数字混沌系统的 LFSR 合成实现结构

4 仿真结果

我们取 $L=8, n=4$, 采用的 m 序列的特征多项式为 $p_1(x) = 1 + x + x^4$, 得到的数字混沌序列的自相关函数值如图5所示, 与图1比较, 可以看出在同样的精度下, 自相关函数的旁峰之间的距离增大, 这说明经过低阶 LFSR 码序列合成处理的数字混沌序列的自相关性有了一定程度的改善, 这种方法可以增大有限精度实现混沌序列的周期, 现在我们增大 LFSR 的级数, 取 n

$=7$, 采用的 m 序列的特征多项式为 $p_2(x) = 1 + x + x^7$, 得到的数字混沌序列的自相关函数值如图6所示, 与图5比较, 可以看出在同样的精度下, LFSR 的级数越大, 自相关函数的旁峰间隔越大, 且旁峰减小。设 T_m 为 m 序列的周期, T_c 为混沌序列的周期, 则周期峰出现的位置在 $lcm(nT_m, T_c)$ ($lcm(\cdot)$ 表示最小公倍), 这说明经 LFSR 码序列合成处理的数字混沌序列的周期能够确定下来, 即为 $lcm(nT_m, T_c)$ 。我们知道 $T_m = 2^n - 1$, 为了最大限度地增大混沌序列的周期, 选择的 LFSR 的级数就要满足 nT_m 和 T_c 互素。我们取 $L=16, n=10$, 采用的 m 序列的特征多项式为 $p_3(x) = 1 + x^3 + x^{10}$, 得到的数字混沌序列的自相关函数如图7所示, 与图2、图3比较, 可以看出在16位精度下, 经 LFSR 码序列合成处理的数字混沌序列的自相关性能有了很大改善, 其自相关性能可以达到与32位精度实现混沌序列差不多的程度。

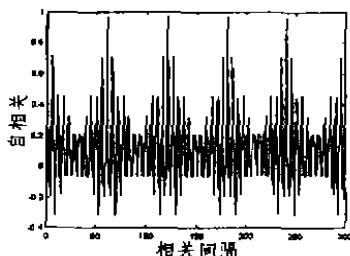


图5 $L=8, n=4$

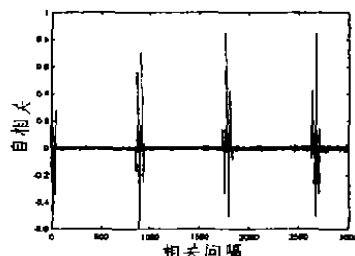


图6 $L=8, n=7$

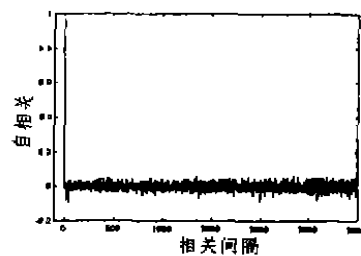


图7 $L=16, n=10$

5 在信息安全上的应用

采用本文提出的 LFSR 合成实现有限精度数字混沌系统的方法, 得到的二进制混沌序列可作为加密信息的密钥流生成器, 对照图4, 下面是该密钥流生成器的描述。

输入: 参数: 一个 n 级最大长 LFSR, 一个混沌模型。

密钥: 混沌系统的模型参数和初始值 x_0 , LFSR 的初态 M_0 。

对 $i=1, 2, \dots$, 完成下列步骤:

(1) 移位 LFSR (记状态变换为 f_i): $m_i = f_i(m_{i-1})$;

(2) 计算 $k_i = m_i \oplus a_i$ 。

输出: 序列 $\{k_i, i \geq 1\}$ 。

该密钥流生成器的特点是实现简单; 由于实现精度不要求很高, 所以成本较低; 序列周期可以通过 LFSR 级数的选取得到很好的控制, 从而可根据信息的长度来产生需要周期长度的密钥流序列; 混沌系统的内在随机性使得密钥流序列具有很强的安全性; 由于密钥流序列是由混沌序列和 LFSR 码序列在 $GF(2)$ 域上作加法得到的, 因此均匀性好。图8是在16位精度, LF-

SR 的级数为11时所生成的混沌密钥流序列的 χ^2 检验结果,从图中可看出,随着序列长度 N 的增加, χ^2 值减小,且对于任意长度的序列,均有 $\chi^2 \leq \chi_{0.05}^2(1)$ (查表可得显著水平5%,自由度为1时 χ^2 的临界值为3.841),因此该密钥流序列通过 χ^2 检验,这说明序列的均匀性很好。总之,该混沌密钥流序列满足安全性方面的要求,可作为流密码序列来使用。

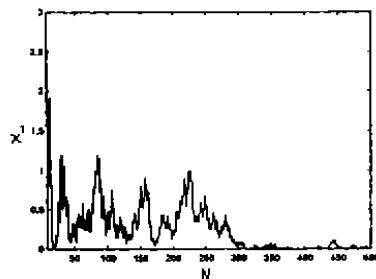


图8 密钥流序列的 χ^2 检验 ($L=16, n=11$)

结束语 本文通过 LFSR 的合成处理来实现有限精度的混沌系统,克服了数字混沌序列的短周期行为,使其相关性能接近于理论比例。我们的结论是经 LFSR 合成处理的混沌序列的周期为混沌序列和 LFSR 码序列周期的最小公倍数,虽然有限精度数字混沌序

列的周期不好确定,但可以选择 nT_m 为素数的 LFSR 的级数 n 来尽可能增大输出序列的周期,或较大级数的 LFSR 来达到同样的效果,经过以上计算机仿真说明了本文所提出方法的有效性,从而为混沌动力学的实际应用提供了一种可行的途径。

参考文献

- 1 Lorenz E N. Deterministic non-periodic flow. J. Atmospheric Sci., 1964, 20(3): 130~141
- 2 Borchers P H, Mccauley G P. The digital tent map and the trapezoidal map. Chaos, Solitons & Fractal, 1993, 3(4): 451~466
- 3 Palmore J, et al. Computer arithmetic, chaos and fractal. Physica, 1990, D42: 99~110
- 4 Gernak J. Digital generators of chaos. Phys. Lett. A, 1996, 214: 151~160
- 5 周红,等.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
- 6 凌聪,孙松庚.一种混沌扩频码序列设计的准则.电子科学学刊, 1998, 20(4): 558~561
- 7 李克,杨绿溪,何振亚.一类混沌映射扩频序列的有限精度实现及其相关性能分析.电路与系统学报, 1998, 3(4): 98~103

(上接第62页)

$$S_1(E(A_5))=0.2, S_2(E(A_1))=0.2,$$

$$S_2(E(A_3))=0.3, S_2(E(A_3))=0.4,$$

$$S_2(E(A_4))=0.5, S_2(E(A_5))=0.6.$$

由上述结果可得:

$$S_1(E(A_1))=S_1(E(A_2))=S_1(E(A_3))=S_1(E(A_4))=S_1(E(A_5))$$

$$S_2(E(A_1))<S_2(E(A_2))<S_2(E(A_3))<S_2(E(A_4))<S_2(E(A_5))$$

显然此时应选择目标 A_5 , 这种情况对应于实际决策中的同时考虑“赞成票”和“反对票”且倾向于“乐观”选择的情况。

c) 当 S_1, S_2 取如下值时: $S_1(E(A_i))=f_{A_i}, S_2(E(A_i))=1-f_{A_i}$, 则有:

$$S_1(E(A_1))=0.2, S_1(E(A_2))=0.3, S_1(E(A_3))=0.4, S_1(E(A_4))=0.5, S_1(E(A_5))=0.6. 由上述结果可得:$$

$$S_1(E(A_1))<S_1(E(A_2))<S_1(E(A_3))<S_1(E(A_4))<S_1(E(A_5))$$

显然此时应选择目标 A_5 , 这种情况对应于实际决

策中的仅考虑“赞成票”的情况。

由以上讨论可见, 由于决策时考虑的重点不同, 以及选择目标的策略不同, 则对于同一个目标集, 可能有多个不同的决策结果, 采用我们提出的计分函数和加权计分函数, 可以得到符合实际情况的决策结果。这为多目标模糊决策提供了一个十分有用的方法。

参考文献

- 1 Yager R R. Fuzzy decision making including unequal objectives. Fuzzy sets and systems, 1978, 1: 87~95
- 2 Ibrahim A, Ayyub B M. Multi-criteria ranking of components according to their priority for inspection. Fuzzy sets and systems, 1992, 48(1): 1~14
- 3 Chen S M, Tan J M. Handling multi-criteria fuzzy decision making problems based on vague sets theory. Fuzzy sets and systems, 1994, 67(2): 163~172
- 4 李凡. 模糊信息处理系统. 北京大学出版社, 1998
- 5 李凡, 徐章艳, 饶勇. Vague 集. 计算机科学, 2000, 27(9): 12~14
- 6 李凡, 饶勇. 基于 Vague 集的加权模糊运算. 华中理工大学学报(待发)