

有限精度条件下时空混沌伪随机序列实现方法研究

郝剑, 柯熙政, 李建勋

(西安理工大学 自动化学院, 陕西 西安 710048)

摘要: 在时域、频域以及相空间对时空混沌系统有限字长效应进行了深入分析。定义了格点间“周期耦合传递”现象, 并设计出两种有限字长效应的改善方案, 即非反馈式扰动方案和反馈式扰动方案。仿真结果显示: 两种方案对有限字长效应都起到了一定的改善作用。

关键词: 时空混沌 有限字长效应 扰动

1990年, 美国海军专家 Pecora 和 Carrol 通过驱动响应法首次成功地实现了混沌系统同步。从此, 全世界范围内掀起了利用混沌序列进行保密通信研究的热潮。经过十几年的发展, 一维混沌通信技术已趋于成熟。现在, 人们把研究的焦点开始转向具有更高复杂度, 更大容量的时空混沌系统。

目前, 一些基于时空混沌序列的通信系统模型已被提出。但在实现工程中, 由于混沌运动是无限精细的, 而硬件系统精度又是有限的, 所以混沌系统有限字长效应使混沌映射经过长期迭代后, 所产生的序列的性质与理论值出现了巨大差异。参考文献[1]指出, 精度有限导致的混沌系统短周期现象难以精确分析; 参考文献[2]认为, 计算精度、硬件类型甚至编程语言都有可能影响有限精度混沌系统的最终结果; 参考文献[3]虽然提出了一定的改进方案, 但仅仅是针对一维混沌系统进行的分析。因此, 时空混沌系统要从理论走向实践, 有限字长效应是它必须克服的一道难关。

本文针对时空混沌系统的有限字长效应做了深入的分析。根据格点间的“周期耦合传递”现象, 设计了两种有限字长效应的改善方案: 非反馈式扰动方案和反馈式扰动方案, 并对各自的处理效果进行了仿真。

1 有限字长效应对时空混沌序列的影响

这里利用金子邦彦提出的单向耦合映象格子模型(OCML)^[4]生成时空混沌序列。单向耦合映象格子模型是一种时间离散、空间离散、状态连续的无穷维动力学系统。其系统表达式为:

$$\begin{cases} X_{n+1}(1) = S(n) \\ X_{n+1}(i) = (1-\alpha)f[X_n(i)] + \alpha f[X_n(i-1)] \\ (i=2,3,4,\dots,L; n=1,2,3,\dots,\infty) \end{cases} \quad (1)$$

式中, L 为系统空间长度; n 是离散化时间坐标; i 是空间坐标; α 为格点间耦合系数; $f(x)$ 是一维 logistic 映射, $x_{n+1} = \lambda x_n(1-x_n)$; $S(n)$ 是驱动信号, 选改进型 logistic 映射即 $s(n+1) = 1 - \mu s(n)^2$ 。当参数 $\lambda = 4, \mu = 1.401156$

时, 系统处于完全发展湍流状态。

在理想条件下, 在完全发展湍流状态的时空混沌系统中, 任意格点时间序列都包含有大量不稳定的周期。在相空间里, 混沌轨道不停地延伸、折叠, 使这些非稳定的周期轨道间出现随机的跳动, 整体呈现出噪声般的非周期特性。在现实工程中, 微处理器字长是有限的。有限字长效应可能使混沌序列性能与理论值出现明显差别。

图 1 给出了 OCML 第 6 格点时间序列在实现精度等于 64 位和 8 位时的功率谱密度和相空间轨道。可以看出: 在 64 位精度条件下, 序列具有噪声般的均匀的宽频谱特性, 相空间中的轨道出现随机延伸、折叠, 表现出复杂的运动形式。在精度降到 8 位后, 功率谱密度出现明显峰值, 相空间里轨道变成在有限点上呈简单、重复

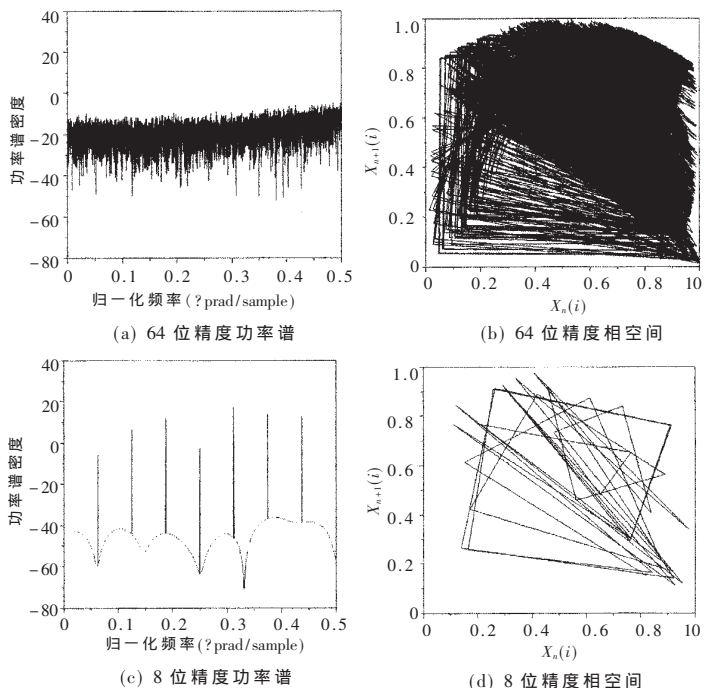


图 1 功率谱密度和相空间轨道

的抖动。由此可见,有限字长效应严重影响着时空混沌系统的演化,低精度条件下生成的时空混沌序列根本无法满足保密通信对伪随机序列性能的要求。

研究中还发现:只要 OCML 任一格点时间序列出现稳定周期,其后所有格点将依次出现同长度的稳定周期;如果驱动序列呈现周期特性,系统将整体呈现出同样的周期特性,这种现象笔者定义为“周期耦合传递”。图 2 给出了 16 位精度时 50 个格点时间序列的“周期耦合传递”现象。受有限字长效应影响,驱动序列在 $n=165$ 时首先出现稳定的 103 点周期。利用它进行驱动,后续格点将迅速按空间顺序进入稳定的 103 点周期状态,即 $X_n(i)-X_{n+103}(i)$ 保持为 0。由此可见,驱动序列在系统迭代过程中起重要的作用,其性能的优劣可以直接影响整个时空混沌系统的演化。

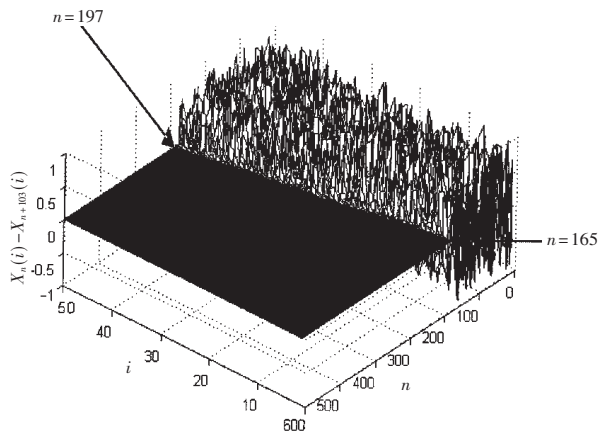


图 2 16 位精度时 50 个格点时间序列的“周期耦合传递”

2 有限字长效应的克服方案

有限字长效应制约着时空混沌系统从理论到实践的转化,如何在较低精度条件下保持混沌系统原有特性成为一道难题。参考文献[3]指出:对混沌系统进行适当地扰动,可以降低有限字长效应对其的影响。结合上面描述的“周期耦合传递”现象,本文设计两种有限字长效应改善方案:非反馈式扰动方案和反馈式扰动方案。通过改善驱动序列的混沌特性,将改善效果自动耦合到整个时空混沌系统中。

2.1 非反馈式扰动方案

非反馈式扰动方案是一种驱动系统的外部扰动方案。其实现方法为:沿时间顺序将混沌驱动序列分组,设码组长度为 N ,则:

$$s_l = [s((l-1) \times N + 1), s((l-1) \times N + 2), \dots, s(l \times N)] \quad (2)$$

$$S(n) = [s_1, s_2, \dots, s_l, \dots] \quad (3)$$

用扰码产生系统循环输出的长度为 d 的二进制平衡伪随机序列 $D(n)$ (如 m 序列)作为干扰源。当 $D(n)=1$ 时混沌码组取反,当 $D(n)=0$ 时保持不变。处理后序列

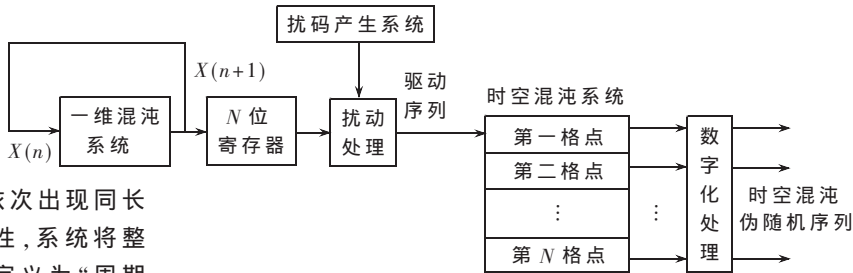


图 3 非反馈式扰动系统框图

作为 OCML 模型第一格点,驱动整个系统的演化。非反馈式扰动系统框图如图 3 所示,处理后序列周期与扰码长度和原始序列周期有关。

2.2 反馈式扰动方案

反馈式扰动方案与 OGY 控制法^[5]类似。当混沌序列靠近或进入某一轨道时,在外力作用下对系统状态进行扰动,迫使其沿着希望的方向演化。区别在于 OGY 法将混沌轨道限制在稳定的周期上,而反馈式扰动方案则致力于使混沌序列从稳定的周期轨道中脱离。图 4 为反馈式扰动方案系统框图,驱动函数如式(4)所示。

$$S(n) = F[S(n-1) \times D(n-1)] \quad (4)$$

反馈式扰动方案可以分为周期性扰动反馈和非周期性扰动反馈。周期性扰动指驱动系统进入稳定周期轨道之前,每隔 N 点提取一个信号,将其幅度改变后反馈回系统输入端。扰动序列 $D(n)$ 如式(5)所示,扰动周期为 $N+1$ 。

$$D(n) = [1, 1, \dots, 1, \varepsilon, 1, 1, \dots, 1, \varepsilon, \dots] \quad (5)$$

非周期性扰动指扰动间隔不具有周期性,例如第一次隔 N 点,第二次隔 $N+1$ 点,第三次隔 $N+2$ 点,依此类推,即 $D(n)$ 满足公式(6)。

$$D(n) = [1, 1, \dots, 1, \varepsilon, 1, 1, \dots, 1, \varepsilon, 1, 1, \dots, 1, \dots] \quad (6)$$

2.3 实验结果分析

在 16 位精度条件下,抽取单向耦合映射格子模型第 20 格点长 10 000 点时间序列,对上述两种方案的处理效果进行仿真。两种扰动方案分别服从以下参数配置。

(1)非反馈式扰动方案: $\lambda=4, \mu=1.43, S(0)=0.776$, 码组长度取 $N=10$, 干扰序列 $D(n)$ 选择 103 点截短 m 序列, 本原多项式为: $x^7+x^4+x^3+x^2+1$ 。

(2)反馈式扰动方案: $\lambda=4, \mu=1.43, S(0)=0.76, N=99$,

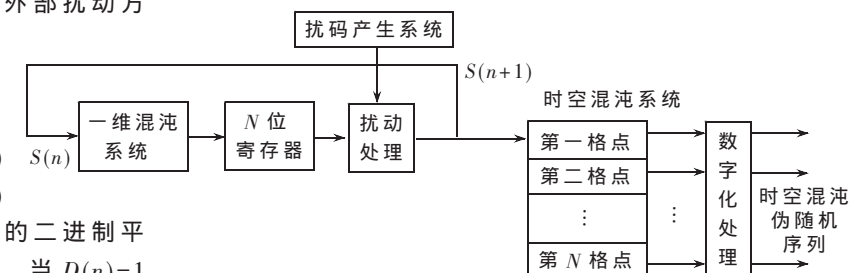


图 4 反馈式扰动系统框图

$\varepsilon=0.5$ 。

通过两种方案处理后,对序列进行了功率谱密度估计,结果如图5所示。其中,图5(a)为扰动前序列的功率谱密度,整体分布很不均匀,在一个均匀宽带噪声谱中叠加了大量较强的频谱峰值;图5(b)为非反馈式扰动后的序列功率谱密度,频谱峰值明显被削弱,但幅度抖动依然比较大;图5(c)和图5(d)为周期性和非周期性反馈扰动后序列的功率谱密度,该方案基本消除了频谱峰值。特别是非周期反馈扰动方案,处理后序列具备了噪声般的均匀的宽频谱特性,有限字长效应得到良好的抑制。

与图5相对应,在图6中重构了处理前后序列的相空间轨道。可以看出,两种扰动方案在未改变原有序列的动力系统形式的基础上,不同程度地提高了轨道复杂度。其中,非周期反馈扰动方案效果尤为明显,处理后轨道复杂度几乎达到图1(b)所示的64位精度水平。

在有限字长效应影响下,OCML格点时间序列呈现出某种稳定的短周期特性,相空间中混沌轨道在有限点上呈现了简单、重复的抖动。本文中设计了两种驱动系统扰动方案来抑制有限字长效应影响,并对处理效果进行了仿真。结果表明:驱动系统扰动方案对整个时空混沌系统的有限字长效应可以起到较好的改善作用。特别是非周期反馈扰动方案,处理后的所有格点时间序列都具有了噪声般的均匀的宽频谱特性和复杂的相空间轨道,效果比较理想,可以成为保密通信系统中有价值的伪随机序列生成候选方案。

参考文献

[1] BORCHERS P H, MCCAULEY G P. The digital tent map

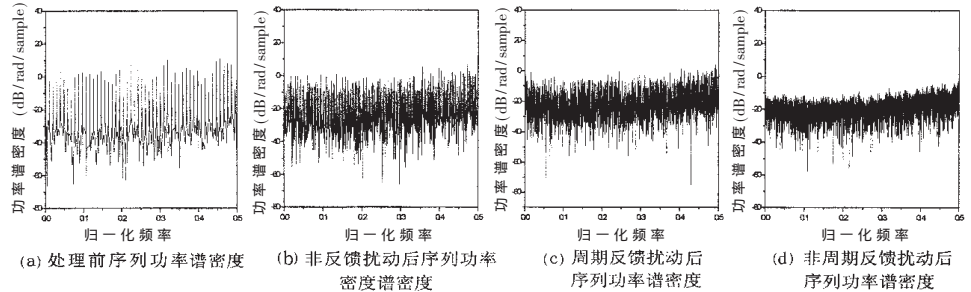


图5 序列功率谱密度

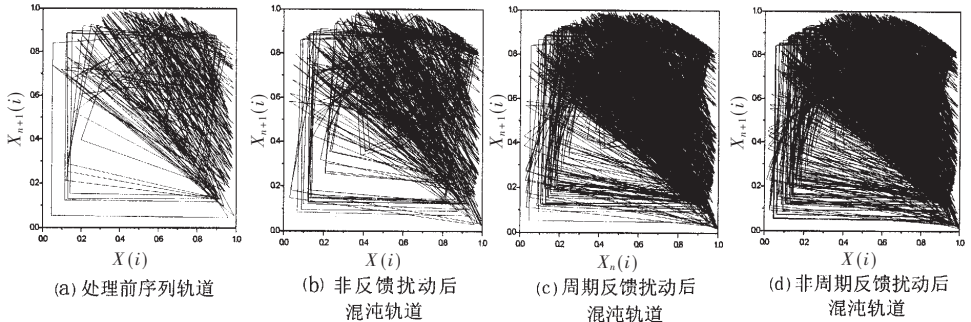


图6 序列的相空间轨道

and the trapezoidal map[J]. Chaos, Solitons & Fractal, 1993,3(4):451-466.

[2] PALMORE L. Computer arithmetic, chaos and fractals[J]. Physica, 1990, D42:99-110.

[3] 周红, 凌雯亭. 有限精度混沌系统的m序列扰动实现[J]. 电子学报, 1997, 25(7):95-97.

[4] KANEKO K. Period-doubling of kink-anticle patterns [J]. Progress of Theoretical Physics, 1984, 72(3):480-486.

[5] OTT E, GREBOGI C, YORKE J A. Controlling chaos [J]. Phys Rev Lett, 1990, 64(11):1196-1199.

[6] 张翌维, 柯熙政, 席晓莉. 一种多级数字混沌编码方案及其硬件实现[J]. 电子技术应用, 2005, 31(2):58-61.

[7] FELDMANN U, HASLER M, SCHWARZ W. Communication by chaotic signals: the inverse system approach[J], Int. J. Circ. Theor. Appl., 1996, 24:551-579.

(收稿日期:2006-07-17)