物理学报 Acta Physica Sinica
Chinese Physical Society
Institute of Physics, CAS

基于忆阻器的数模混合随机数发生器

袁泽世　李洪涛　朱晓华

A digital-analog hybrid random number generator based on memristor

Yuan Ze-Shi　Li Hong-Tao　Zhu Xiao-Hua

引用信息 Citation: Acta Physica Sinica, 64, 240503 (2015)　DOI: 10.7498/aps.64.240503
在线阅读 View online: http://dx.doi.org/10.7498/aps.64.240503
当期内容 View table of contents: http://wulixb.iphy.ac.cn/CN/Y2015/V64/I24

您可能感兴趣的其他文章
Articles you may be interested in

空间关联白噪声影响下小世界神经元网络系统的同步动力学
Synchronous dynamics of small-world neuronal network system with spatially correlated white noise
物理学报.2015, 64(22): 220503　http://dx.doi.org/10.7498/aps.64.220503

六边形格子态斑图的数值模拟
Numerical simulations of hexagonal grid state patterns
物理学报.2015, 64(21): 210505　http://dx.doi.org/10.7498/aps.64.210505

电压控制正极性输出罗变换器的改进平均模型建模及稳定性分析
Improved averaged model and stability analysis of voltage-mode controlled positive output super-lift Luo converter
物理学报.2015, 64(21): 210506　http://dx.doi.org/10.7498/aps.64.210506

一种忆感器模型及其振荡器的动力学特性研究
Study on dynamical characteristics of a meminductor model and its meminductor-based oscillator
物理学报.2015, 64(21): 210504　http://dx.doi.org/10.7498/aps.64.210504

单稳系统的脉冲响应研究
Pulse response of a monostable system
物理学报.2015, 64(21): 210503　http://dx.doi.org/10.7498/aps.64.210503

基于忆阻器的数模混合随机数发生器*

袁泽世 李洪涛† 朱晓华

(南京理工大学电子工程与光电技术学院, 南京 210094)

(2015 年 8 月 12 日收到; 2015 年 9 月 22 日收到修改稿)

数字方法实现的混沌随机数发生器存在有限字长效应, 无法保证随机数良好的统计特性. 本文构建了一类包含最少模拟器件的新数模混合系统, 分析了混合系统的非线性动力学行为. 利用现场可编程逻辑门阵列和一阶广义忆阻器实现了复杂混沌映射, 克服了有限字长效应, 构造了稳定的高速混沌随机数发生器, 可以产生 100 Gbit/s 以上速率的随机数. 研究表明, 数模混合系统的混沌性对元件参数变化不敏感. 混合系统易于集成在图像加密、保密通信和雷达波形设计等应用系统中.

关键词: 随机数发生器, 有限字长效应, 数模混合系统, 忆阻器

PACS: 05.45.–a, 05.45.Gg, 05.45.Pq, 05.45.Ra **DOI:** 10.7498/aps.64.240503

1 引 言

随机数在图像加密 [1]、保密通信 [2,3] 以及雷达波形设计 [4] 等领域均有着广泛的应用. 随机数可以由模拟或数字等方法产生, 模拟实现方法包括利用基于混沌的确定性算法或物理熵源等 [5,6]. 然而, 所有的模拟实现方案 [7] 都存在系统对参数和初始值误差敏感的问题 [8], 容易导致系统状态 [9−11] 发生显著改变. 以典型的蔡氏 (Chua) 混沌电路实现为例, 当电阻 R 由于环境或器件参数误差等因素而发生微小的改变时, 都可能会导致电路状态发生改变, 严重影响所产生随机数的统计特性 [12].

基于数字方法实现的混沌随机数发生器能降低模拟方法实现时系统对参数和初始值误差敏感的影响, 但是数字系统的有限字长效应必然会引起动力特性退化 [13,14], 难以保证序列的随机性. 一些基于数模混合方法的实现 [15−20] 由于需要引入模拟混沌系统的扰动, 因此系统的模拟部分仍存在对参数与初始值误差敏感的问题.

Deng 等 [15] 设计了一个脉冲式的控制器, 与状态反馈控制器一起保证了不确定连续混沌系统同步的鲁棒性, 缓解了数字系统动力特性退化的问题. Ergun 和 Güler [16−18] 采用了以连续时间混沌振荡器为核心的思路, 借助部分数字器件, 实现了高速随机数发生器. 然而由于在电路的整体设计中采用了运算放大器等模拟器件, 限制了随机数产生的速率和系统的鲁棒性. Hu 等 [19] 归纳了解决数字系统动力特性退化常用的方法, 包括增加计算精度、级联多个混沌系统、利用随机数对系统进行扰动、切换多个混沌系统以及误差补偿方法等. 同时 Hu 提出了新的方法, 即将给定的数字混沌映射与模拟混沌系统进行耦合, 利用模拟系统反控制数字映射. 虽然这一方法能有效解决数字系统动力特性退化问题, 但是由于其引入了一个完整的模拟混沌系统, 使得混合系统的鲁棒性也受到了限制. Yeniçeri 和 Yalçın [20] 提出了一种时延采样数据反馈系统, 利用模拟器件产生动力学行为的同时, 利用数字器件组成采样和时延线作为系统反馈. 该设计同样采用了以模拟系统为主的思路, 因此也存在着序列产生速率和系统鲁棒性受限的问题.

为了减小模拟部分对整个数模混合系统的影

* 国家自然科学基金 (批准号: 61401204)、江苏省科技计划支撑类项目 (前瞻性联合研究项目)(批准号: BY2015004-03) 和江苏省博士后基金 (批准号: 1501104C) 资助的课题.

† 通信作者. E-mail: liht@njust.edu.cn

© 2015 中国物理学会 Chinese Physical Society

响, 本文尝试用尽可能少的模拟器件构造数模混合系统, 探讨仅用一个模拟器件的数模混合系统产生混沌随机数的可能. 本文采用忆阻器和数字器件组成反馈结构, 构造混沌系统.

1971年, 华裔科学家蔡少棠[21]根据变量组合完备性原理, 从理论上预测了描述电荷和磁通关系的元件, 即忆阻器的存在性, 并阐述了其特性、合成原理及应用[22]. 但是直到2008年惠普实验室的Strukov等[23]报道了忆阻器的可实现性后, 关于忆阻器应用的研究才逐渐引起研究者们的兴趣. 忆阻元件的发现具有重大意义, 它将电路设计中的基础元件由传统的电阻、电容、电感三个元件扩展到四个, 为忆阻电路的设计和应用开辟了新的发展空间.

由于成本限制以及纳米尺度器件研发技术上的难题, Strukov等[23]提出, 商用的忆阻器在未来一段时间内是难以出现的. 因此, 一些与忆阻器有着相同特性的等效电路陆续被开发出来, 用于研究忆阻器的潜在应用[24,25]. 此外, 一些忆阻模拟器也相继被提出[26−29], 并用于基于忆阻器的实时面包板电路实验. Corinto和Ascoli[30]提出了一种广义忆阻器, 由一个完整的波形整流器和一个二阶RLC滤波器组成, 其优势在于只采用了二极管、电感、电容和电阻等基础电路元件. Bao等[31]在这种广义忆阻器的基础上, 将二阶RLC滤波器替换为一并联的RC滤波器, 由此提出了一个新的一阶广义忆阻器.

本文采用Bao等[31]提出的一阶广义忆阻器, 结合数字器件组成反馈结构, 构造数模混合混沌随机数发生器. 混合系统本质上解决了数字系统的动力特性退化问题, 同时最大程度地减小了模拟部分参数对系统混沌性的影响, 降低了模拟器件对随机数产生速率和系统鲁棒性的限制, 仅采用单个模拟器件也可使得混合系统更加易于集成. 实验证明, 本文提出的数模混合随机数发生器以现场可编程逻辑门阵列(FPGA)实现时, 可产生100 Gbit/s以上速率的随机数, 性能优于已有的系统.

2 基于忆阻器的数模混合混沌系统

2.1 一阶广义忆阻器模型

本文所采用的一阶广义忆阻器模型如图1(a)所示, 为一个包含二极管桥和并联RC滤波器的一阶忆阻电路[31].

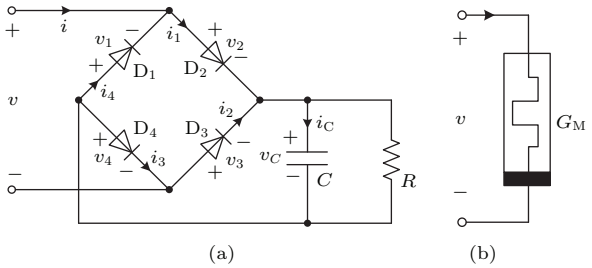

图1 基于忆阻电路的广义忆阻器 (a) 忆阻二极管桥和并联RC滤波器; (b) 广义忆阻器

Fig. 1. Generalized memristor realized by a memristive circuit: (a) Memristive diode bridge with parallel RC filter; (b) generalized memristor.

二极管D_1—D_4的基本关系可表示为:

$$i_k = I_\mathrm{s}\left(\mathrm{e}^{2\rho v_k} - 1\right), \tag{1}$$

其中$k = 1,2,3,4$, $\rho = 1/(2nV_\mathrm{T})$; v_k, i_k分别为二极管D_k两端的电压和流过二极管的电流; I_s, n和V_T分别为二极管反向饱和电流、发射系数和热电压.

利用基尔霍夫电压定律并进行推导化简, 可得图1(a)所示一阶忆阻电路的数学模型为[31]

$$i = g(v_\mathrm{c}, v)\, v = 2I_\mathrm{s}\,\mathrm{e}^{-\rho v_C}\sinh(\rho v), \tag{2}$$

$$\frac{\mathrm{d}v_C}{\mathrm{d}t} = f(v_C, v) = \frac{2I_\mathrm{s}\left(\mathrm{e}^{-\rho v_C}\cosh(\rho v) - 1\right)}{C} - \frac{v_C}{RC}, \tag{3}$$

其中i为输入电流, v为输入电压, v_C为电容器两端电压. (2)和(3)式所示的数学模型与广义忆阻器的定义式是相符的[32], 如图1(b)所示, 证明图1(a)的基本电路为一阶广义忆阻器. 文献[31]所提的一阶忆阻电路本质上为一压控忆阻器, 其忆阻大小可表示为$G_\mathrm{M} = i/v = g(v_C, v)$, 与输入电压和电容电压均有关.

图2给出了输入电压幅度不变、频率变化时广义忆阻器的磁滞回线图, 其中电容$C = 1$ μF, 电阻$R = 1$ kΩ, 输入电压$v = 5\sin(2\pi ft)$ V, $I_\mathrm{s} = 2.682$ nA, $n = 1.836$, $V_\mathrm{T} = 25$ mV, 频率f分别为0.2, 2和10 kHz. 由图2可知, 广义忆阻器的v-i曲线为一在原点处紧缩的磁滞回线, 并且随着输入电压频率的增加, 紧磁滞回线瓣单调递减. 当频率趋于无穷大时, 紧磁滞回线收缩成一个非线性单值函数.

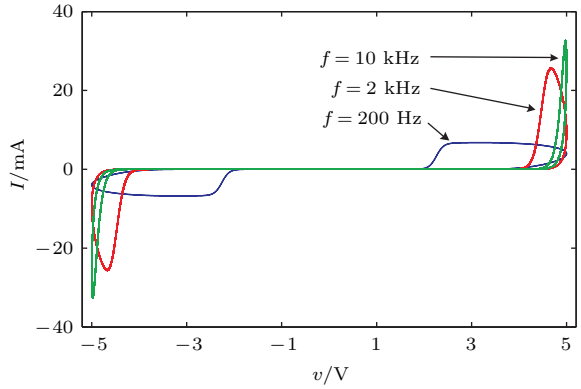

图 2 (网刊彩色) 不同频率输入电压下广义忆阻器的磁滞回线

Fig. 2. (color online) Pinched hysteresis loop of the generalized memristor driven by periodic input voltages with different frequencies.

2.2 数模混合系统动力学模型的构建

基于一阶广义忆阻器反馈的数模混合系统框图如图 3 所示, 其中忆阻器输入负极接地, 正极接 D/A 输出, 并从正极引出一条反馈线路至 A/D 输入. 整个系统的工作过程如下: 1) 数字部分 (即 FPGA) 中混沌映射输出的信号每隔 M, $M = 1, 2, 3, \cdots$ 个时钟周期即经过数模转换器 D/A 转换为模拟信号, 以激励忆阻器; 2) 在下一个采样时钟到来时, 将忆阻器产生的电压响应经过模数转换器 A/D 的采集反馈回数字部分, 对数字系统中的混沌映射进行扰动. 如此循环. 忆阻器的引入将在本质上避免数字系统的有限状态相空间问题.

图 3 所示的电阻 R_1 处有如下关系:

$$i = \frac{g(t) - v}{R_1} = \frac{v_x - v}{R_1}, \tag{4}$$

其中 $v_x = g(t)$ 为 D/A 输出电压, v 为忆阻器输入电压, i 为忆阻器输入电流, R_1 为电阻的阻值. (4) 式联立 (2) 和 (3) 式, 即得到整个数模混合系统的数学模型如下:

$$\begin{cases} i = \dfrac{v_x - v}{R_1}, \\ i = 2I_{\rm s}\,{\rm e}^{-\rho v_C}\sinh(\rho v), \\ \dfrac{{\rm d}v_C}{{\rm d}t} = \dfrac{2I_{\rm s}\left({\rm e}^{-\rho v_C}\cosh(\rho v) - 1\right)}{C} - \dfrac{v_C}{RC}, \end{cases} \tag{5}$$

其中 $v_x = g(t)$ 为数字器件通过 D/A 输出的有限状态变量, v 是由忆阻器引入的模拟量, 因此 (5) 式所示模型本质上是属于实数空间, 从而避免了有限字长效应; 同时作为模拟量的 v 为一单一线性项, 对整个系统动力学行为的影响易于分析和控制.

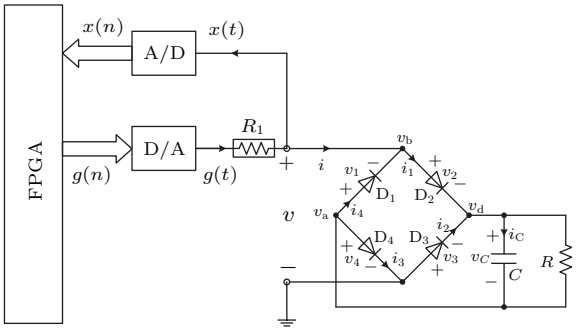

图 3 基于一阶广义忆阻器反馈的数模混合系统框图

Fig. 3. Block diagram of digital-analog hybrid system based on a generalized memristor.

接下来我们对忆阻器模型中 4 个二极管的通断状态做具体分析以简化电路, 共有如表 1 所列的 16 种情况, 其中 $v_{\rm a}$, $v_{\rm b}$, $v_{\rm d}$ 分别为端点处的电势, 如图 3 所示. 由表 1 可知, 16 种情况中有 2 种情况由于电势关系存在矛盾, 实际电路中是不存在的. 因此, 忆阻器的简化电路共可以分为 4 种情况, 即忆阻器被短路, 被断路以及 case A 和 case B, 其中 case A, case B 相应的简化电路图如图 4 所示.

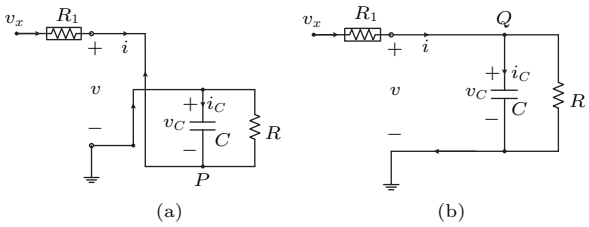

图 4 广义忆阻器的简化电路 (a) case A; (b) case B

Fig. 4. Simplified circuit of the generalized memristor: (a) Case A; (b) case B.

分别利用图 4 中所示节点 P, Q 处的电流关系

$$\frac{v_x - (\mp v_{\rm c})}{R_1} = C\frac{{\rm d}(\mp v_{\rm c})}{{\rm d}t} + \frac{(\mp v_{\rm c})}{R},$$

可以推导出 case A 和 case B 分别满足以下关系:

$$v_{\rm c} = \frac{a}{b}v_x\left({\rm e}^{-bt} - 1\right) + v_{\rm c}(0)\,{\rm e}^{-bt}, \tag{6}$$

$$v_{\rm c} = \frac{a}{b}v_x\left(1 - {\rm e}^{-bt}\right) + v_{\rm c}(0)\,{\rm e}^{-bt}, \tag{7}$$

其中 $a = 1/(R_1C)$, $b = R_3/C$, $R_3 = (1/R_1) + (1/R)$, $v_{\rm c}(0)$ 为电容 C 上的初始电压值.

由以上分析可知, 该一阶广义忆阻器可以近似等效为短路, 断路, case A 和 case B 四种状态交替工作.

表 1 忆阻器模型的具体分析

Table 1. Specific analysis of the generalized memristor.

情况	二极管通断情况				二极管两端电势关系	是否形成有效通路	忆阻器状态
	D_1	D_2	D_3	D_4			
1	通	通	通	通	$v_a > v_b, v_b > v_d, v_d < 0, v_a > 0$	否	忆阻器被短路
2	通	通	通	断	$v_a > v_b, v_b > v_d, v_d <, v_a < 0$	否	忆阻器被短路
3	通	通	断	通	$v_a > v_b, v_b > v_d, v_d > 0, v_a > 0$	否	忆阻器被短路
4	通	通	断	断	$v_a > v_b, v_b > v_d, v_d > 0, v_a < 0$	否	电势关系矛盾
5	通	断	通	通	$v_a > v_b, v_b < v_d, v_d < 0, v_a > 0$	否	忆阻器被短路
6	通	断	通	断	$v_a > v_b, v_b < v_d, v_d < 0, v_a < 0$	是	Case A
7	通	断	断	通	$v_a > v_b, v_b < v_d, v_d > 0, v_a > 0$	否	忆阻器被断路
8	通	断	断	断	$v_a > v_b, v_b < v_d, v_d > 0, v_a < 0$	否	忆阻器被断路
9	断	通	通	通	$v_a < v_b, v_b > v_d, v_d < 0, v_a > 0$	否	忆阻器被短路
10	断	通	通	断	$v_a < v_b, v_b > v_d, v_d < 0, v_a < 0$	否	忆阻器被断路
11	断	通	断	通	$v_a < v_b, v_b > v_d, v_d > 0, v_a > 0$	是	Case B
12	断	通	断	断	$v_a < v_b, v_b > v_d, v_d > 0, v_a < 0$	否	忆阻器被断路
13	断	断	通	通	$v_a < v_b, v_b < v_d, v_d < 0, v_a > 0$	否	电势关系矛盾
14	断	断	通	断	$v_a < v_b, v_b < v_d, v_d < 0, v_a < 0$	否	忆阻器被断路
15	断	断	断	通	$v_a < v_b, v_b < v_d, v_d > 0, v_a > 0$	否	忆阻器被断路
16	断	断	断	断	$v_a < v_b, v_b < v_d, v_d > 0, v_a < 0$	否	忆阻器被断路

2.3 基于 Logistic 映射的混合系统分析

将 Logistic 映射分别引入数字系统以及本文的数模混合系统, 并对比分析两者的仿真结果, 可初步验证本文方法的有效性.

已知 Logistic 映射可以表示为

$$x(t) = ax(t-\tau)(1-x(t-\tau)),$$
$$a \in [0,4], x \in (0,1). \tag{8}$$

图 5 分别给出了采用数字系统时所得到的 Logistic 映射分岔图及其时序图, 其中参数 $a = 3.9$, 量化位数为 $N = 10$. 图 5 (a) 所示分岔图与原 Logistic 映射分叉图在结构上基本保持一致, 但图 5 (b) 所示时间序列在约 $t = 32$ 以后退化为周期序列, 说明系统并未进入混沌状态. 这是由于数字系统存在有限字长效应, 且系统映射斜率恒为 0, 导致系统的 Lyapunov 指数为负无穷大, 系统始终不会产生混沌现象, 也就无法保证序列的非周期性.

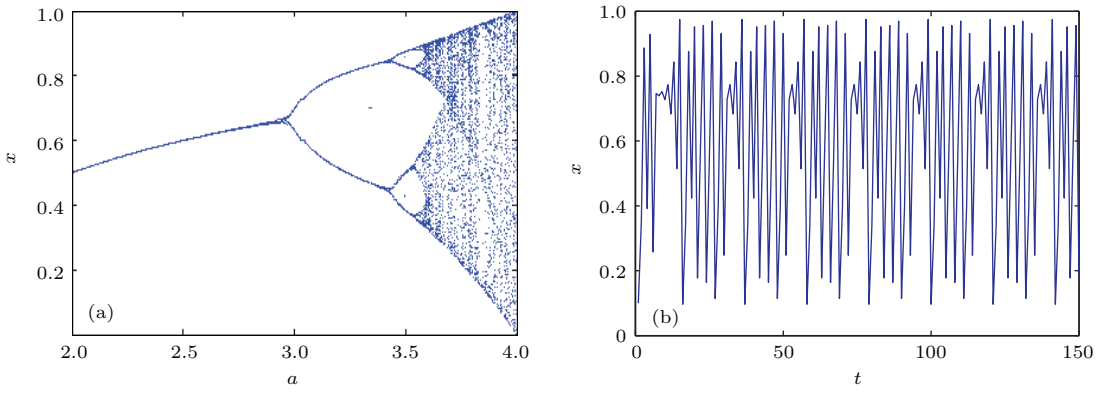

图 5 (网刊彩色) 数字系统 Logistic 映射 (a) 分岔图; (b) 时序图

Fig. 5. (color online) Logistic map realized in digital system: (a) Bifurcation diagram; (b) sequence diagram.

作为对比, 将Logistic映射应用到本文提出的基于忆阻器的数模混合系统中, 系统框图如图3所示. 由2.1节的仿真分析可知, 忆阻器的激励信号应为一正弦信号, 而Logistic映射的输出$v_x \in [0,1]$, 为了使v_x能够激励忆阻器, 令$v_x = 20(v_x - 0.5) \in [-10,10]$. 图6为本文数模混合方法所得到的Logistic映射的相轨图、分岔图及其时序图, 其中映射参数$a = 3.9$, 量化位数$N = 10$, 电容$C = 1$ μF, v_C初值为0.01 V, 电阻$R = 1$ kΩ, $R_1 = -100$ Ω, 二极管反向饱和电流$I_s = 2.682$ nA, 发射系数$n = 1.836$, 热电压$V_T = 25$ mV.

从图6(a)和图6(b)可以看出, 数模混合系统所得到的Logistic映射相轨图、分岔图与理想Logistic映射相比分为了两部分, 每一部分相应的结构与理想Logistic映射保持一致, 即映射的基本性质未发生改变. 由2.1节中对忆阻器电路的详细分析可知, 当忆阻器被短路或断路时, 整个电路退化为数字电路, 结合对数字系统Logistic映射的分析可知, 此时系统是不会进入混沌状态的, 只有当忆阻器处于case A和case B状态时系统才有可能产生混沌, 因此图6(a)和图6(b)中出现的两部分分别对应了忆阻器的两种工作状态case A和case B, 理论分析与数值仿真结果是一致的. 将图6(c)与图5(b)对比可知, 由于在映射迭代中引入了忆阻器的扰动, 在相同参数条件$a = 3.9$, 量化位数为$N = 10$下, 数模混合系统所得到的映射其时间序列不再退化为周期序列, 而是保持了非周期状态, 即混合系统有效解决了数字系统的有限字长问题, 保证了序列的随机性, 证明了本文方法的有效性.

图6(d)给出了电路元器件参数改变10%时混合系统的Logistic映射相轨图, 以模拟环境和参数误差对系统的影响. 对比图6(a)可以发现, 参数微小改变后系统的相轨图几乎未发生变化, 这是因为在上述参数条件下, 系统的映射斜率保持在远大于1的水平, 即使参数发生微小变化, 也不会导致系统混沌状态发生改变. 再加上混合系统仅采用了一个模拟器件, 且数字器件输出十分稳定, 也降低了模拟器件参数改变对整个混合系统的影响, 使系统达到鲁棒混沌. 而对于传统的模拟电路实现, 其模拟器件非常多, 若每个器件的参数均因环境或误差等因素产生10%的改变, 必然会增加整个混沌系统的不确定性, 严重时会导致系统性质和状态发生改变. 以上分析进一步证明了本文方法的有效性.

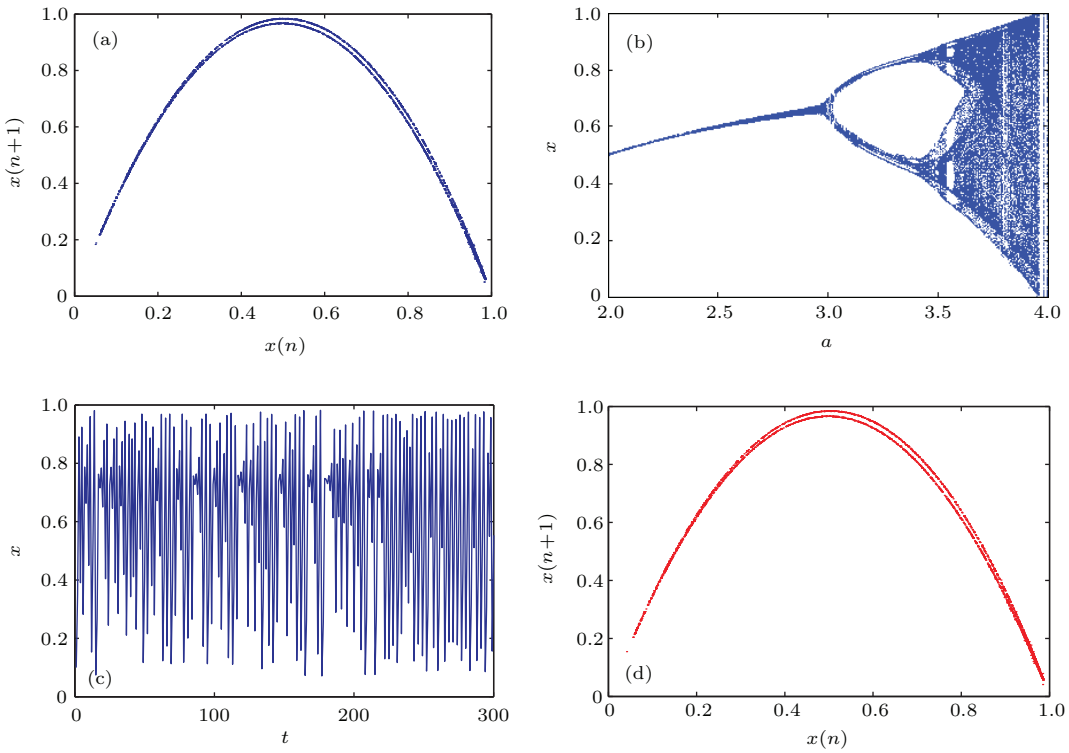

图6 (网刊彩色) 数模混合系统Logistic映射 (a) 相轨图; (b) 分岔图; (c) 时序图; (d) 参数改变后的相轨图

Fig. 6. (color online) Logistic map realized in hybrid system: (a) Phase portrait; (b) bifurcation diagram; (c) sequence diagram; (d) phase portrait after the change of parameters.

3 混沌随机数发生器

本文第2部分给出了采用本文基于一阶广义忆阻器反馈的数模混合系统实现Logistic映射的仿真结果, 并与数字系统相比较验证了本文方法的有效性. 然而在实际应用中, Logistic映射较为简单, 难以产生满足实际应用需求的随机数, 因此本文采用更为复杂的近邻耦合映像格子模型[33]来设计随机数发生器.

近邻耦合映像格子模型可以表示为

$$\begin{aligned} x_n(i) = {} & (1-\eta) f(x_{n-1}(i)) \\ & + \frac{\varepsilon}{2}\left[f(x_{n-1}(i-1)) \right. \\ & \left. + f(x_{n-1}(i+1))\right], \end{aligned} \tag{9}$$

其中, n表示离散时间步数; $i = 1, 2, \cdots, L$为离散格点坐标, L为系统级数; η为耦合系数, 且满足$0 < \eta < 1$. 边界条件服从$x_n(L) = x_n(0)$, 初始条件取$[0, 1]$内的随机数. (9)式中非线性函数$f(x)$为格子的局部状态演化方程, 本文采用锯齿映射, 其迭代方程如下:

$$x_{n+1} = F(x_n) = \beta x_n \pmod 1, \tag{10}$$

其中$F: [0, 1] \to [0, 1]$, 当$1 < \beta \in \mathbb{R}$时, 系统处于混沌状态.

图7分别给出了耦合锯齿映像格子模型原分岔图, 采用数模混合系统后的分岔图、相轨图以及时序图, 其中混合系统的分岔参数$\beta \in (0, 4]$, 耦合系数$\eta = 0.01$, 系统级数$L = 15$, 扰动输入级数$L = 7$, 数字部分输出级数$L = 5$. 数模混合系统中量化位数$N = 10$, 电容$C = 1$ μF, v_C初值为0.01 V, 电阻$R = 1$ kΩ, $R_1 = -100$ Ω, 二极管反向饱和电流$I_s = 2.682$ nA, 发射系数$n = 1.836$, 热电压$V_T = 25$ mV. 从图7(a)和图7(b)中可以看出, 当$\beta > 1$时, 原系统和数模混合系统均处于混沌状态. 图7(c)给出了数模混合系统的相轨图, 输出级数$L = 5$, 图7(d)为混合系统的时序图, 为一非周期序列.

为了得到只包含0和1元素的随机数列, 还需要对混合系统输出进行量化, 才能得到0/1二进制序列$\{s_n(t)\}|_{t=1}^{\infty}$, 其量化函数$T_n(x_i)$定义如下:

$$\begin{aligned} & \{s_n(t)\}|_{t=1}^{\infty} = T_n(x_i) \\ & = \begin{cases} 0, & x \in U_{d=0}^{2^{n-1}-1} I_{2d}^n, \\ 1, & x \in U_{d=0}^{2^{n-1}-1} I_{2d+1}^n, \end{cases} \end{aligned} \tag{11}$$

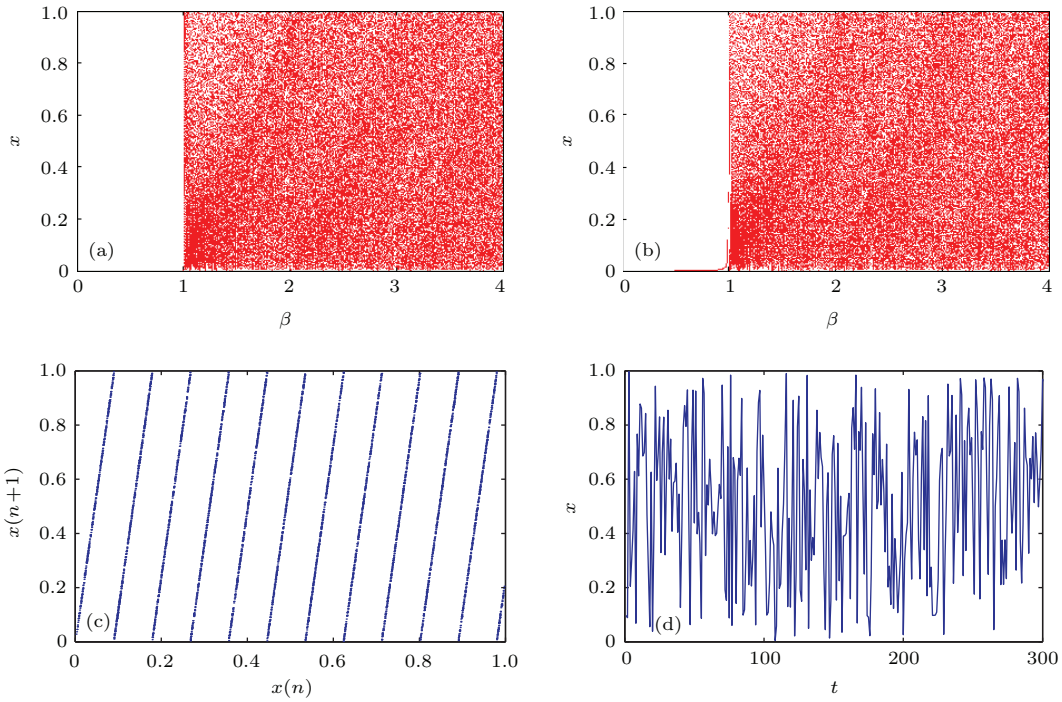

图7 (网刊彩色) 近邻耦合锯齿映像格子模型 (a) 原系统分岔图; (b) 数模混合系统分岔图; (c) 相轨图; (d) 时序图

Fig. 7. (color online) Two-way coupled saw tooth map lattice: (a) Bifurcation diagram of original system; (b) bifurcation diagram of hybrid system; (c) phase portrait; (d) sequence diagram.

其中 n 为正整数, I_0^n, I_1^n, $\cdots$, $I_{2^n-1}^n$ 为 $[0, 1]$ 间的 2^n 个连续等分区间, $U_{d=0}^{2^{n-1}-1} I_{2d}^n$, $U_{d=0}^{2^{n-1}-1} I_{2d+1}^n$ 分别代表偶数区间和奇数区间取并集. 选取适当的 n 值, 量化函数 $T_n(x_i)$ 即可保证序列具有良好的统计特性.

4 电路实现与结果分析

图 8 给出了基于一阶广义忆阻器反馈的数模混合随机数发生器的电路结构图, 分为数字模块、数模转换模块以及模拟模块. 其中数字模块又包括序列输出子模块和映射子模块, 映射子模块由 L 级映射单元组成; 模拟模块中的忆阻器电路采用图 1 (a) 所示的一阶广义忆阻器模型. 图 9 给出了从该随机数发生器中输出的耦合锯齿映像格子模型吸引子示波器图, 与图 7 (c) 的数值仿真结果是一致的.

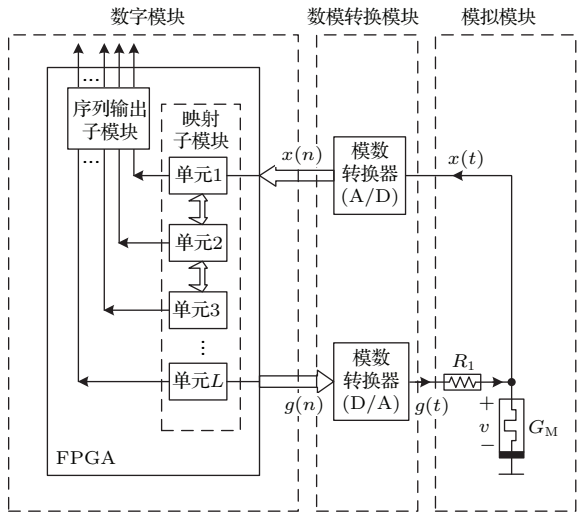

图 8 数模混合随机数发生器电路结构图

Fig. 8. Structure diagram of hybrid system random sequence generator.

随机数发生器的工作流程如下: 1) 数字模块基于 FPGA 产生耦合锯齿映像格子模型的输出 $g(n)$; 2) 每隔 M, $M = 1, 2, 3, \cdots$ 个时钟周期将 $v_x = g(n)$ 经过 D/A 转换后输入到模拟模块, 作为忆阻器的激励信号; 3) 在下一个采样时钟到来时, 对忆阻器输入端进行采样, 得到电压响应 $x(t)$; 4) 电压响应 $x(t)$ 经过 A/D 转换后反馈给数字模块, 对数字系统中的混沌映射进行扰动. 如此反复. 其中映射子模块中的单元 $1, 2, \cdots, L$ 分别对应近邻耦合锯齿映像格子模型中的 $1, 2, \cdots, L$ 级, 序列输出子模块可以根据具体需求, 从映射子模块中抽取任意单元, 经组合和量化后得到所需的随机数.

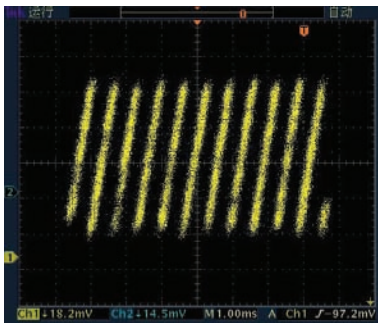

图 9 (网刊彩色) 吸引子示波器图

Fig. 9. (color online) Attractor on oscilloscope.

本数模混合随机数发生器具有如下优点: 1) 以最少的模拟器件保证系统的混沌性, 有效缓解了模拟器件参数不稳定对整体电路的影响, 保证了电路的稳定性; 2) 引入了具有记忆功能的非线性电阻, 忆阻器, 增强了所产生序列的随机性; 3) 映射子模块占用芯片资源极少, 单元数 L 可以任意扩展, 只需相应增加映射的级数 L 就可以产生更高速率的随机数, 例如 FPGA 工作频率为 200 MHz, 若采用映射子模块每一级输出数据进行组合量化的工作方式, 那么产生的随机数带宽可达 $200L$ MHz. 根据目前 FPGA 芯片的容量及规模, 可产生 100 Gbit/s 以上速率的随机数, 易于满足各种实际需求; 4) 混合系统基于数字芯片和一个模拟器件实现, 保证了序列产生速率和系统鲁棒性, 结构上兼容性好且易于集成到现有的电路系统中.

本文利用 Nist-800-22rev1a 测试套件对得到的随机数进行测试 [16]. 该套件共有 15 项测试标准, 专用于测试由硬件或软件产生的长随机数的随机性, 从不同角度检验被测序列在统计特性上相对于理想随机数的偏离程度.

测试时选取一定长度的随机数, 将其分为若干个数据流进行测试. 对应于每种测试标准, 都会计算出相应的 P-value, 将所得 P-value 与已知的显著性水平 α 相比较, 当 P-value$< \alpha$ 时, 即判定所测序列未通过测试, 否则判定为通过测试. 本测试套件所选取的显著性水平 $\alpha = 0.01$.

表 2 给出了利用图 8 混合系统所产生的随机数进行 NIST 测试时所得到的结果, 选取映射子模块的级数 $L = 500$, 序列长度为 40 Mbit, 将其分为 100 个数据流进行测试. 从表 2 中可以看出, 所产生

的随机数顺利通过所有测试, 且成功比例高, 序列的随机性好, 能够适应实际的应用需求.

表 2 数模混合系统随机数的 NIST 测试结果

Table 2. NIST test results of hybrid system PN sequence.

测试项目	*P*-value	成功比例	测试结果
Frequency	0.224821	98/100	通过
Block frequency	0.719747	100/100	通过
Cumulative sums	0.215387	97/100	通过
Cumulative sums	0.971699	98/100	通过
Runs	0.494392	99/100	通过
Longest run	0.466882	99/100	通过
Rank	0.554420	98/100	通过
FFT	0.946308	99/100	通过
Non-overlapping template	0.554420	98/100	通过
Overlapping template	0.911413	99/100	通过
Universal	0.474986	98/100	通过
Approximate entropy	0.494392	100/100	通过
Random excursions	0.242986	40/42	通过
Random excursions variant	0.739918	41/42	通过
Serial	0.304126	100/100	通过
Serial	0.190936	99/100	通过
Linear complexity	0.867692	98/100	通过

5 结 论

随着随机数在各个领域的广泛使用, 对随机数发生器的要求也日益增高. 基于模拟方法实现的混沌随机数发生器存在系统对参数和初始值敏感的问题, 从而影响所得随机数的统计特性, 大大限制了其应用范围; 基于数字方法实现的随机数发生器能降低模拟实现时系统对参数和初始值误差敏感的影响, 然而数字系统的有限字长效应又必然会使混沌序列退化为周期序列, 无法产生真正意义上的随机数.

基于对以上问题的分析, 本文综合了模拟实现方法与数字实现方法的优点, 尝试用尽可能少的模拟器件构造数模混合系统, 提出了仅有一个模拟器件的数模混合系统, 解决了系统动力特性退化、系统模拟器件过多限制了序列产生速率和系统鲁棒性等问题, 使系统更加易于集成.

忆阻器作为除电阻、电容和电感三个基础元件之外的第四种基础元件, 自惠普公司实验室报道了其可实现性以来, 极大地激发了人们开展忆阻器研究的兴趣. 本文介绍了 Bao 等[31] 提出的一阶广义忆阻器, 忆阻器由一个有记忆功能的桥电路和一个一阶并联 RC 滤波器组成. 该一阶广义忆阻器与 FPGA 一起实现了本文所提的基于数模混合系统的随机数发生器.

本文给出了基于单个忆阻器反馈的数模混合系统框图, 分析了数模混合系统的实现方法, 验证了方法的有效性, 并结合典型映射给出了仿真结果图. 实际电路验证了系统具有较强的鲁棒性、无有限字长效应、易于产生高速率随机数以及便于集成的优点. 最终数模混合随机数发生器产生的随机数以较高成功率顺利通过 NIST 所有测试. 本文方法所产生的随机数将能够很好地满足图像加密、保密通信以及雷达波形设计等领域的实际工程需求.

参考文献

[1] Sivakumar T, Venkatesan R 2015 *KSII Trans. Internet Inf. Syst.* **9** 6

[2] van Wiggeren G D, Roy R 1998 *Phys. Rev. Lett.* **81** 3547

[3] Yao J, Chen G R, Yue C, Zhao Y 2002 *ICCA the 2002 International Conference on Control and Automation* Xiamen, June 19–19, 2014 p152

[4] Gini F, Maio A D, Patton L 2012 *Waveform Design and Diversity for Advanced Radar Systems* (UK: The Institution of Engineering and Technology) pp31–32

[5] Li W, Reidler I, Aviad Y, Huang Y Y, Song H L, Zhang Y H, Rosenbluh M, Kanter I 2013 *Phys. Rev. Lett.* **111** 044102

[6] Naruse M, Kim S J, Aono M, Hori H, Ohtsu M 2014 *Sci. Rep.* **4** 6039

[7] Petrie C S, Connelly J A 2000 *IEEE Trans. Circ. I* **47** 5

[8] Bao B C, Hu W, Xu J P, Liu Z, Zou L 2011 *Acta Phys. Sin.* **60** 120502 (in Chinese) [包伯成, 胡文, 许建平, 刘中, 邹凌 2011 物理学报 **60** 120502]

[9] Li C B, Sprott J C 2014 *Int. J. Bifurc. Chaos* **24** 1450131

[10] Li C B, Sprott J C, Thio W 2014 *J. Exp. Theor. Phys.* **118** 494

[11] Li C B, Sprott J C 2014 *Phys. Lett. A* **378** 178

[12] Bao B C 2013 *An Introduction to Chaotic Circuits* (Vol. 1) (Beijing: Science Press) pp87–89

[13] Shao S Y, Min F H, Wu X H, Zhang X G 2014 *Acta Phys. Sin.* **63** 060501 (in Chinese) [邵书义, 闵富红, 吴薛红, 张新国 2014 物理学报 **63** 060501]

[14] Wang G Y, Bao X L, Wang Z L 2008 *Chin. Phys. B* **17** 3596

[15] Deng Y S, Hu H P, Xiong N X, Xiong W, Liu L F 2015 *Inform. Sci.* **305** 146
[16] Ergun S, Özoğuz S 2010 *Int. J. Circ. Theor. Appl.* **38** 1
[17] Güler Ü, Ergün S 2010 *ICECS 17th IEEE International Conference* Athens, December 12–15, 2010 p1037
[18] Ergün S 2014 *Circuits and Systems (APCCAS), 2014 IEEE Asia Pacific Conference* Ishigaki, November 17–20, 2014 p217
[19] Hu H P, Deng Y S, Liu L F 2014 *Commu. Nonlinear Sci.* **19** 1970
[20] Yeniçeri R, Yalçın M E 2013 *Electron. Lett.* **49** 543
[21] Chua L O 1971 *IEEE Trans. Circ. Theor.* **18** 507
[22] Chua L O, Kang S M 1976 *Proc. IEEE* **64** 209
[23] Strukov D B, Snider G S, Stewart D R, Williams R S 2008 *Nature* **453** 80
[24] Bao B C, Ma Z H, Xu J P, Liu Z, Xu Q 2011 *Int. J. Bifurc. Chaos* **21** 2629
[25] Wang L D, Drakakis E, Duan S K, He P F, Liao X F 2012 *Int. J. Bifurc. Chaos* **22** 1250205
[26] Bao B C, Xu J P, Zhou G H, Ma Z H, Zou L 2011 *Chin. Phys. B* **20** 120502
[27] Muthuswamy B 2010 *Int. J. Bifurc. Chaos* **20** 1335
[28] Kim H, Sah M P, Yang C J, Cho S, Chua L O 2012 *IEEE Trans. Circ. Syst. I* **59** 2422
[29] Yu D S, Liang Y, Chen H, Iu H H C 2013 *IEEE Trans. Circ. Syst. II* **60** 207
[30] Corinto F, Ascoli A 2012 *Electron. Lett.* **48** 824
[31] Bao B C, Yu J J, Hu F W 2014 *Int. J. Bifurc. Chaos* **24** 1450143
[32] Chua L O 2012 *Proc. IEEE* **100** 1920
[33] Tong Q Y, Zeng Y C 2003 *Acta Phys. Sin.* **52** 285 (in Chinese) [童勤业, 曾以成 2003 物理学报 **52** 285]

A digital-analog hybrid random number generator based on memristor*

Yuan Ze-Shi Li Hong-Tao† Zhu Xiao-Hua

(*School of Electronic and Optical Engineering, Nanjing University of Science and Technology, Nanjing 210094, China*)

(Received 12 August 2015; revised manuscript received 22 September 2015)

Abstract

Random number generator (RNG) plays an important role in many areas including image encryption, secure communication, radar waveform generation, etc. However, existing analog methods for random number (RN) cannot satisfy the demand of bit rate. In the even worse case, system parameters from analog devices are easily distorted by surroundings, leading to a weak system robustness. As a result, researchers start to turn to digital implementation which is stabler and more efficient than analog counterpart to produce RN. However, digital methods suffer dynamical degradation due to the limited word length effect. Though some remedies, such as increasing computing precision, cascading multiple chaotic systems, pseudo-randomly perturbing the chaotic system, switching multiple chaotic systems, and error compensation method, are proposed, the limitations are even inevitable. Recently, some continuous-time chaotic oscillators combined with digital devices were used to realize RNG, and a novel approach was proposed to solve the dynamical degradation of digital chaotic system by coupling the given digital chaotic map with an analog chaotic system, where the analog chaotic system is used to anti-control the given digital chaotic map. But this method requires a whole continuous-time system realized with analog devices which restrict the performance of the integral system.

In this paper, a novel digital-analog hybrid chaotic system with only one analog device is constructed for the production of RN. The chosen analog device is a generalized memristor consisting of a diode bridge and a parallel RC filter.

Memristor is the fourth fundamental electronic component which has provoked extensive researches since the successful realization by Stan Williams's group at HP Labs in 2008.

The paper is arranged as follows. Firstly, a generalized memristor realized by a memristive circuit is introduced and its basic properties are given. Then the block diagram of the digital-analog hybrid system based on a single memristor feedback is depicted, and the mathematical model of the system is derived from the block diagram. Thirdly, the simple Logistic map is applied to the hybrid model and its dynamic behaviors are simulated and compared with those from the ideal Logistic before a more complex two-way coupled saw tooth map is applied to the same simulation, verifying the effectiveness of the proposed hybrid system. Finally, the complex coupled map is applied to the practical circuit producing RN which passes the NIST test suite smoothly.

The hybrid system has the following advantages: firstly, the introduction of the analog memristor is able to overcome the dynamical degradation in a digital system, avoiding the limited word length effect essentially. Secondly, the least analog device alleviates the sensibility to parameters and the restriction on bit rate in analog systems, ensuring that the hybrid system is robust. Thirdly, the system structure can be easily integrated into a relevant system. By designing the circuits of the system, the field programmable logic gate array of digital part can be used to realize chaotic map while the single memristor acts as a feedback to the digital part.

The experimental results show that the novel hybrid system is insensitive to the variations of circuit parameters and the produced RN is of great randomness, satisfying the practical applications.

Keywords: random number generator, limited word length, digital-analog hybrid, memristor

PACS: 05.45.–a, 05.45.Gg, 05.45.Pq, 05.45.Ra **DOI:** 10.7498/aps.64.240503

* Project supported by the National Natural Science Foundation of China (Grant No. 61401204), the Science and Technology Plan Support Project of Jiangsu Province, China (Prospective Joint Research Project) (Grant No. BY2015004-03), and the Postdoctoral Foundation Project of Jiangsu Province, China (Grant No. 1501104C).

† Corresponding author. E-mail: liht@njust.edu.cn