

数字混沌信号发生器的设计与实现

薛 华, 韩春艳

(滨州学院 物理与电子科学系, 山东 滨州 256603)

(hyd100_xh@163.com)

摘 要:为产生新的数字混沌伪随机序列,构造了一个新的混沌系统。利用理论分析和数值仿真的方法对系统的一些基本特性,如耗散性、平衡点、稳定性、Lyapunov 指数、分叉进行了详细分析,通过设计一个模拟混沌电路验证了系统的混沌性。在此模拟电路的基础上,设计了一个由集成运放构成的电压比较器来量化这个模拟混沌信号,在实验中获得数字伪随机序列。这种产生数字混沌序列的方法可应用于保密通信和信息加密之中。

关键词:混沌系统;伪随机序列;电路设计;量化

中图分类号: TP309 **文献标志码:** A

Design and implementation of digital chaotic signal generator

XUE Hua, HAN Chun-yan

(Department of Physics and Electronic Science, Binzhou University, Binzhou Shandong 256603, China)

Abstract: In order to generate new chaotic pseudo-random sequences, a new chaotic system was constructed. Some basic properties, including dissipativity, equilibrium, stability, Lyapunov exponent spectrum and bifurcation of this chaotic system were analyzed in detail through theoretical analysis and numerical simulation. Chaotic behaviors of the system were confirmed by designing an analog chaotic circuit. Moreover, a voltage comparator consisting of integrated op-amps was designed to quantify the chaotic analog signal, and the digital pseudo-random sequences generated from the quantization circuit were experimentally obtained. The approach to generating digital chaotic sequence can be applied in secret communications and information encryption.

Key words: chaos system; pseudo-random sequences; circuit design; quantization

0 引言

混沌系统的类随机性、类噪声、宽带功率谱、对初值敏感性等特性表明,它是一类天然的性能优良的伪随机序列发生器的源^[1-3]。由混沌系统迭代产生的序列经量化和判决后可得到混沌伪随机序列,其主要优点是具有良好的相关特性、对初始条件和控制参数的敏感性,同时便于产生和复制,因而可以取代传统的伪随机序列,应用于扩频通信、密码学、自动控制等领域^[4]。近期许多文献提出了伪随机序列的实现方法^[5-8],可用模拟电路或数字电路产生 PN 序列,但大多以低维混沌映射作为产生伪随机序列的“源”。而低维混沌结构简单,密钥空间相对较小,由此产生的 PN 序列用于信息加密其安全性较差。

因此,本文提出了一个连续的三维混沌系统,在对其基本特性分析的基础上,以该混沌系统作为产生伪随机序列的信号源,利用简单的量化电路设计并实现了一种新的混沌伪随机序列发生器,该伪随机序列发生器可应用于混沌保密通信或混沌信息加密之中。

1 混沌模型

构造了如下混沌系统(以下简称系统1):

$$\begin{cases} \dot{x} = ax - yz \\ \dot{y} = -cy + xz \\ \dot{z} = -bz + xy \end{cases} \quad (1)$$

在新的混沌系统(系统1)中每个方程都含有一个非线性乘积项,具有5个平衡点和较大的混沌范围,有更复杂的分叉行为和动力学特性。当 $a=3, b=4, c=10$ 时系统存在一个混沌吸引子,如图1所示。

2 基本动力学特性

2.1 系统的耗散性

系统1的散度为:

$$\nabla V = \frac{\partial \dot{x}}{\partial x} + \frac{\partial \dot{y}}{\partial y} + \frac{\partial \dot{z}}{\partial z} = a - c - b$$

只有当 $a - c - b < 0$ 时,系统1是耗散的,符合产生混沌的耗散性条件。例如,当 $a=3, b=4, c=10$ 时, $a - c - b = 3 - 10 - 4 = -11 < 0$ 。

2.2 平衡点及稳定性

先求系统1的平衡态(定常状态解),令式左边 $\dot{x}=0, \dot{y}=0, \dot{z}=0$,则得:

$$\begin{cases} ax = yz \\ cy = xz \\ bz = xy \end{cases}$$

解这个方程得到系统的5个平衡点:

$$s_0 = (0, 0, 0)$$

$$s_1 = (\sqrt{bc}, \sqrt{ab}, \sqrt{ac})$$

$$s_2 = (\sqrt{bc}, -\sqrt{ab}, -\sqrt{ac})$$

$$s_3 = (-\sqrt{bc}, -\sqrt{ab}, \sqrt{ac})$$

$$s_4 = (-\sqrt{bc}, \sqrt{ab}, -\sqrt{ac})$$

在 s_0 处线性化方程,得 Jacobian 矩阵:

$$J_0 = \begin{bmatrix} a & -z & -y \\ z & -c & x \\ y & x & -b \end{bmatrix} = \begin{bmatrix} a & 0 & 0 \\ 0 & -c & 0 \\ 0 & 0 & b \end{bmatrix}$$

其特征方程为 $|J| - \lambda I = 0$, 得到方程:

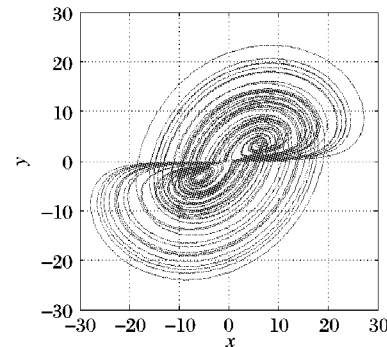
$$\lambda^3 + (b+c-a)\lambda^2 + (bc-ac-ab)\lambda - abc = 0$$

判断系统1的平衡点是否稳定从而判断是否可能出现混沌有两种方法:1)利用 Routh-Hurwitz 稳定判据,由特征方程各项系数所构成的 Hurwitz 行列式的各阶主子式至少有一项为负,证明该平衡点是不稳定的,系统可能产生混沌。2)特征方程的特征根,至少有一项大于零时,证明该平衡点是不稳定的,系统可能产生混沌^[9]。令:

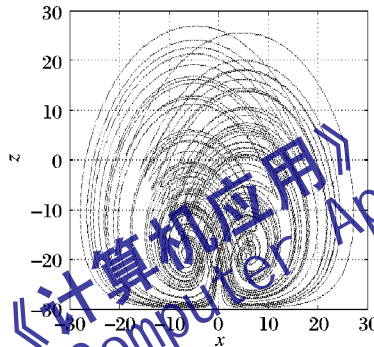
$$a_0 = 1$$

$$a_1 = b+c-a$$

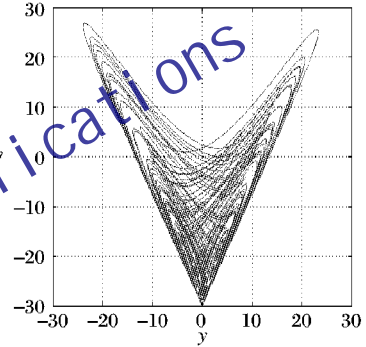
$$a_2 = bc-ac-ab$$



(a) x-y平面



(b) x-z平面



(c) y-z平面

图1 系统1的混沌吸引子在相平面上的投影

在 s_0 处,当 $a=3, b=4, c=10$ 时系统1的特征方程变为:

$$\lambda^3 + 11\lambda^2 - 2\lambda - 120 = 0$$

解方程得特征根: $\lambda_1 = -10, \lambda_2 = -4, \lambda_3 = 3$ 。

系统1的特征方程特征根 $\lambda_3 = 3 > 0$, 由此证明平衡点 s_0 不稳定。两种情况都保证原点是一个三维相空间中的鞍点。

在平衡点 s_1, s_2, s_3, s_4 线性化系统,得到相同的特征多项式:

$$\lambda^3 + (b+c-a)\lambda^2 + 4abc = 0$$

当 $a=3, b=4, c=10$ 时,线性化系统在 s_1, s_2, s_3, s_4 的 Jacobian 矩阵具有相同的特征值: $\lambda_1 = -13.596, \lambda_{2,3} = 1.2982 \pm j5.7981$,且满足 Shil'nikov 定理,即对于三阶自治系统平衡点的特征值 γ_1 及 $\sigma_1 \pm j\omega_1$,若满足 $\sigma_1 \gamma_1 < 0$,且 $|\gamma_1| > |\sigma_1|$,此时,系统1满足产生混沌的鞍焦点条件^[10]。

2.3 Lyapunov 指数和分岔图

为了研究参数变化对系统动力学特性的影响,固定参数 $a=3, c=10$,使参数 b 在区间 $[0, 8]$ 内变化, Lyapunov 指数随 b 变化的指数图谱和变量 x 随 b 变化的分岔图见图2~3。

由图2~3可看出,当 b 由0逐渐增加至1.08时,该区间存在着3个周期窗口,与弱混沌区、拟周期区交替出现, $b \in [1.08, 1.16]$ 时,系统是周期的; $b \in [1.16, 1.7]$ 时,系统是混沌的; $b \in [1.7, 1.8]$ 时,系统是周期的; $b \in [1.8, 4.65]$ 时,系统是混沌的; $b \in [4.65, 4.69]$ 时,系统是周期的; $b \in [4.68, 6.8]$ 时,系统是混沌的; $b \in [6.8, 8]$ 时,系统在周期

$$a_3 = -abc$$

根据 Routh-Hurwitz 稳定判据,系统稳定的充分必要条件是:由特征方程各项系数所构成的 Hurwitz 行列式的各阶主子式均大于0,即:

$$\begin{cases} D_1 = a_1 > 0; b+c-a > 0 \\ D_2 = \begin{vmatrix} a_1 & a_3 \\ a_0 & a_2 \end{vmatrix} > 0; \\ (b+c-a)(bc-ac-ab) + abc > 0 \\ D_3 = \begin{vmatrix} a_1 & a_3 & 0 \\ a_0 & a_2 & 0 \\ 0 & a_1 & a_3 \end{vmatrix} > 0; \\ (b+c-a)(bc-ac-ab)(-abc) - a^2b^2c_2 > 0 \end{cases} \quad (2)$$

为使系统1产生混沌,式(2)中各项至少应至少有一项为负。当 $a=3, b=4, c=10$ 时,经过计算, $D_1 > 0, D_2 > 0, D_3 < 0$, 由此证明平衡点 s_0 不稳定。

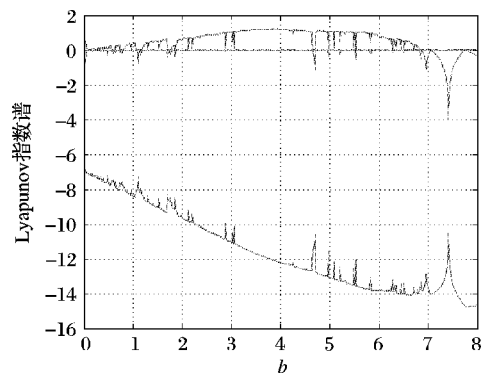


图2 Lyapunov 指数谱($a=3, c=10, b \in [0, 8]$)

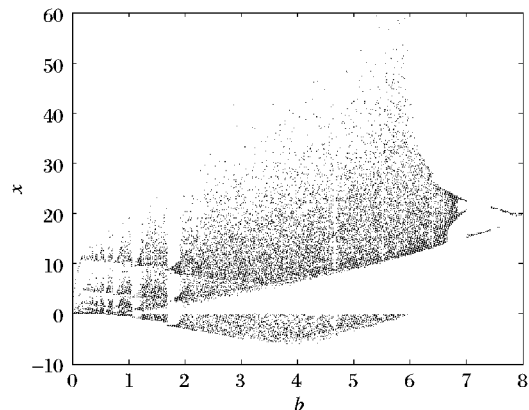


图3 分岔图($a=3, c=10, b \in [0, 8]$)

和拟周期区交替出现。

3 混沌系统的电路设计与实现

为了利用模拟电路产生数字混沌信号,基于模拟电子电

路的设计原理设计了如图4所示的混沌电路。该电路由集成运放(LF347)及其外围电路可实现加、减、反相、积分运算,电路中的乘法器(AD633)可实现非线性乘积项,乘法器的增益为0.1。

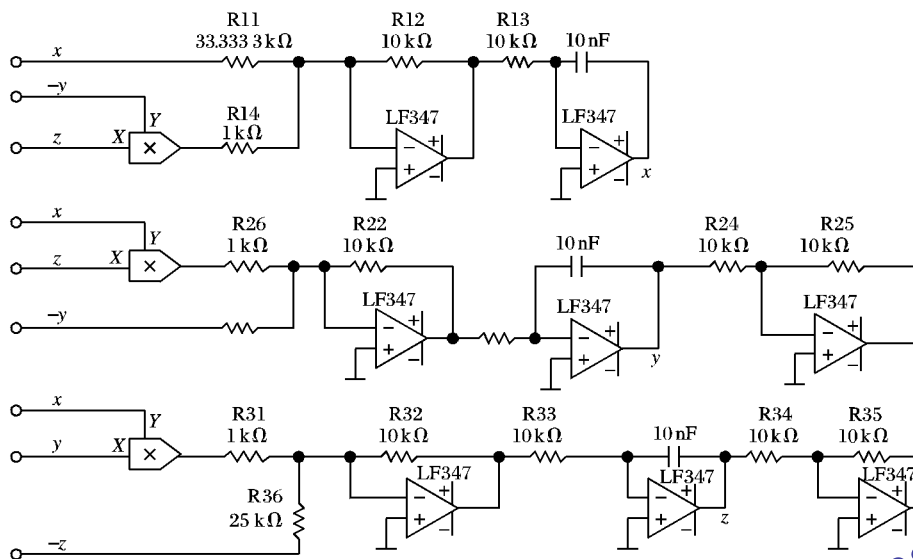


图4 系统1的混沌电路

固定参数:

$$R_{12} = R_{22} = R_{32} = 10 \text{ k}\Omega$$

解得:

$$R_{14} = R_{26} = R_{31} = 1 \text{ k}\Omega$$

$$R_{11} = 33.3333 \text{ k}\Omega$$

$$R_{21} = 10 \text{ k}\Omega$$

$$R_{36} = 25 \text{ k}\Omega$$

根据图4所示的电路搭建硬件电路,通过示波器观察到的混沌吸引子如图5所示,其实验结果和Matlab仿真结果相同。

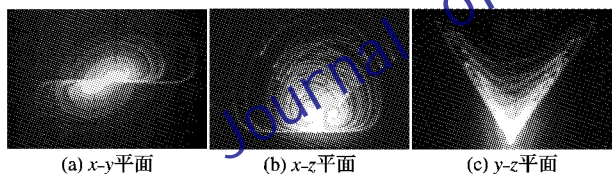


图5 从实验中观察到的混沌吸引子相图

4 数字混沌信号的实现

在非线性电路系统中,混沌信号由于具有内在的随机行为,它的非周期、连续宽带频谱、类似的噪声等特性是很适用于保密通信系统的。由于数字通信明显优于模拟通信,数字通信已成为当代通信技术的主流。当把混沌信号应用到数字通信加密中时,需要把模拟混沌信号量化为二进制的数字混沌信号^[11]。量化的方法有门限判决方法、有限精度量化方法、均匀量化方法等。

量化的原理是采用一阶离散化公式:

$$\dot{x} = \frac{x[k+1] - x[k]}{dt}$$

将式(1)离散化,得到系统的离散化方程如下:

$$\begin{cases} x[k+1] = x[k] + dt(ax[k] - y[k]z[k]) \\ y[k+1] = y[k] + dt(-cy[k] + x[k]z[k]) \\ z[k+1] = z[k] + dt(-bz[k] + x[k]y[k]) \end{cases} \quad (2)$$

本文采用门限判决量化的方法,在混沌模拟电路的输出端引入一个反相放大器和一个滞回比较器,形成一个量化电路。如图6所示。

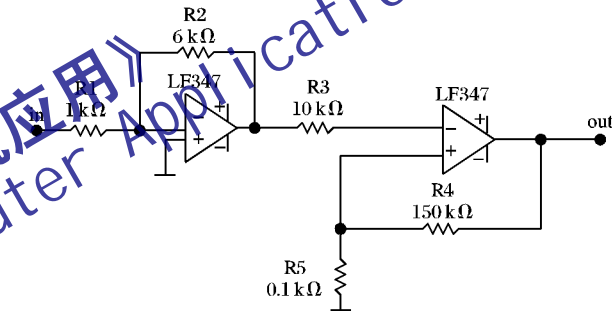


图6 量化电路的原理

在该量化电路中,反相放大器可以把混沌序列的状态值控制在一定的范围之内,根据混沌序列的状态值的取值范围,设定比较器的上门限电平为 v_{ih} 和下门限电平为 v_{il} ,如果混沌序列的状态值 $x(t)$ 大于上门限 v_{ih} ,则二进制序列 $q(x)$ 为1;如果混沌序列的状态值 $x(t)$ 小于下门限 v_{il} ,则二进制序列 $q(x)$ 为0,输出电压由 $+U_z$ 跳变为 $-U_z$ 即:

$$q(x) = \begin{cases} 1, & x > v_{ih} \\ 0, & x < v_{il} \end{cases}$$

相应的门限宽度为:

$$\Delta U_T = \frac{2R_5}{R_4 + R_5} U_z$$

通过量化电路,在滞回比较器的输出即为混沌数字信号。

在量化电路中,设置合适的参数,通过电子工作平台(Electronic Workbench,EWB)对 x 端输出的模拟信号进行量化,可以观察到该量化的二进制数字信号,如图7所示。搭建的硬件电路通过数字示波器观察到的 x 端输出的量化序列,如图8所示。

5 结语

本文提出了一个新的三维二次自治混沌系统,该系统含有3个参数,每个方程含有一个非线性乘积项,利用理论推导、数值仿真、Lyapunov指数谱和Hopf分叉图对系统的基本动力学特性进行了分析。结果表明,该系统具有5个平衡点,

当参数满足一定条件时,系统是混沌的,该系统具有较大的 Lyapunov 指数,能够产生复杂的混沌吸引子和一些奇特的动力学行为。设计了实现该系统的模拟混沌电路,电路实验结果和动力学特性分析、数值仿真完全相同。同时,为了得到二进制的数字信号,在模拟电路的基础上,设计了一个量化电路,通过 EWB 仿真和硬件电路验证,可以得到数字混沌信号。本文提出的混沌系统和混沌电路,可产生混沌伪随机序列并应用于混沌通信和混沌信息加密之中。

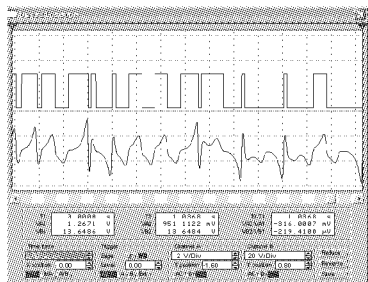


图 7 通过 EWB 仿真观察到 x 输出时的量化序列图

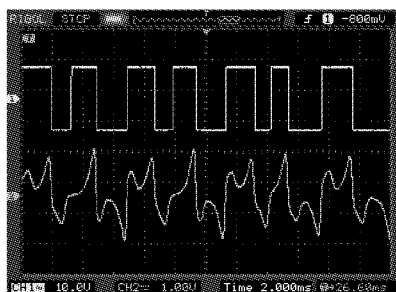


图 8 数字示波器观察到 x 输出时的量化序列图

参考文献:

- [1] 雷莉萍. 基于混沌的随机序列发生器设计及其应用[D]. 南京: 南京航空航天大学, 2007.
- [2] WANG GUANG-YI, QIU SHUI-SHENG, LI HONG-WEI, *et al.* A new chaotic system and its circuit realization[J]. Chinese Physics, 2006, 15(12): 2872 - 2977.
- [3] WANG GUANGYI, BAO XULEI. Design and FPGA implementation of a new hyperchaotic system [J]. Chinese Physics B, 2008, 17(10): 3596 - 3602.
- [4] 罗松江, 丘水生, 骆开庆. 混沌伪随机序列的复杂度的稳定性研究[J]. 物理学报, 2009, 58(9): 6045 - 6049.
- [5] STOJANOVSKI T, KOCAREV L. Chaos-based random number generators, Part I: analysis [J]. IEEE Transactions on Circuits Systems I, 2001, 48(3): 281 - 288.
- [6] STOJANOVSKI T, PIHL J, KOCAREV L. Chaos-based random number generators, Part II: practical realization [J]. IEEE Transactions on Circuits Systems, 2001, 48(3): 382 - 385.
- [7] DING Q, PANG J, FANG J, *et al.* Designing of chaotic system output sequence circuit based on FPGA and its applications in network encryption card [J]. International Journal of Innovative Computing, Information and Control, 2007, 3(2): 449 - 456.
- [8] LING C, WU X. Design and realization of an FPGA-based generator for chaotic frequency hopping sequences[J]. IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications, 2001, 48(5): 521 - 532.
- [9] 黄国生. 混沌及其应用[M]. 武汉: 武汉大学出版社, 2003.
- [10] 王义文, 丘水生, 许志益. 一个新的三维二次混沌系统及其电路实现[J]. 物理学报, 2006, 55(7): 3295 - 3301.
- [11] 韩春艳, 薛华, 吴新华. 一个新的混沌模型及其数字伪随机信号的实现[J]. 河北师范大学学报, 2010, 34(2): 165 - 169.

(上接第 2976 页)

表 5 FRGHT 与 FGHT、RGHT 的比较

缩放 s	旋转 $\alpha / (^{\circ})$	匹配方法	投票峰值	峰值位置 (x'_c, y'_c)	理想位置 (x''_c, y''_c)	匹配误差 E	计算时间/s
0.8	-16	RGHT	41.0000	(87, 109)		4.2426	3.3560
		FGHT	77.5821	(90, 104)	(90, 106)	1.4142	12.5620
		FRGHT	57.4374	(90, 106)		0	3.4370
1.0	16	RGHT	53.0000	(100, 113)		5.3852	3.7380
		FGHT	82.4375	(104, 111)	(105, 111)	1.0000	13.5820
		FRGHT	61.8782	(104, 112)		1.4142	3.8840
1.2	32	RGHT	59.0000	(118, 154)		6.4031	3.0300
		FGHT	83.5224	(116, 158)	(114, 159)	2.2361	14.7370
		FRGHT	70.1374	(113, 59)		1.0000	3.9880

6 结语

本文结合 FGHT 和 RGHT 算法提出了 FRGHT 算法,对该方法的理论基础和具体实现进行了详细的论述。经过上述实验验证了此算法具有精度高、计算量小等优点。利用本文算法得到的参数信息再经过多项式拟合等算法可以得到亚像素精度位姿。此算法经过优化可以较好地满足工业应用中实时性及高精度的要求。

参考文献:

- [1] HOUGH V, PAUL C. Method and mean for recognizing complex patterns: USA, 3069654 [P]. 1962.
- [2] BALLARD D H. Generalizing the Hough transform to detect arbitrary shapes [J]. Pattern Recognition, 1981, 13(2): 111 - 122.
- [3] FUNG P-F, LEE W-S, KING I. Randomized generalized Hough transform for 2-D grayscale object detection [C]// ICPR'96: Proceedings of the 13th International Conference on Pattern Recogni-

tion. Washington, DC: IEEE Computer Society, 1996, 2: 511 - 515.

- [4] IZADINIA H, SADEGHI F, EBAZADEH M M. Fuzzy generalized Hough transform invariant to rotation and scale in noisy environment [C]// Proceedings of the 18th International Conference on Fuzzy Systems. Washington, DC: IEEE, 2009: 153 - 158.
- [5] ROSS T J. Fuzzy logic with engineering applications [M]. New York: McGraw-Hill, 1995.
- [6] MAMDANI E H, ASILIAN S. An experiment in linguistic synthesis with a fuzzy logic controller [J]. International Journal of Human-Computer Studies, 1999, 51(2): 135 - 147.
- [7] XU LEI, OJA E. Randomized Hough Transform (RHT): Basic mechanisms, algorithms, and computational complexities [J]. CVGIP: Image Understanding, 1993, 57(2): 131 - 154.
- [8] ULRICH M, STEGER C, BAUMGARTNER A. Real-time object recognition using a modified generalized Hough transform [J]. Pattern Recognition, 2003, 36(11): 2557 - 2570.