第 38 卷　第 6 期
2023 年 12 月

天津科技大学学报
Journal of Tianjin University of Science & Technology

Vol. 38　No. 6
Dec. 2023

DOI:10.13364/j.issn.1672-6510.20230075
数字出版日期：2023–07–20；数字出版网址：http://kns.cnki.net/kcms2/detail/12.1355.N.20230720.1434.003.html

一种基于多卷保守混沌系统的伪随机信号发生器的设计及实现

贾红艳，李　伟，刘靖雯
（天津科技大学电子信息与自动化学院，天津 300222）

摘　要：为产生新的数字混沌伪随机序列，提出一个哈密顿能量与体积均保守的多卷保守混沌系统，且分别利用理论分析和数值分析的方法研究系统的保守性、稳定性、多卷特性等动力学特性。可以发现，系统具有很好的遍历性、复杂性以及较强的伪随机性。对系统进行美国国家标准技术研究所（NIST）测试，所有的测试指标均满足伪随机信号的标准条件。另外，还利用现场可编程门阵列（FPGA）技术设计实现了该多卷保守混沌系统，为混沌应用提供多卷保守混沌系统模型及伪随机信号发生器。

关键词：保守混沌系统；NIST 测试；FPGA 实现；伪随机信号
中图分类号：TP309　　**文献标志码**：A　　**文章编号**：1672-6510（2023）06-0069-06

Design and Implementation of a Pseudo-Random Signal Generator Based on Multi-Scroll Conservative Chaotic System

JIA Hongyan，LI Wei，LIU Jingwen
（College of Electronic Information and Automation，Tianjin University of Science & Technology，Tianjin 300222，China）

Abstract：In order to generate a new digital chaotic pseudo-random sequence，a multi-scroll conservative chaotic system with both Hamiltonian energy conservation and volume conservation is proposed in our present study. Dynamic characteristics of the system including conservative characteristics，stability，and multi-scroll characteristics were also respectively studied based on theoretical analysis and numerical analysis. It is found that the system has good ergodicity，complexity and strong pseudo-randomness. National Institute of Standards and Technology（NIST）test was further performed for the system，and all the results met standard conditions for pseudo-random signals. Moreover，the multi-scroll conservative chaotic system was designed to implement by field programmable gate array（FPGA）technology，which has provided a multi-scroll conservative chaotic system model and a pseudo-random signal generator for chaos applications.

Key words：conservative chaotic systems；NIST test；FPGA implementation；pseudo-random signal

伪随机序列产生技术是集数学、计算机科学、电子与通信科学等诸多学科于一身的技术，该产生技术自 20 世纪末至今一直是国内外的研究热点，并取得了大量的成果[1–2]。混沌系统的伪随机性、宽带功率谱、对初值敏感性等特性表明它能够有效地产生伪随机信号[3–6]。由混沌系统迭代产生的序列经量化和判决后可得到伪随机序列，其主要优点是具有良好的相关特性以及对初始条件和控制参数的敏感性，同时该伪随机序列便于产生和复制，因而可以取代传统的伪随机序列[7–11]。最初，基于混沌系统产生的伪随机信号通常由模拟电路产生，常用于保密通信研究。然而，模拟电路的元器件易受温度、外界磁场强度等因素影响，影响了伪随机信号的性能[12–14]。近几年，随着电子技术的快速发展，使利用数字电路设计伪随机

收稿日期：2023–03–29；**修回日期**：2023–05–19
基金项目：国家自然科学基金项目（61903274）
作者简介：贾红艳（1972—），女，天津人，副教授，jiahy@tust.edu.cn

信号发生器成为可能。现场可编程门阵列(FPGA)作为数字混沌电路的有效实现方法之一，能够很好地解决模拟电路中存在的问题[15–19]。目前，FPGA 被大量使用在通信设备上，通过 FPGA 设计基于混沌系统的伪随机信号发生器，可以为保密通信提供新的物理模型[20–25]。另外，与单卷或双卷保守混沌系统相比，多卷保守混沌系统具有遍历性和复杂性好、伪随机性强，且混沌序列类似于均匀分布白噪声等优点，更适合用于保密通信[26–30]。因此，本文提出一种多卷保守混沌系统，在对其特性进行分析的基础上，利用 FPGA 技术设计伪随机信号发生器，进一步丰富现有混沌系统模型与伪随机信号发生器种类。

1　多卷保守混沌模型

1.1　一种多卷保守混沌系统

基于现有哈密顿保守混沌系统理论基础，提出混沌系统模型，为

$$\begin{cases}\dot{x}=ay(y^2-d^2)(y^2-4d^2)+byw\\ \dot{y}=-ax(x^2-4d^2)\\ \dot{z}=cw\\ \dot{w}=-bx(x^2-4d^2)y-cz\end{cases}\tag{1}$$

式中：x、y、z、w 为状态变量，a 、b 、c 、d 为大于 0 的参数。

改变参数 d 的值可以控制系统相图涡卷中心点的位置。通过改变系统哈密顿能量的不变曲面拓展平衡点，理论上能够得到任意卷数的混沌流，但实际实施起来的难度随着卷数的增加而增大。因此本文选取固定参数 $a=6$ 、$b=4$ 、$c=6$ 、$d=1.2$，绘制 2×3 六卷保守混沌流。

当哈密顿能量为 $H(\boldsymbol{x})=\int x(x^2-4d^2)\mathrm{d}x+\int y(y^2-d^2)(y^2-4d^2)\mathrm{d}y+\int z\mathrm{d}z+\int w\mathrm{d}w=\frac{1}{4}x^4-2dx^2+\frac{1}{6}y^6-\frac{5}{4}d^2y^4+2d^4y^2+\frac{1}{2}z^2+\frac{1}{2}w^2$ 时，系统可以表示为

$$\dot{\boldsymbol{x}}=\boldsymbol{J}(\boldsymbol{x})\nabla H(\boldsymbol{x})=\begin{bmatrix}0&a&0&by\\-a&0&0&0\\0&0&0&c\\-by&0&-c&0\end{bmatrix}\cdot\begin{bmatrix}x(x^2-4d^2)\\y(y^2-d^2)(y^2-4d^2)\\z\\w\end{bmatrix}\tag{2}$$

可以观察到系统 $\boldsymbol{J}(\boldsymbol{x})$ 为反对称矩阵，即哈密顿能量的导数为

$$\dot{H}(\boldsymbol{x})=\nabla H^{\mathrm{T}}(\boldsymbol{x})\dot{\boldsymbol{x}}=\nabla H^{\mathrm{T}}(\boldsymbol{x})\boldsymbol{J}(\boldsymbol{x})\nabla H(\boldsymbol{x})=0\tag{3}$$

即，哈密顿能量为常数，说明系统(1)满足哈密顿能量保守。

进一步发现，系统的散度为

$$\nabla\cdot f=\frac{\partial\dot{x}}{x}+\frac{\partial\dot{y}}{y}+\frac{\partial\dot{z}}{z}+\frac{\partial\dot{w}}{w}=0\tag{4}$$

即，散度为零，说明系统(1)同时满足体积保守。

1.2　基本动力学特性

从数值角度研究系统的动力学特性，当系统哈密顿能量为常数即导数为零时，表明系统哈密顿能量保守。系统(1)哈密顿能量只与参数和初值有关，设定初值 $x(0)=y(0)=w(0)=z(0)=1.8$ 时，计算哈密顿能量 $H(\boldsymbol{x})\approx-3.26$ 。绘制系统(1)的哈密顿能量及其导数随时间 t 的变化如图 1 所示，可以观察到哈密顿能量为非零常数，哈密顿能量的导数为零，即系统(1)的哈密顿能量保守。

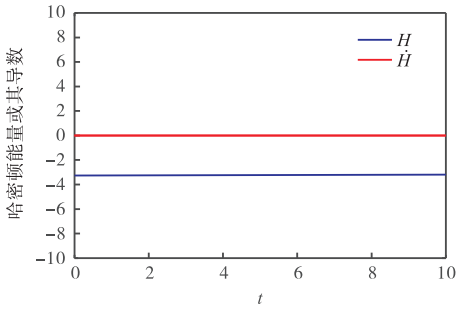

图 1　哈密顿能量及其导数图

Fig. 1　Hamiltonian energy and its derivatives

为了进一步研究参数变化对系统动力学特性的影响。绘制 $y(0)=w(0)=z(0)=1.8$ 时，系统的李雅普诺夫指数随 $x(0)$ 变化的图像，结果如图 2 所示。其中，E_{L1}、E_{L2}、E_{L3}、E_{L4} 分别表示 x、y、z、w 4 个状态变量的李雅普诺夫指数。可以观察到系统(1)最大李雅普诺夫指数大于零，即在相应初值条件下系统处于混沌状态，且李雅普诺夫指数关于 x 轴对称，表明李雅普诺夫指数和为 0。进一步从李雅普诺夫指数角度说明系统(1)相体积保守。绘制同等条件下系统(1)的分岔图，如图 3 所示。

根据对系统的哈密顿能量、李雅普诺夫指数图与分岔图进行分析，当初值为(1.8，1.8，1.8，1.8)时，系统处于保守混沌状态，绘制系统的相轨迹图如图 4 所示，可以观察到此时系统为分别沿 x、y 方向的 2×3 六卷保守混沌流。当初值为(0.3，1.8，1.8，1.8)时，系统

处于拟周期状态，绘制系统的相轨迹图如图 5 所示。

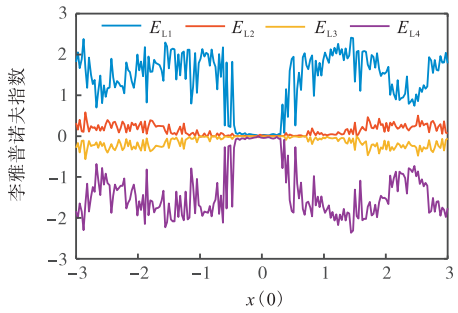

图 2　李雅普诺夫指数图

Fig. 2　Diagram of Lyapunov exponents

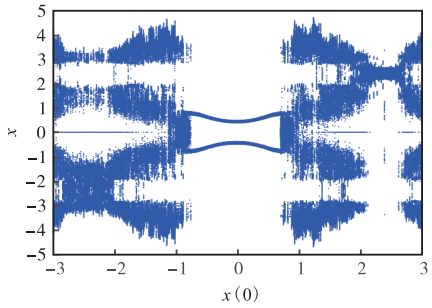

图 3　分岔图

Fig. 3　Bifurcation diagram

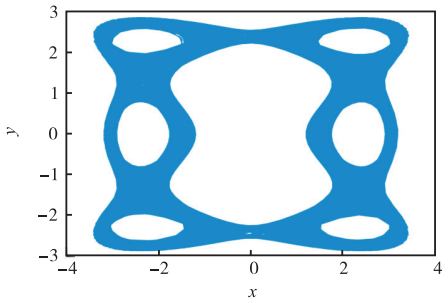

图 4　初值为 (1.8, 1.8, 1.8, 1.8) 时系统的相轨迹图

Fig. 4　Phase trajectory diagram of the system with initial values of (1.8, 1.8, 1.8, 1.8)

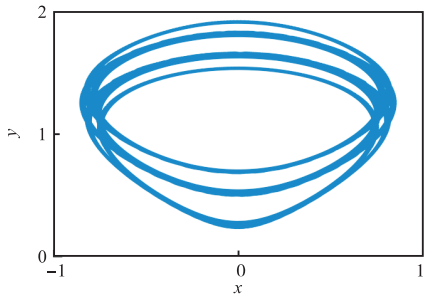

图 5　初值为 (0.3, 1.8, 1.8, 1.8) 时系统的相轨迹图

Fig. 5　Phase trajectory diagram of the system with initial values of (0.3, 1.8, 1.8, 1.8)

2　伪随机性测试

采用最具代表性且被普遍认可的美国国家标准技术研究所 (NIST) SP800-22 测试标准进行伪随机性测试。该标准将理想的随机序列作为参考，在统计特性上从不同角度检验目标伪随机序列的偏离程度，其中包括 15 项测试指标。15 项测试结果均用 P 值表示，能通过测试的序列具有良好的伪随机性能。

所有测试均取显著性水平 $\alpha=0.01$，测试序列 15 组，可定义通过率的置信区间为 (0.970 2, 1.009 8)。通常只有满足以下 3 个条件时，才能通过测试：(1) 每一项测试结果的 P 值都大于显著性水平 ($\alpha=0.01$)；(2) 测试序列的通过率位于置信区间 (0.970 2, 1.009 8) 内；(3) P 值的分布应该服从均匀性分布。

数据测试结果见表 1。通过表 1 的各项测试结果数据可以看出，系统 (1) 的 15 项测试的 P 值均大于显著性水平 ($\alpha=0.01$)，并且系统 (1) 的 15 项测试的通过率均位于置信区间内，因此该系统满足条件 (1) 和条件 (2)。15 组数据 P 值均应服从均匀性分布，本文以非重叠模块匹配检验 P 值为例进行验证，P 值分布的直方图如图 6 所示。由图 6 可以观察到非重叠模块匹配检验 P 值的分布相对均匀，无分布差距比较明显的区间，即满足条件 (3)。

表 1　数据测试结果

Tab. 1　Test results for the data

序号	测试项目	P 值	通过率/%
1	频率检验	0.401 199	100
2	块内频数检验	0.419 021	100
3	累加和检验	0.122 325	100
4	游程检验	0.175 719	99
5	块内最长游程检验	0.037 566	99
6	二元矩阵秩检验	0.534 146	99
7	离散傅里叶变换检验	0.122 325	99
8	非重叠模块匹配检验	0.779 188	99
9	重叠模块匹配检验	0.437 274	99
10	Maurer 的通用统计检验	0.657 933	99
11	近似熵检验	0.102 526	99
12	随机游动检验	0.585 209	100
13	随机游动频数检验	0.452 799	100
14	序列检验	0.437 274	100
15	线性复杂度检验	0.699 313	100

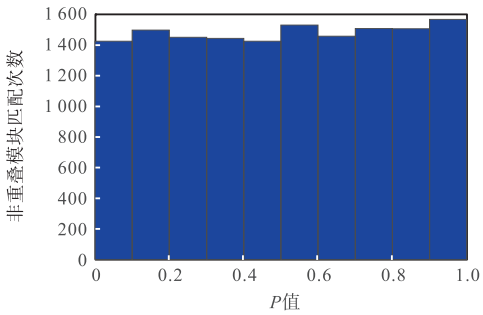

图 6　非重叠模块匹配 *P* 值的分布

Fig. 6　Distribution of matching *P*-values of non-overlapping modules

3　伪随机信号发生器物理实现

FPGA 具有非常丰富的运算单元，运算速度极快。目前，通过 FPGA 技术实现连续混沌系统的方法主要包含两种。

(1)利用 FPGA 特有的编程语言 Verilog HDL、System Verilog、VHDL 对混沌系统进行描述，编写程序完成对混沌系统的物理实现。

(2)使用 Xilinx 公司提供的 System generator 技术或者 Intel 公司提供的 DSP-builder 技术，在 MATLAB 的 Simulink 开发环境下，从上述两项技术的软件库中调取现有的硬件模块，搭建离散化后的混沌系统模型。

第一种方法程序编写十分困难，且产生的混沌信号不能被其他系统模块直接调用，不利于后续再进行其他研究；第二种方法不需要太多的编程基础，容易实现。本文系统结构相对简单，不需要占用太多硬件资源，因此采用第二种方法对混沌系统进行物理意义上的实现，验证其物理可实现性且产生伪随机信号。在设计电路模型时，采用欧拉法对系统进行离散化。

$$\begin{cases} x(n+1)=x(n)+\{ay(n)[y(n)y(n)-d^2]\cdot \\ \qquad [y(n)y(n)-4d^2]+by(n)w(n)\}\Delta T \\ y(n+1)=y(n)-ax(n)[x(n)x(n)-4d^2]\Delta T \\ z(n+1)=z(n)+cw(n)\Delta T \\ w(n+1)=w(n)-\{bx(n)[x(n)x(n)-4d^2]\cdot \\ \qquad y(n)+cz(n)\}\Delta T \end{cases} \tag{5}$$

式中：$\Delta T=0.001$，为离散采样时间；$x(n)$、$y(n)$、$z(n)$、$w(n)$ 为当前时间的迭代序列；$x(n+1)$、$y(n+1)$、$z(n+1)$、$w(n+1)$ 为下一周期的迭代序列。

对离散化后的系统进行物理仿真，在 Simulink 中搭建初值为(1.8，1.8，1.8，1.8)时系统的电路模型，如图 7 所示。子模块 1 的电路模型如图 8 所示，子模块 2、3 的电路模型如图 9 所示。

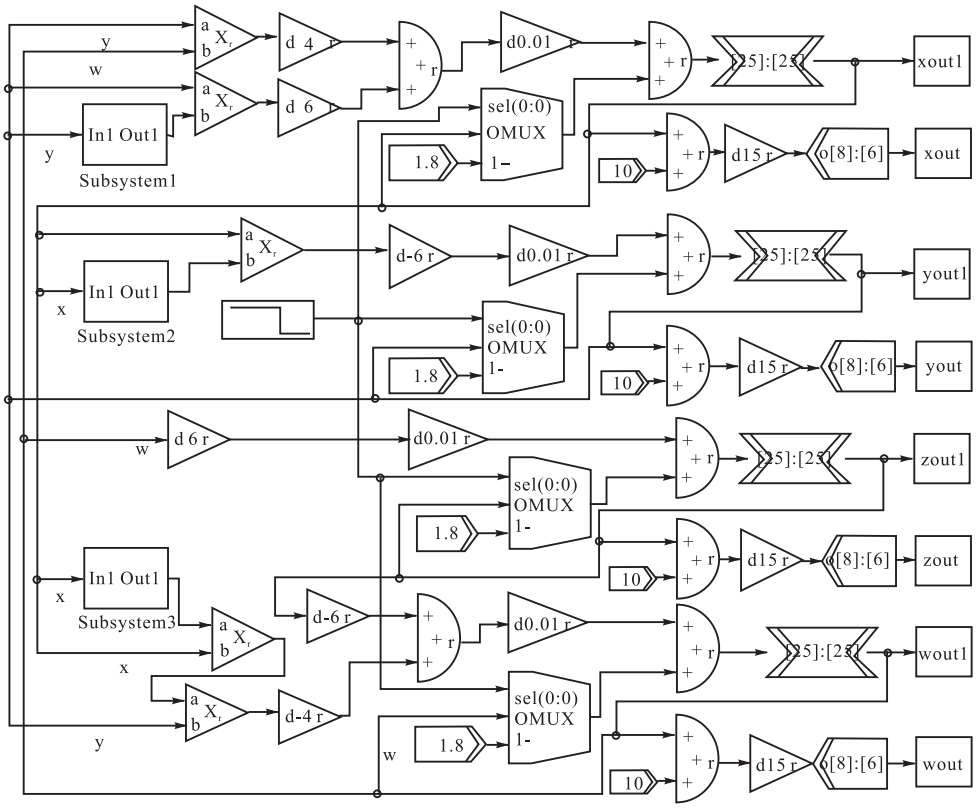

图 7　系统的电路模型

Fig. 7　Circuit model for the system

图7在示波器观察到随时间变化且无序的随机信号，截取其中一段 y 信号波形图如图 10 所示，同时观察到相轨迹图与数值分析结果一致，如图11 所示。

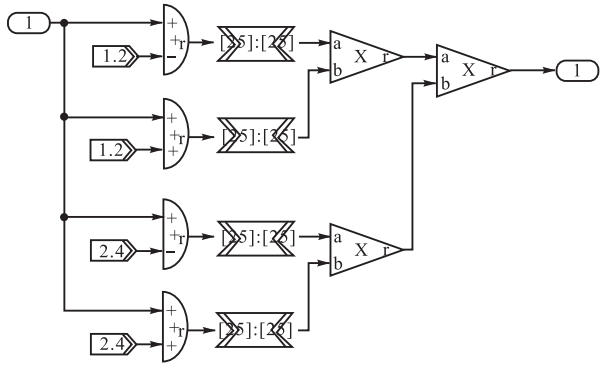

图 8　子模块 1 的电路模型

Fig. 8　Circuit model for the subsystem 1

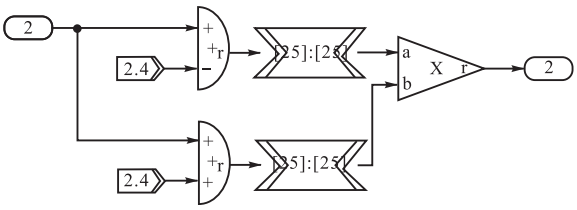

图 9　子模块 2、3 的电路模型

Fig. 9　Circuit model for the subsystems 2 and 3

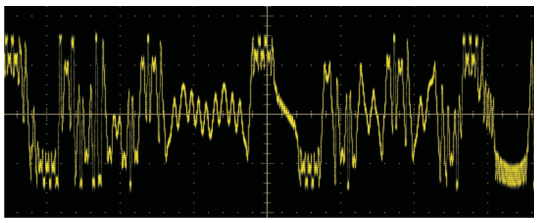

图 10　通过示波器观察到的波形图

Fig. 10　Oscillogram observed by an oscilloscope

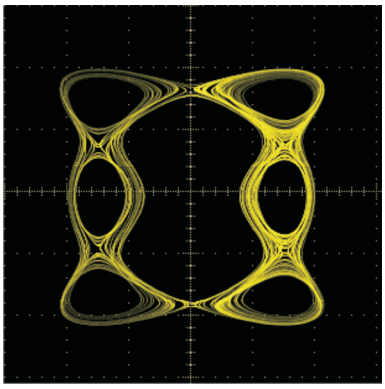

图 11　通过示波器观察到的相轨迹图

Fig. 11　Phase trajectory diagram observed by an oscilloscope

4　结　语

本文提出一种保守混沌系统模型，该系统具有很好的遍历性与伪随机性，同时满足哈密顿能量守恒与体积守恒。通过 NIST 测试验证了该系统能够产生符合 3 个标准条件的伪随机信号。利用 FPGA 技术设计了实现该系统的混沌电路，观察实验结果与数值仿真结果完全相同。本研究为混沌系统应用研究提供了一种新的保守混沌系统模型及伪随机信号发生器，进一步丰富了基于保守混沌系统的伪随机信号发生器的种类。

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] 王庆飞. 非线性物理的研究现状与展望[J]. 安阳工学院学报，2007(1)：120–122.

[3] CANG S J，WU A G，WANG Z H，et al. On a 3-D generalized Hamiltonian model with conservative and dissipative chaotic flows[J]. Chaos，solitons & fractals，2017，99：45–51.

[4] SUN F Y，LÜ Z W. Digital image encryption with chaotic map lattices[J]. Chinese physics B，2011，20(4)：040506.

[5] 张错玲，韦良芬. 基于 Lorenz 超混沌理论的数字图像加密算法研究[J]. 湖北大学学报(自然科学版)，2016，38(6)：551–556.

[6] 谢红梅，夏磊，朱孟元，等. 基于 Logistic 混沌映射的图像加密系统及 FPGA 实现[J]. 航空兵器，2016(2)：56–60.

[7] GAO T G，CHEN Z Q. A new image encryption algorithm based on hyper-chaos[J]. Physics letters A，2008，372(4)：394–400.

[8] YE G D. Image scrambling encryption algorithm of pixel bit based on chaos map[J]. Pattern recognition letters，2010，31(5)：347–354.

[9] ZHU Z L，ZHANG W，WONG K W，et al. A chaos-based symmetric image encryption scheme using a bit-level permutation[J]. Information sciences，2011，181(6)：1171–1186.

[10] MIRZAEI O，YAGHOOBI M，IRANI H. A new image encryption method：parallel sub-image encryption with hyper chaos[J]. Nonlinear dynamics，2012，67(1)：557–566.

[11] BELAZI A, EL-LATIF A A A, BELGHITH S. A novel image encryption scheme based on substitution-permutation network and chaos[J]. Signal processing, 2016, 128: 155–170.

[12] SILVA-GARCÍA V M, FLORES-CARAPIA R, RENTERÍA-MÁRQUEZ C, et al. Substitution box generation using chaos: an image encryption application[J]. Applied mathematics and computation, 2018, 332: 123–135.

[13] TANG H, SUN Q T, YANG X, et al. A network coding and DES based dynamic encryption scheme for moving target defense[J]. IEEE Access, 2018, 6: 26059–26068.

[14] LIN H R, WANG C H. Influences of electromagnetic radiation distribution on chaotic dynamics of a neural network[J]. Applied mathematics and computation, 2020, 369: 124840.

[15] ZHAO Q, WANG C H, ZHANG X. A universal emulator for memristor, memcapacitor, and meminductor and its chaotic circuit[J]. Chaos: an interdisciplinary journal of nonlinear science, 2019, 29(1): 013141.

[16] ZHANG X, WANG C H. Multiscroll hyperchaotic system with hidden attractors and its circuit implementation[J]. International journal of bifurcation and chaos, 2019, 29(9): 1950117.

[17] 徐沛帆. 随机性测试方法实现与应用[D]. 成都: 电子科技大学, 2019.

[18] YU S M, LU J H, LEUNG H, et al. Design and implementation of n-scroll chaotic attractors from a general jerk circuit[J]. IEEE Transactions on circuits and systems Ⅰ: regular papers, 2005, 52(7): 1459–1476.

[19] LIU C X, YI J, XI X C, et al. Research on the multi-scroll chaos generation based on Jerk mode[J]. Procedia engineering, 2012, 29: 957–961.

[20] YU S M, LÜ J H, CHEN G R, et al. Design and implementation of grid multiwing butterfly chaotic attractors from a piecewise Lorenz system[J]. IEEE Transactions on circuits and systems Ⅱ: express briefs, 2010, 57(10): 803–807.

[21] YU F, LIU L, HE B Y, et al. Analysis and FPGA realization of a novel 5D hyperchaotic four-wing memristive system, active control synchronization, and secure communication application[J]. Complexity, 2019, 2019: 1–18.

[22] PASINI A, PELINO V. A unified view of Kolmogorov and Lorenz systems[J]. Physics letters A, 2000, 275(5/6): 435–446.

[23] YANG F M, HUANG W H, SHUI G H, et al. A pseudo-random signal generator for offset calibration circuit[J]. Journal of physics: conference series, 2022, 2356(1): 012013.

[24] 贾红艳, 陈忠告, 石文欣, 等. 一个具有多稳定流的广义 Hamiltonian 保守混沌系统[J]. 山东大学学报(工学版), 2022, 52(2): 74–79.

[25] PEREZ J C N, VALDEZ M A E, ADEYEMI V A, et al. FPGA board implementation of two Hamiltonian conservative chaotic systems[C]// Proceedings of 2021 IEEE International Conference on Engineering Veracruz (ICEV). Veracruz: IEEE, 2021.

[26] DHAMALA M, LAI Y C, KOSTELICH E J. Analyses of transient chaotic time series[J]. Physical review E, 2001, 64(5): 056207.

[27] ZHANG X, WANG C H, YAO W, et al. Chaotic system with bondorbital attractors[J]. Nonlinear dynamics, 2019, 97(4): 2159–2174.

[28] DENG Q L, WANG C H. Multi-scroll hidden attractors with two stable equilibrium points[J]. Chaos: an interdisciplinary journal of nonlinear science, 2019, 29(9): 093112.

[29] 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(自然科学版), 2010, 34(2): 165–169.

[30] 王思淼, 杜宝祥, 彭琪琪. 基于位平面和保守混沌系统的图像加密算法[J]. 黑龙江大学自然科学学报, 2022, 39(5): 613–620.

责任编辑: 周建军