

引用格式: 周 围, 吴周青. 一个新的超大范围超混沌系统分析与 FPGA 实现 [J]. 微电子学与计算机, 2019, 36(8): 49-53.
[ZHOU W, WU Z Q. Analysis and FPGA implementation of a novel super-wide range hyperchaotic system [J]. Microelectron-
ics & Computer, 2019, 36(8): 49-53.]

一个新的超大范围超混沌系统分析与 FPGA 实现

周 围, 吴周青

(重庆邮电大学 光电工程学院/国际半导体学院, 重庆 400065)

摘 要: 超混沌系统与混沌系统相比动力学特性更加复杂, 但是目前大多数超混沌系统参数范围较小, 提供的密钥空间较小, 而且在系统参数发生改变时系统容易跳出混沌状态. 针对这个问题, 本文提出了一个新的超大范围超混沌系统. 该系统在参数 c 属于 $[1, 10^7]$ 时都表现为超混沌状态. 理论分析了新系统的基本动力学行为, 包括系统相图、平衡点、Lyapunov 指数谱和分岔图. 本文进一步用 FPGA 实现了该混沌系统, 给出了系统参数 c 分别为 5、100、1000 和 10^5 时, 在示波器上捕捉到的 x - z 相轨迹图, 验证了该超大范围超混沌系统的 FPGA 可实现性.

关键词: 超混沌; 超大范围; 动力学分析; 现场可编程门阵列 (FPGA)

中图分类号: TN273

文献标识码: A

文章编号: 1000-7180(2019)08-0049-05

Analysis and FPGA implementation of a novel super-wide range hyperchaotic system

ZHOU Wei, WU Zhou-qing

(College of Electronics Engineering / International Semiconductor College, Chongqing University of
Posts and Telecommunications, Chongqing 400065, China)

Abstract: The hyperchaotic system has more complex dynamic characteristics than the chaotic system. However, most hyperchaotic systems currently have a small parameter range and provide a small key space, and the system easily jumps out of the chaotic state when the system parameters change. Aiming at this problem, a novel super-wide range hyperchaotic system is proposed in this paper. The system is hyperchaotic when the parameter c is $[1, 10^7]$. The basic dynamics behaviors of the novel system are analyzed theoretically, including system phase diagrams, equilibrium points, Lyapunov exponent spectrums and bifurcation diagrams. In this paper, the chaotic system is implemented by FPGA, and the x - z phase trajectories captured on the oscilloscope are given when the system parameters c are 5, 100, 1000 and 10^5 respectively, verified the FPGA achievability of the super-wide range hyperchaotic system.

Key words: hyperchaotic; super-wide range; dynamic analysis; field programmable gate array (FPGA)

1 引言

混沌是确定的非线性系统产生的伪随机现象, 是非线性系统中所特有的一种运动形式; 由于混沌具有伪随机性、对初始条件敏感等特性, 且可以控制

和同步, 使得它在保密通信、密码学等领域有着广泛的应用前景^[1]. 超混沌系统由于具有两个或两个以上正的 Lyapunov 指数, 使其相轨在更多方向扩展, 从而形成比混沌系统更复杂的动态行为, 因此受到国内外学者的广泛关注与研究. 但目前大多数超混

沌系统的参数的范围不够大,如文献[2]中系统处于超混沌系统状态的参数为 $\delta \in [0.95, 1]$, 文献[3]中参数的范围为 $\alpha \in [0.4, 1.2]$. 这些系统在实际应用中,当参数发生微小变化时,很容易跳出混沌状态,变为周期或伪周期状态,加大了工程应用的难度;而具有超大范围超混沌特性的系统,在某个参数变动时始终处于超混沌状态,其始终至少有两个大于零的 Lyapunov 指数,这使得该系统具有更丰富的动力学特性,在保密通信^[4,5],混沌雷达^[6]等领域具有更大的优势. 但总的来说,关于超大范围超混沌系统的研究还处于起步阶段,文献[5]基于忆阻器构建了一个四维的超大范围混沌系统,参数范围为 $p \in (0, 10^6]$;文献[7]构建了一个新的超大范围超混沌系统,参数范围为 $k \in [0, 10^5]$.

电路实现是混沌系统应用的前提,目前的实现方法主要有两种,一种是模拟电路,另一种是数字电路. 模拟电路由于易受环境、器件老化等影响且电路参数离散性较大、通用性差,从而限制了它的实际应用^[8]. 而数字电路可以很好的解决模拟电路的这些问题. 随着数字化技术的发展,FPGA 具有速度快、并行处理等特性,因此混沌系统越来越多的使用 FPGA 技术实现^[9,10]. 但是超大范围超混沌系统的 FPGA 实现还非常少,文献[4]和文献[5]都只是给出模拟电路的实现.

基于上述研究,本文提出了一个新的超大范围超混沌系统,其参数范围比本文提到的其他系统都要大,而且该系统在参数 $c \in [1, 5000]$ 时,系统的最大 Lyapunov 指数逐渐增加,系统的动态特性逐渐变得复杂;在参数 $c \in [5000, 10^7]$ 时,系统 Lyapunov 指数保持恒定,表现为恒 Lyapunov 指数特性. 同时分析了参数 a 和 b 对系统的影响,发现在参数 a 或 b 变化时,系统在周期、伪周期、混沌和超混沌之间切换,系统表现出丰富的动态特性. 在此基础上重点分析了所构建的超大范围超混沌系统的动力学特性和 FPGA 数字电路实现.

2 超大范围超混沌系统

新的超大范围超混沌系统的数学模型为

$$\begin{cases} \dot{x} = yz - ax \\ \dot{y} = xz - y^3 - zw \\ \dot{z} = -4xy + bz \\ \dot{w} = cx \end{cases} \tag{1}$$

式中 x, y, z, w 为系统状态变量; a, b, c 为系统参数. 当 $a = 8, b = 7, c = 5$, 初始值为 $[1, 3, 1, 2]$ 时,四个 Lyapunov 指数分别为: $LE_1 = 1.630\ 6, LE_2 = 0.888\ 2, LE_3 = -0.002\ 3, LE_4 = -72.606\ 2$, 此时系统产生四翼超混沌吸引子,系统相图如图 1 所示.

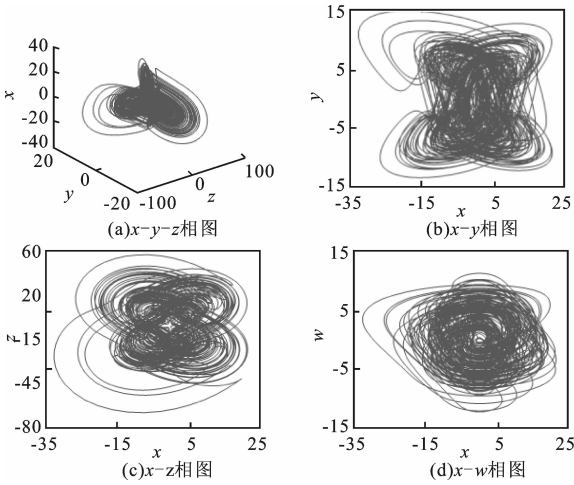


图 1 系统相图

3 基本动力学特性

3.1 耗散性及吸引子的存在性

根据系统(1),有

$$\nabla V = \frac{\partial \dot{x}}{\partial x} + \frac{\partial \dot{y}}{\partial y} + \frac{\partial \dot{z}}{\partial z} + \frac{\partial \dot{w}}{\partial w} = b - a - 3y^2 \tag{2}$$

当 $a = 8, b = 7$ 时, $\nabla V = -1 - 3y^2 < 0$, 此时系统是耗散的;系统的轨迹最终被限制在一个体积为 0 的集合上,渐进动力学行为被固定在一个吸引子上,说明了吸引子的存在性.

3.2 平衡点及稳定性

令系统的 $\dot{x} = \dot{y} = \dot{z} = \dot{w} = 0$, 可得:

$$\begin{cases} 0 = yz - ax \\ 0 = xz - y^3 - zw \\ 0 = -4xy + bz \\ 0 = cx \end{cases} \tag{3}$$

解方程(3),得到系统仅有一个平衡点,
 $S = (0, 0, 0, 0)$.

在平衡点 S 处线性化系统(1),得其 Jacobian 矩阵为:

$$J = \begin{bmatrix} -a & z & y & 0 \\ z & -3y^2 & x-w & -z \\ -4y & -4x & b & 0 \\ c & 0 & 0 & 0 \end{bmatrix} \tag{4}$$

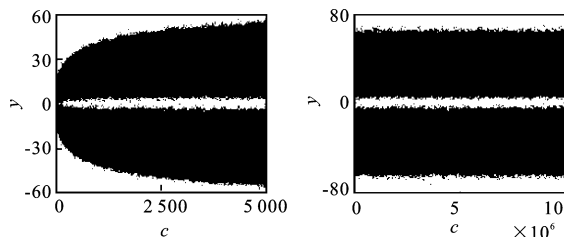
对于上式,当 $a = 8, b = 7$, 并将平衡点 S 代入,

可以求得该 Jacobian 矩阵的特征值为 $\lambda_1 = 0, \lambda_2 = -8, \lambda_3 = 0, \lambda_4 = 7$. 根据 Routh-Hurwitz 条件, 可得该平衡点是不稳定平衡点.

3.3 Lyapunov 指数谱和分岔图

当混沌系统的参数发生改变时, 系统的运动状态会随之变化. 一般用分岔图分析系统某个参数变化时系统状态的运动变化情况. Lyapunov 指数虽然是为了定量刻画混沌系统对初值的敏感性而提出来的, 但是由于仅从分岔图很难区分混沌系统与超混沌系统, 所以 Lyapunov 指数还被应用于判断系统是否为超混沌系统. 对于一个四维连续自治的系统, 在它的四个 Lyapunov 指数中, 当最大的 Lyapunov 指数为零, 其他三个为负时, 系统是周期的; 当两个最大的 Lyapunov 指数都为零, 另外两个为负时, 系统是伪周期的; 当最大 Lyapunov 指数为正, 次大 Lyapunov 指数为零, 另外两个 Lyapunov 指数为负时, 系统为混沌的; 当有两个 Lyapunov 指数大于零, 另外两个 Lyapunov 指数一个为零, 一个为负时, 系统为超混沌的^[6]. 下面的分析会根据这些规则判断参数变化时系统的状态, 并且由于系统(1)的最小 Lyapunov 指数远小于零, 所以未将其画出.

当 $a=8, b=7$, 初始值为 $[1, 3, 1, 2]$ 时; 分析系统随着参数 c 变化, 系统状态变量 y 的动力学变化特性仿真结果如图 2 所示. 图 2(a) 是 $c \in [1, 5000]$ 时的分岔图, 图 2(b) 是 $c \in [5000, 10^7]$ 时的分岔图.



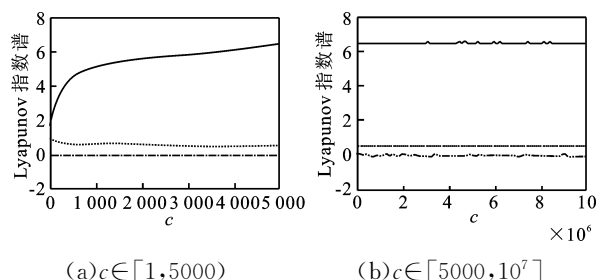
(a) $c \in [1, 5000]$ (b) $c \in [5000, 10^7]$

图 2 系统随 c 变化的 y - c 分岔图 ($a=8, b=7$)

图 3 为系统随参数 c 变化的 Lyapunov 指数谱. 由图 3 可知, 在 $c \in [1, 10^7]$ 时, 有两个大于 0 的 Lyapunov 指数, 一个接近 0 的 Lyapunov 指数和一个远小于 0 的 Lyapunov 指数, 所以该系统在这个超大范围内都是超混沌的. 在 $c \in [1, 5000]$ 时, 最大 Lyapunov 指数随着 c 增大而增大, 第二大 Lyapunov 指数则逐渐减小到 0.5; 在 $c \in [5000, 10^7]$ 时, 四个 Lyapunov 指数不变, 表现出恒 Lyapunov 指数特性.

通过上面的分析, 可以看出随参数变化时, 系统

(1) 在周期、伪周期、混沌和超混沌之间切换, 表现出非常丰富的动力学特性, 而且可以看出系统的 Lyapunov 指数比较大, 两个最大的 Lyapunov 指数可能都大于 2, 具有更加复杂的动力学特性. 所以该系统不仅在超大范围内表现为超混沌特性, 而且动力学特性更加复杂, 使其应用于保密通信时具有更高的安全性.



(a) $c \in [1, 5000]$ (b) $c \in [5000, 10^7]$

图 3 系统随 c 变化的 Lyapunov 指数谱 ($a=8, b=7$)

4 结果分析与讨论

基于 FPGA 技术, 并采用定点数的方法, 对超混沌系统进行硬件实验, 主要元器件包括, Xilinx 型号为 xc7z020clg400 的 FPGA 开发板、型号为 AD9767 的双口并行最高转换速率为 125 MHz 的 D/A 转换器. 软件是 Vivado 2016.4, 编程语言为 verilog 硬件编程语言.

由于 FPGA 是数字处理技术, 不能处理连续系统, 所以必须对混沌系统进行离散化处理. 常用的离散化算法有三种, 分别是龙格-库塔法、改进的欧拉法和欧拉法. 其中龙格-库塔法和改进的欧拉法计算精度较高, 但是迭代次数较多, 消耗的硬件资源和输出时延较大, 实现相对复杂. 而欧拉法精度虽然稍低, 但是只需要迭代一次, 硬件资源消耗和输出延时都较小, 实现也较容易, 所以综合考虑本文用欧拉法对混沌系统进行离散化. 欧拉算法的数学公式如式(5)所示:

$$\frac{dx_i}{dt} = \lim_{h \rightarrow 0} \frac{[x_i(n+1) - x_i(n)]}{h} \quad (5)$$

根据式(5), 将混沌系统离散化为式(6):

$$\begin{cases} x(n+1) = x(n) + [y(n)z(n) - ax(n)]h, \\ y(n+1) = y(n) + [x(n)z(n) - y(n)^3 - z(n)w(n)]h, \\ z(n+1) = z(n) + [bz(n) - 4x(n)y(n)]h, \\ w(n+1) = w(n) + [cx(n)]h. \end{cases} \quad (6)$$

式中, h 是步长, $h = 1/2^{12}$.

利用 FPGA 对式(6)进行硬件设计如图 4 所示.

图 4 中,“/”表示线宽为 35 位,“+”表示有符号定点数的加减运算模块,“-”表示进行减法运算,“ $\times$ ”表示有符号定点数乘法运算模块,“ $\gg$ ”表示右移,“||”表示截位. 定点数乘法的计算不同于浮点数,乘积的位宽是两个乘数位宽之和,所以为了进行下一步运算需要对结果进行截位. 由式(6)可知,乘积需要与步长 h 相乘,也即是乘积除以 $1/h$,而 $1/h$ 为 2^{12} ,在 FPGA 里可以右移 12 位实现. 由于超混沌系统的参数 c 的取值范围太大,先计算 $cx(n)$,计算结果会超出本文定点数的表示范围,为了解决这个问题,调整 $cx(n)h$ 的计算顺序为 $chx(n)$.

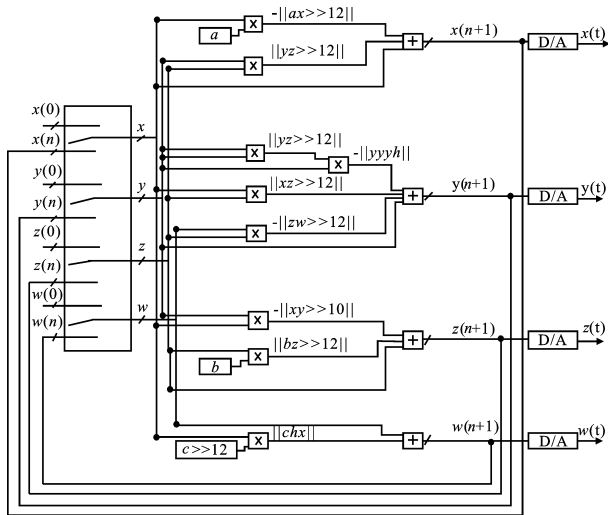


图 4 超混沌系统 FPGA 结构图

系统的顶层模块如图 5 所示,主要包括混沌系统模块、按键模块、数据输出选择模块和数模转换模块. 各个模块的功能分别是,混沌系统模块主要是通过状态机及图 4 所示的结构图实现混沌系统;按键模块用于控制混沌系统状态各个相的输出,从而丰富混沌系统的输出,增加系统的复杂性从而提高其在保密通信中应用的安全性;数据输出选择模块是根据按键的键值控制混沌系统各个相的输出;数模转换模块是将数字信号转化为模拟信号.

根据图 4 和图 5,编写程序. 编译通过后,将生成的 bit 文件下载到 FPGA 中,通过 D/A 转换器,获得连续信号. 在参数 $a=8$ 和 $b=7$ 固定不变, c 分别取 5、100、1000 和 10^5 时,其 FPGA 在型号为 DPO4102B-L 示波器上输出的 x - z 相图如图 6 所示.

5 结束语

本文构造了一个超大范围超混沌系统,分析了

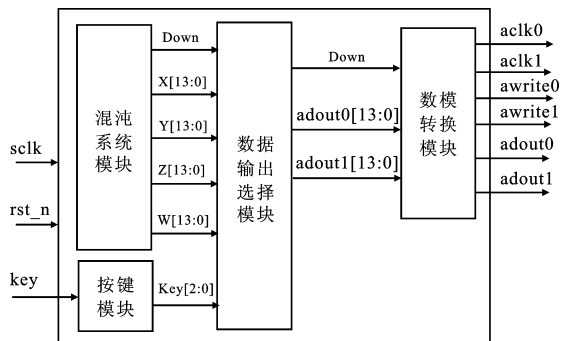


图 5 超混沌系统顶层模块结构图

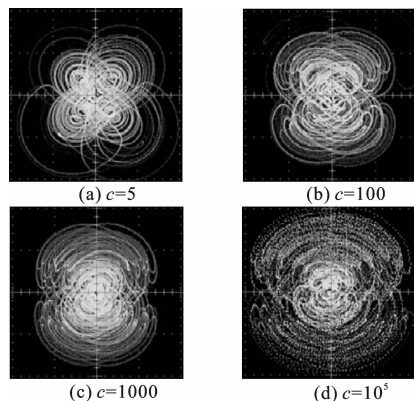


图 6 系统 FPGA 实现的示波器捕捉的 x - z 相图

系统的耗散性和平衡点,并对系统的 Lyapunov 指数谱、分岔图进行了数值仿真. 根据数据结果发现该系统有三大特点,一是系统能在参数 $c \in [1, 10^7]$ 时始终保持超混沌特性;二是系统在参数 $c \in [5000, 10^7]$ 时 Lyapunov 指数保持恒定,表现为恒 Lyapunov 指数特性;三是由于系统的 Lyapunov 指数较大,所以该系统的动力学特性更加复杂. 由于具有这三大特点,使其应用于保密通信时具有更高的安全性. 最后,用 FPGA 采用定点数的方式实现了此超大范围超混沌系统,为其在实际工程中的应用奠定了基础.

参考文献:

- [1] LIU Z, ZHANG L, RAO W, et al. Demonstrating high security subcarrier shifting chaotic OFDM cognitive radio system using USRP[C]// IEEE/CIC International Conference on Communications in China. IEEE, 2017:1-6.
- [2] JEEVAREKHA A, SABARATHINAM S, THAMILMARAN K, et al. Analysis of 4D autonomous system with volume-expanding phase space[J]. Nonlinear Dynamics, 2016, 84(4):1-12.
- [3] VOLOS C, MAAITA J O, VAIDYANATHAN S, et

- al. A Novel Four-Dimensional Hyperchaotic Four-Wing System With a Saddle-Focus Equilibrium[J]. IEEE Transactions on Circuits & Systems II Express Briefs, 2017, 64(3):339-343.
- [4] XUE H W, DU J, LI S L, et al. Region of interest encryption for color images based on a hyperchaotic system with three positive Lyapunov exponents[J]. Science Direct, 2018, 106(1):506-516.
- [5] WANG Z, SUN C, JIN F, et al. A widely amplitude-adjustable chaotic oscillator based on a physical model of HP memristor[J]. IEICE Electronics Express, 2018, 15(8):1-6.
- [6] ZENG T, CHANG S Q, FAN H Y, et al. Design and processing of a novel chaos-based stepped frequency synthesized wideband radar signal[J]. Sensors, 2018, 18(4):1-23.
- [7] 梅蓉, 陈谋. 一类超大范围超混沌系统的动力学分析和电路实现[J]. 工程科学与技术, 2012, 44(5): 171-175.
- [8] ZHONG G, MAN K F, CHEN G R. A systematic approach to generating n-scroll attractors [J]. International Journal of Bifurcation & Chaos, 2002, 12(12):2907-2915.
- [9] TLELO-CAUTLE E, PANO-AZUCENA A D, RANGEL-MAGDALENO J J, et al. Generating a 50-scroll chaotic attractor at 66 MHz by using FPGAs [J]. Nonlinear Dynamics, 2016, 85(4):1-15.
- [10] LAI Q, ZHAO X W, RAJAGOPAL K, et al. Dynamic analyses, FPGA implementation and engineering applications of multi-butterfly chaotic attractors generated from generalised Sprott C system[J]. Pramana, 2018, 90(1):6-17.

作者简介:

周 围 男, (1971-), 博士, 教授. 研究方向为电路与系统、通信系统及信号处理等.

吴周青(通讯作者) 男, (1991-), 硕士研究生. 研究方向为混沌理论及其应用研究. E-mail: cejin@foxmail.com

(上接第 48 页)

- [4] CHEN L, MITRA T. Graph minor approach for application mapping on CGRAs[C]//2012 International Conference on Field-Programmable Technology. Seoul: IEEE, 2012: 285-292.
- [5] HAMZEH M, SHRIVASTAVA A, VRUDHULA S. EPIMap: Using epimorphism to map applications on CGRAs[C]// DAC Design Automation Conference 2012. San Francisco: IEEE, 2012: 1280-1287.
- [6] HAMZEH M, SHRIVASTAVA A, VRUDHULA S. REGIMap: register-aware application mapping on coarse-grained reconfigurable architectures (CGRAs) [C]//Proceedings of the 50th Annual Design Automation Conference. Austin: ACM, 2013: 18.
- [7] DAVE S, BALASUBRAMANIAN M, SHRIVASTAVA A. RAMP: resource-aware mapping for CGRAs[C]//2018 55th ACM/ESDA/IEEE Design Automation Conference (DAC). San Francisco: IEEE, 2018: 1-6.
- [8] ZHAO Z, SHENG W, JING N, et al. Resource-saving compile flow for coarse-grained reconfigurable architectures [C]//2015 International Conference on ReConFigurable Computing and FPGAs (ReConFig). Cancun: IEEE, 2015: 1-8.
- [9] LEVI G. A note on the derivation of maximal common subgraphs of two directed or undirected graphs[J]. Calcolo, 1973, 9(4): 341-352.
- [10] RAU B R. Iterative module scheduling: An algorithm for software pipelining loops[C]//The 27th Annual IEEE/ACM International Symposium on Microarchitecture. San Jose: IEEE, 1994: 63-74.

作者简介:

尹文志 男, (1994-), 硕士研究生. 研究方向为粗粒度可重构处理器编译器后端技术. E-mail: mrwensim@sjtu.edu.cn

赵仲元 男, (1989-), 博士研究生. 研究方向为可重构计算的编译架构.

毛志刚 男, (1962-), 教授. 研究方向为可重构硬件结构设计技术研究.

王 琴 女, (1975-), 副教授. 研究方向为大规模集成电路设计、先进集成电路设计方法.

绳伟光 男, (1977-), 助理研究员. 研究方向为高可靠集成电路设计.