基于 FPGA 技术的混沌系统设计与实现

李登辉,闵富红,马美玲

(南京师范大学电气与自动化工程学院,江苏 南京 210042)

[**摘要**] 以经典的 Lorenz 系统为研究对象,利用 FPGA 数字信号处理技术实现 Lorenz 混沌系统,减少了外界因素的干扰. 首先,对 Lorenz 连续系统的方程进行分解,得到离散化状态方程,接着基于 DSP-Builder 软件开发平台获得系统的电路模型,该模型可直接转化为 VHDL 语言;其次,采用硬件描述语言(Verilog HDL)直接编程的形式,对系统进行验证,并从示波器中观测到 Lorenz 系统的混沌波形. 通过比较上述 2 种实现混沌系统的方法,总结其优缺点及适用范围,为进一步利用 FPGA 实现一类非线性系统及相关领域的研究提供实用的方法.

[**关键词**] 混沌系统,FPGA,Verilog HDL,DSP-Builder

[**中图分类号**]TP391.3　[**文献标志码**]A　[**文章编号**]1672-1292(2015)01-0008-07

The Design and Implementation of Chaotic System Based on FPGA Technology

Li Denghui,Min Fuhong,Ma Meiling

(School of Electrical and Automation Engineering,Nanjing Normal University,Nanjing 210042,China)

Abstract:In this paper,the chaotic Lorenz system is carried out through FPGA technology,which can decrease the deviation from the expected effect. Firstly,the differential equation is decomposed in discretized equation,and then the circuit model by DSP-Builder software platform is obtained,which can be translated directly into the VHDL language. Secondly, Lorenz system is tested through the program in hardware description languages,i. e. Verilog HDL. By analyzing the simulation results of the above two methods,the advantages and disadvantages are summarized,respectively. These results provides a reference method to achieve the research in nonlinear system by using FPGA.

Key words:chaotic system,FPGA,Verilog HDL,DSP-Builder

混沌作为一种复杂的非线性运动行为,具有对初始值极为敏感和类似噪声等特点,已被广泛应用于生物学、工程学和信息学等领域[1-3]. 近年来,随着数字信号处理技术的兴起,各领域对数字混沌信号的需求逐渐增加,传统的模拟电子硬件电路虽设计简便且易实现,但极易受到外界物理因素的影响,如温度、焊接老化和通电时间,已不能满足现代处理器的快速性和稳定性要求. 解决该问题的主要途径之一是对连续混沌系统进行离散化,并利用先进性的数字信号处理技术进行混沌系统的数字实现.

现场可编程门阵列(FPGA)是一种具有大容量、高密度和高可靠性等特点的数字信号处理技术,在设计复杂数字硬件系统方面具有极大的优越性,在现代数字系统中应用广泛. 利用 FPGA 技术实现连续混沌系统以及相关应用,目前已经有一定的研究成果[4-12]. 归纳起来,主要有两种处理方法:一种是利用硬件描述语言对混沌系统进行描述[6-9],得到系统状态变量的混沌序列;另一种是在 Matlab/Simulink 环境下,基于 DSP-Builder 软件开发平台,将离散化的混沌系统模型转换成 HDL 语言输出[10-12],最终借助 Altera 公司的 Quartus 9.0 软件将代码导入 FPGA 开发板. 前者编写困难,但具有通用型和可移植性;后者设计方法简单,但产生的混沌信号不能被其他模块直接调用,不利于后续的同步和保密通信的处理. 两种方法各有利弊,针对具体的混沌系统,应采用何种方法进行数字信号的处理才能获得更好的效果,目前还没有文献

收稿日期:2014-09-21.

基金项目:国家自然科学基金(51475246)、江苏省自然科学基金(BK20131402)、教育部留学回国人员科研启动基金(教育司[2012]1707号)和江苏省六大人才高峰资助课题.

通讯联系人:闵富红,博士,副教授,研究方向:非线性电路分析与控制. E-mail:minfuhong@ njnu.edu.cn

给出明确的对比和选择方案.

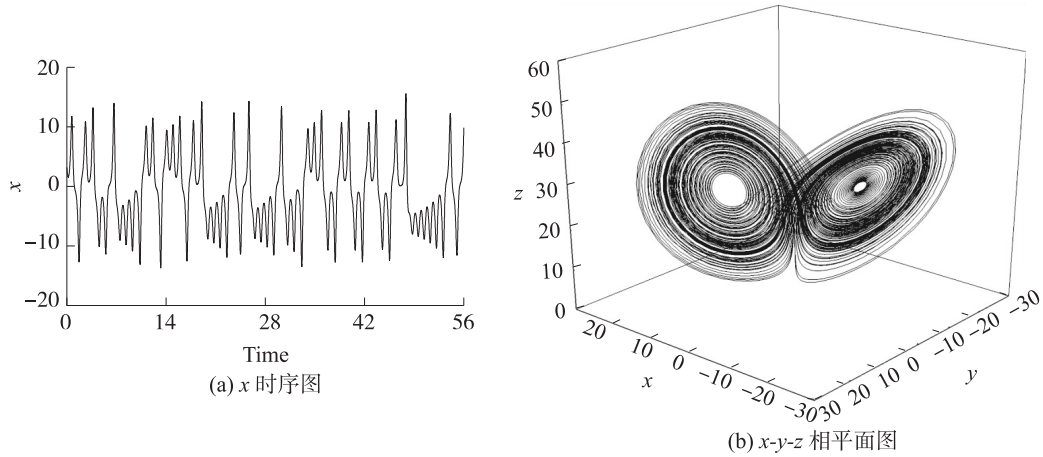
本文以 Lorenz 系统为例,分别采用 DSP-Builder 模型建立和硬件描述语言直接描述两种方法来实现系统的离散化设计,并下载到 FPGA 硬件电路板上,利用示波器观察输出图形,其结果与仿真一致;并从资源占用的角度详细比较了两种方法的优缺点,总结了各自的适用范围,为今后利用 FPGA 实现非线性系统及相关领域的研究提供可参考的方法.

1 Lorenz 系统

Lorenz 混沌吸引子是 20 世纪 60 年代美国气象学家洛伦兹[13]在对大气环流的研究中首次发现的,其经典的连续动力学特性,无论是从数学还是物理的角度都值得研究. 其系统方程如下所示:

$$\begin{cases}\dot{x}=a(y-x),\\ \dot{y}=cx-y-xz,\\ \dot{z}=xy-bz.\end{cases} \tag{1}$$

当取不同参数和初始值时会得到不同的运动状态. 这里取系统参数 $a=10,b=8/3,c=28$,初始值取 $x_0=0.1,y_0=0.1,z_0=0.15$,得到仿真图形如图 1 所示.



(a) x 时序图　　(b) x-y-z 相平面图

图 1　Lorenz 系统仿真图形

Fig. 1　Simulation results for Lorenz system

2 Lorenz 系统的数字实现

随着数字混沌信号在各个领域中的广泛应用,学者们开始相继利用各种数字信号处理技术实现混沌系统的数字化,其中以 FPGA 技术居多. 目前利用 FPGA 技术实现混沌系统的数字化主要有利用 DSP-Builder 开发平台和硬件描述语言两种方法实现.

2.1 基于 DSP-Builder 开发平台混沌电路的实现

采用 Altera 公司和 Mathworks 公司共同合作开发的 1 款设计工具软件(DSP-Builder),通过该工具可以将设计的系统模型转化成为 1 个基于 FPGA 技术的工程文件.

首先,根据微分方程定义,对 Lorenz 系统进行离散化. 通常微分方程可表示为:

$$\frac{\mathrm{d}x_i}{\mathrm{d}t}=f(x_1,x_2,\cdots,x_n)=\lim_{\tau\to 0}\frac{x_{i(n+1)}-x_{i(n)}}{\tau}. \tag{2}$$

式中,τ 为采样时间. 设采样频率 $f_s=1/\tau$,式(1)可变形为:

$$x_{i(n+1)}=\frac{f(x_1,x_2,\cdots x_n)}{f_s}+x_{i(n)}. \tag{3}$$

利用式(3)对 Lorenz 系统(1)进行离散化处理,取系统参数 $a=10,b=8/3,c=28$ 得到如下模型:

$$\begin{cases} x(k+1)=(1-9\Delta t)x(k)+9\Delta t\cdot y(k), \\ y(k+1)=35\Delta t\cdot x(k)+(1-\Delta t)y(k)-20\Delta t\cdot x(k)z(k), \\ z(k+1)=(1-1.5\Delta t)z(k)+5\Delta t\cdot x(k)y(k). \end{cases} \tag{4}$$

采样频率选择 100 Hz,因此,$\Delta t=0.01$ s,代入式(4)可得到离散化模型:

$$\begin{cases} x(k+1)=0.91x(k)+0.09y(k), \\ y(k+1)=0.35x(k)+0.99y(k)-0.2x(k)z(k), \\ z(k+1)=0.985z(k)+0.05x(k)y(k). \end{cases} \tag{5}$$

其次,利用 DSP-Builder 开发平台实现 Lorenz 混沌系统. DSP-Builder 开发平台是依赖于数学分析工具 Matlab/Simulink,以 Simulink 的 Blockset 的形式出现,通过先在 Simulink 中进行图形化设计和仿真以实现系统的功能,而后经过 Signal Compiler 读取模型设计文件(. mdl)并将其转化成 Quartus Ⅱ 工程文件(.qpf),最后导入 Quartus Ⅱ 进行后续处理. 在使用 DSP Builder 工具箱进行系统设计时,只需说明设计完成的功能和相关的约束,而不必关心系统的实现方式. 它架构在多个软件工具之上,并把系统级(算法仿真建模)和 RTL 级(硬件实现)两个设计领域的设计工具联系起来,都放在 Matlab/Simulink 图形设计平台上,而将 Quartus Ⅱ 最为底层设计工具置于后台,省去了编写代码的繁琐,最大程度地发挥了其优势. 根据式(5)可搭建离散化模型如图 2 所示.

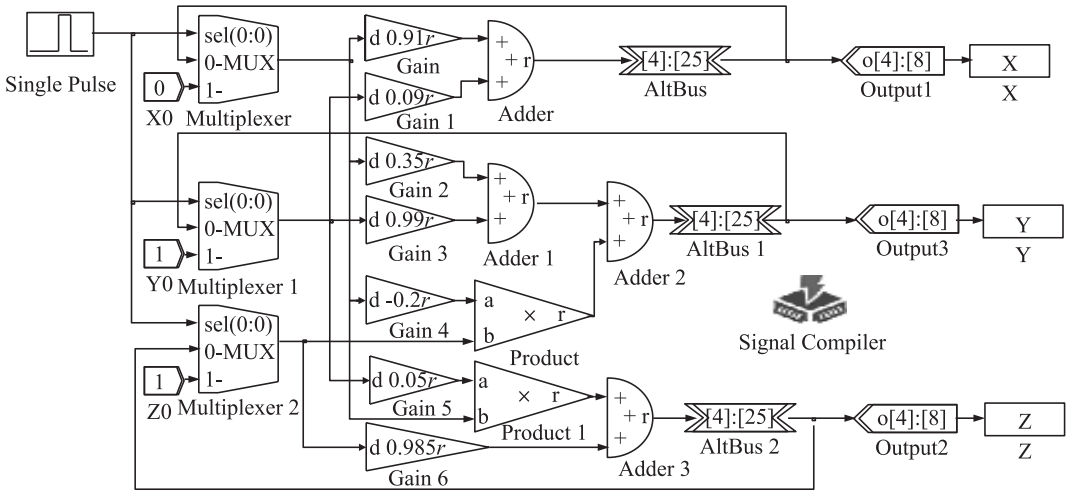
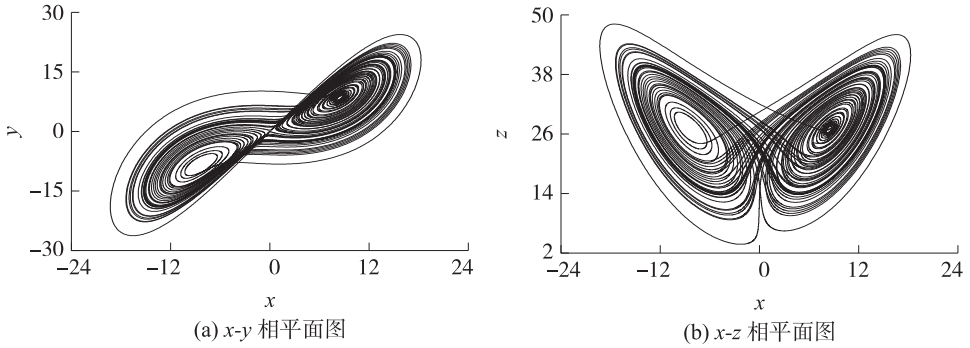


图 2　基于 DSP-Builder 开发平台 Lorenz 系统的实现

Fig. 2　Lorenz system based on DSP-Builder platform

由于 DSP-Builder 开发平台所处理的数据最终输出位是有限的,所以在乘法器模块要不断测试选取合适的有效位数,选取的有效位数必须同时满足输出精度的要求和占用资源最少两个方面. 最终选取乘法器模块整数部分为 4 位,小数部分为 25 位,输出模块考虑到实际的 D/A 转换是 12 位,在保证精度的前提下选取整数部分为 4 位,小数部分为 8 位.



(a) x-y 相平面图　　(b) x-z 相平面图

图 3　Lorenz 相轨迹

Fig. 3　The trajectories for Lorenz system

通过观察以上系统仿真图形验证了离散结果的正确性,利用 Signal Compiler 模块将模型转化成 Quartus Ⅱ工程文件(. qpf),并导入 Quartus Ⅱ软件进行仿真验证. 为了检测系统输出是否正确,利用示波器观测系统输出变量 x、y 和 z 的数字量为一系列不规律变化的“0”、“1”序列. 图 4 所示为随机选取的输出管脚分配情况,图中 0~1 序列杂乱无规则,对应了混沌系统的随机性,初步证明了代码编写的正确性.

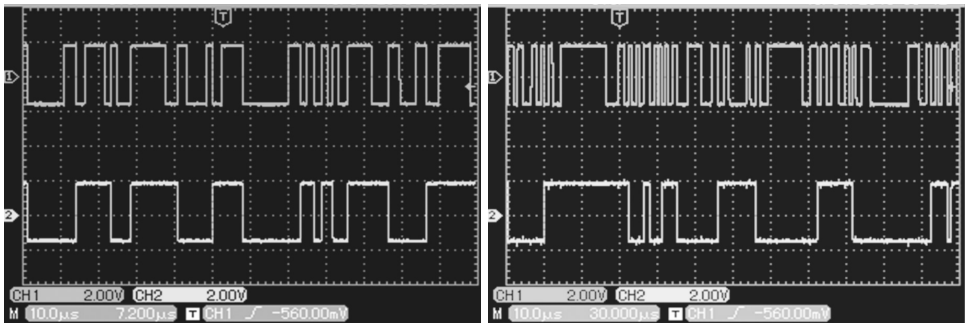


图 4　随机 2 组管脚的数字量输出

Fig. 4　Two groups of digital output at random

2.2　利用 Verilog HDL 语言混沌系统的实现

很多 FPGA 内部都有硬件乘法器资源,使用内部硬件乘法器可大幅度提高电路的运行速度. 由于受到数字系统字长的限制,在编写硬件描述语言时,根据国际电子电工学会制定的浮点标准格式,采用 32 位的定点数据,其中符号位 1 位,整数位 5 位,小数位 26 位. 由于这种格式小数点后有 26 位,也被称为 Q26 格式,其计算公式为 $x_1 = x \times 2^{26}$,取 x_1 的整数部分并转化为相应的二进制数. 则这 3 个初始值和系统参数 $a = 10$,$b = 8/3$,$c = 28$ 转化为浮点数格式后分别为:

$$\begin{cases} x_0 = 32'b0\_00000\_00011001100110011001100110(0.10), \\ y_0 = 32'b0\_00000\_00011001100110011001100110(0.10), \\ z_0 = 32'b0\_00000\_00100110011001100110011001(0.15), \\ a = 32'b0\_01010\_00000000000000000000000000(10), \\ b = 32'b0\_00010\_00100110011001100110011001(8/3), \\ c = 32'b0\_11100\_00000000000000000000000000(28). \end{cases}$$

龙格-库塔(Runge-Kutta)方法是一种在工程上应用广泛的高精度单步算法,具有精度高、收敛、稳定(在一定条件下)、计算过程中可以改变步长、不需要计算高阶导数等优点. 二阶龙格-库塔算法公式可表示为:

$$y_{n+1} = y_n + hf\left(x_n + \frac{h}{2}, y_n + \frac{h}{2} f(x_n, y_n)\right). \tag{6}$$

式中,h 为步长,$h = 1/128$.

根据式(6)利用状态机来描述多个电路模块,适当地把乘法运算分为几部分并行运行来提高计算的速度,在做变量相乘时为了防止变量取值的溢出,设计比例压缩系数 k,则压缩后式(1)可表示为:

$$\begin{cases} \dot{x} = 10k_1\left(\dfrac{y}{k_2} - \dfrac{x}{k_1}\right), \\ \dot{y} = 28\dfrac{k_2}{k_1}x - y - \dfrac{k_2}{k_1 k_3}xz, \\ \dot{z} = \dfrac{k_3}{k_1 k_2}xy - 8/3z. \end{cases} \tag{7}$$

取 $k_1 = k_2 = k_3 = 1/64$,即可保证变量取值不发生溢出,设计状态机流程图如图 5 所示.

根据图 5 编写 Lorenz 系统的 Verilog HDL 语言程序,将编写好的嵌套程序在 Quartus 软件中进行编译,编译无误后生成 RTL 电路如图 6 所示.

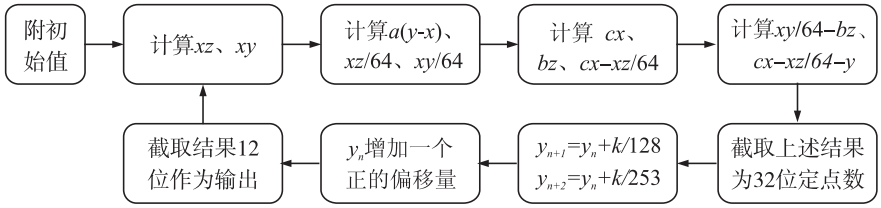


图 5　状态机描述

Fig. 5　The state machine description

在仿真和编译无误后,将程序通过 JTAG 接口烧写至 FPGA 开发板. 本文所使用的开发板芯片为 Altera 公司的飓风Ⅱ代 EP2C8Q208C8 芯片,芯片共有 208 个 I/O 口. 为了检测系统输出是否正确,利用示波器观测系统输出变量 x,y,z 的数字量为一系列不规律变化的“0”、“1”序列. 图 7 所示为随机选取的输出管脚分配情况,图中被选中的 2 组管脚对应的数字量输出情况如图 8 所示. 图 8 所输出的序列杂乱无规则,对应了混沌系统的随机性,初步证明了代码编写的正确性.

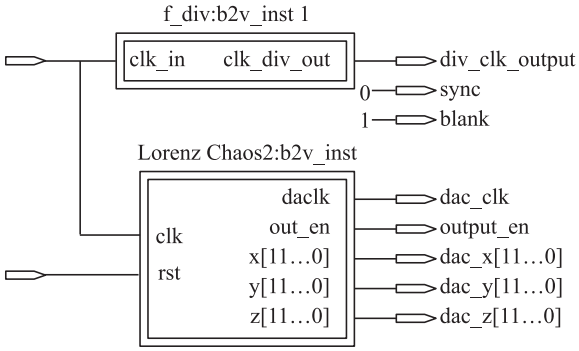


图 6　整体 RTL 电路

Fig. 6　The integral RTL circuit

由于 FPGA 开发板只能输出数字量,必须通过外接 D/A 转换芯片,将数字量转变为模拟量并通过示波器观察其时序图和相图. 本文采用 2 块 12 位高速 D/A 转换芯片 MX7541,将 FPGA 开发板输出的数字量通过两路 D/A 转换得到连续的模拟量图形.

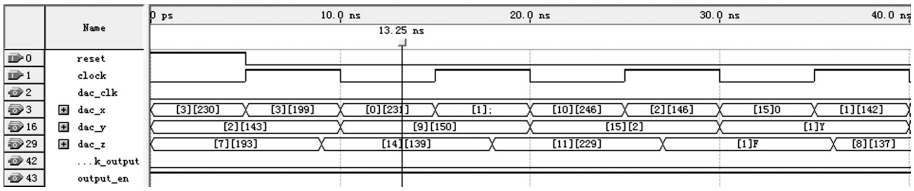
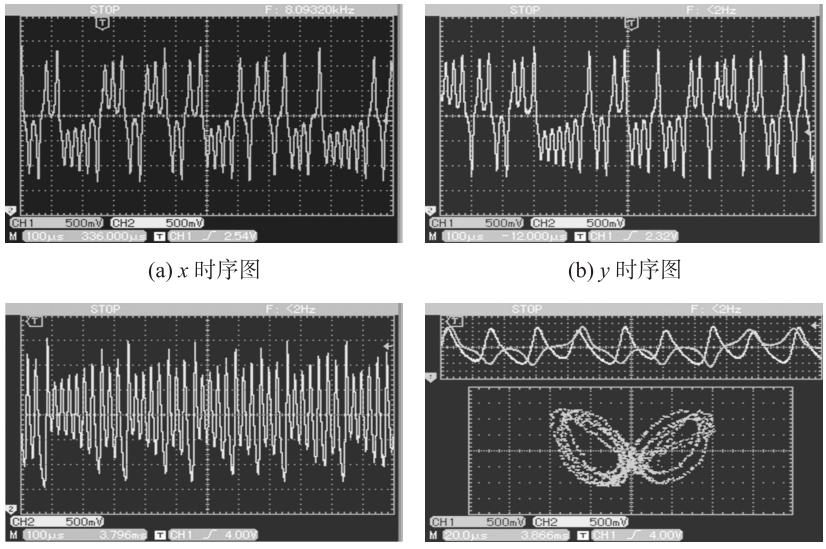


图 7　时序仿真

Fig. 7　The time-history simulations



(a) x 时序图　　(b) y 时序图

(c) z 时序图　　(d) x-z 时序图

图 8　硬件电路实现

Fig. 8　The implementation for hardware circuit

2.3 2 种方法的对比

在以上实现 Lorenz 系统的两种方法中,采用了不同的离散方法,最终通过硬件输出的图形相差并不大. 采用 DSP-Builder 开发平台实现混沌吸引子的离散方法相对比较简单,利用内置的加法器、乘法器、放大器等模块搭建混沌电路比较方便. 但是,模型所占内存相对比较大(例如实现同样的 Lorenz 系统所需的总逻辑元素,DSP-Builder 开发平台需要 2 847 个,硬件描述语言则只需要 1 502 个),对于 FPGA 开发板的配置要求较高,且有一定的时滞. 利用硬件语言编程的方式虽然编程过程比较繁琐,但模型所占的内存相对较小且无时滞现象,具体对比如表 1 所示.

表 1 2 种实现方法的对比

Table1 The compare of two methods

	DSP-Builder 开发平台	硬件描述语言
总逻辑元素/个	2 847	1 502
总组合函数/个	2 847	1 164
专用逻辑寄存器/个	154	752
时滞	有	无
可移植性	不可移植	可移植

3 结语

本文采用 DSP-Builder 软件开发平台和 Verilog HDL 硬件描述语言两种方法实现了 Lorenz 系统的离散化和混沌吸引子,并使用 FPGA 技术产生了数字混沌信号,并比较了两种方法各自的优缺点. 当实现 1 个简单的混沌系统(如三维系统或更低维的系统)时,可采用 DSP-Builder 软件开发平台的方法;若利用 FPGA 实现较复杂的系统或实现同步控制和保密通信时,采用硬件语言编程的方法更容易. 通过两种方法的对比和总结,为后续利用 FPGA 实现非线性系统的相关应用提供了良好的依据.

[参考文献](References)

[1] 禹思敏. 混沌系统与混沌电路—原理、设计及其在通信中的应用[M]. 西安:西安电子科技大学出版社,2011.
Yu Simin. Chaotic Systems and Chaotic Circuits-Principle,Design and its Application in Communications[M]. Xi'an:Xidian University Publishing House,2011.(in Chinese)

[2] 晋建秀,丘水生. 基于物理混沌的混合图像加密系统研究[J]. 物理学报,2010,59(2):792-800.
Jin Jianxiu,Qiu Shuisheng. Cascaded image encryption systems based on physical chaos[J]. Acta Physica Sinica,2010,59(2):792-800.(in Chinese)

[3] Merah L,Ali-Pacha A,Said N H. Design and FPGA implementation of Lorenz chaotic system for information security issues[J]. Applied Mathematical Sciences,2013,7(5):237-246.

[4] 刘强,方锦清,赵耿,等. 基于 FPGA 技术的混沌加密系统研究[J]. 物理学报,2012,61(13):78-83.
Liu Qiang,Fang Jinqing,Zhao Geng,et al. Research of chaotic encryption system based on FPGA technology[J]. Acta Physica Sinica,2012,61(13):78-83.(in Chinese)

[5] 张家树,肖先赐. 基于广义混沌映射切换的混沌同步保密通信[J]. 物理学报,2001,50(11):2 121-2 125.
Zhang Jiashu,Xiao Xianci. Chaotic synchronization secure communications based on the extended chaotic maps switch[J]. Acta Physica Sinica,2001,50(11):2 121-2 125.(in Chinese)

[6] 周武杰,禹思敏. 基于 IEEE-754 标准和现场可编程门阵列技术的混沌产生器设计与实现[J]. 物理学报,2008,57(8):4 738-4 747.
Zhou Wujie,Yu Simin. Design and implementation of chaotic generators based on IEEE-754 standard and field programmable gate array technology[J]. Acta Physica Sinica,2008,57(8):4 738-4 747.(in Chinese)

[7] 邵书义,闵富红,吴薛红,等. 基于现场可编程逻辑门阵列的新型混沌系统实现[J]. 物理学报,2014,63(6):060501-1-9.
Shao Shuyi,Min Fuhong,Wu Xuehong,et al. Implementation of a new chaotic system based on field programmable gate array[J].

Acta Physica Sinica,2014,63(6):060501-1-9.(in Chinese)

[8] 刘玉民,张雨虹,姚明林. 基于 FPGA 的混沌信号发生器的设计与实现[J]. 计算机工程与设计,2010,31(18):3 972-3 974.
Liu Yumin,Zhang Yuhong,Yao Minglin. Design and implementation of chaotic signal generator based on FPGA[J]. Computer Engineering and Design,2010,31(18):3 972-3 974.(in Chinese)

[9] 王日明,刘明华,盛堰,等. 基于龙格库塔算法和可编程门阵列技术的混沌系统实现[J]. 西南师范大学学报:自然科学版,2012,37(1):41-46.
Wang Riming,Liu Mnighua,Sheng Yan,et al. Implementation of a chaotic system based on Runge-Kutta algorithm and programmable gate array technology[J]. Journal of Southwest China Normal University:Natural Science Edition,2012,37(1):41-46.(in Chinese)

[10] 王忠林,王光义. 基于 FPGA 的混沌系统设计与实现[J]. 计算机工程与设计,2009,30(14):3 365-3 370.
Wang Zhonglin,Wang Guangyi. Design and implementation of chaotic system based on FPGA[J]. Computer Engineering and Design,2009,30(14):3 365-3 370.(in Chinese)

[11] 张钰,禹思敏,刘明华. 用 FPGA 技术产生多涡卷超混沌吸引子的研究[J]. 电路与系统学报,2007,12(1):39-43.
Zhang Yu,Yu Simin,Liu Minghua. Generating multi-scroll hyperchaotic attractors based on FPGA technology[J]. Journal of Circuits and Systems,2007,12(1):39-43.(in Chinese)

[12] 左建政,王光义. 基于 FPGA 技术的数字混沌信号产生[J]. 杭州电子科技大学学报:自然科学版,2008,28(6):5-8.
Zuo Jianzheng,Wang Guangyi. Generation of digital chaotic signals based on FPGA technology[J]. Journal of Hangzhou Dianzi University:Natural Science Edition,2008,28(6):5-8.(in Chinese)

[13] Lorenz E N. Deterministic nonperiodic flow[J]. Journal of the Atmospheric Sciences,1963,20:130-141.

[责任编辑:严海琳]