

文章编号: 1001-893X(2011)04-0026-05

混沌噪声产生器及其 FPGA 实现^{*}

王喜风, 王可人, 冯 辉, 田上成

(解放军电子工程学院, 合肥 230037)

摘 要: 为实时产生混沌噪声, 设计了一种基于 Tent 映射双向耦合映象格子和“接收-拒绝”法的混沌噪声产生器, 将其由浮点运算转换为定点运算后在 FPGA 上实现。所实现的混沌噪声产生器具有结构简单、运算复杂度低、资源占用少且易于控制等优点。性能测试结果表明: 混沌噪声产生器能够产生具有任意分布和平坦功率谱的混沌噪声, 且随机性较好。

关键词: 混沌噪声; 耦合映象格子; “接收-拒绝”法; FPGA

中图分类号: TN97 **文献标识码:** A doi: 10.3969/j.issn.1001-893x.2011.04.006

Chaotic Noise Generator and its FPGA Realization

WANG Xi-feng, WANG Ke-ren, FENG Hui, TIAN Shang-cheng

(Electronic Engineering Institute, Hefei 230037, China)

Abstract: To generate chaotic noise, a chaotic noise generator is designed based on Tent double-way coupled map lattice and “acceptance-rejection”. The generator is realized on FPGA after it is converted from floating pointed operation to fixed pointed operation. The realized generator has advantages including simple structure, low complexity of algorithm, accounting for few resources and easy control. The results of performance test show that the generator can generate chaotic noise with arbitrary distribution, flat power spectrum and good randomness.

Key words: chaotic noise; coupled map lattice; “acceptance-rejection” method; FPGA

1 引 言

传统噪声多由模拟噪声源产生, 易受温度和其它环境因素影响而发生漂移, 且可控性差, 难于对其进行加工和复制^[1]。随着数字电路的发展, 数字化噪声逐渐取代模拟噪声, 但现有的多种产生方法都有其缺陷: m 序列的随机性较差, 数量有限; 多频选择调相方式和直接序列移相键控方式产生的信号频谱不满足白噪声的要求^[1]。

混沌信号具有类噪声性、带宽较宽、可控性和可再生性等优点, 可以替代以上方法来产生数字化噪声信号。

本文基于 Tent 映射双向耦合映象格子 (Tent Double-way Coupled Map Lattice, TDCML) 和“接收-

拒绝”法提出了一种混沌噪声产生方法, 并将该产生方法在 FPGA 上实现为混沌噪声产生器。对实际产生的混沌噪声序列进行性能测试, 并与相应的理论值和仿真结果进行了比较, 结果表明混沌噪声产生器能够产生具有任意分布和平坦功率谱的混沌噪声, 且结构简单, 易于控制。

2 混沌噪声的产生

与低维的混沌映射相比, TDCML 映射在时间和空间上都是混沌的, 具有更复杂的混沌行为和更丰富的混沌特性, 通过序列间的相互扰动可以有效克服有限精度问题, 同时不影响序列本身的混沌特性^[2]。另外, TDCML 映射运算简单, 数据间没有乘除运算, 且其并行运算的特点使序列的产生速度更

^{*} 收稿日期: 2011-01-13; 修回日期: 2011-03-03

快^[3],所以本文采用 TDCML 映射作为混沌噪声源。

2.1 TDCML 映射

TDCML 映射的数学表达式^[4]为

$$\begin{cases} x_i(n+1)=(1-\varepsilon)f(x_i(n))+\frac{\varepsilon}{2}[f(x_{i+1}(n))+f(x_{i-1}(n))] \\ f(x_i(n))=\begin{cases} x_i(n)/a, & x_i(n)\in(0,a) \\ [1-x_i(n)]/(1-a), & x_i(n)\in(a,1) \end{cases} \end{cases} \quad (1)$$

式中, ε 是耦合系数且 $0<\varepsilon<1$, L 是系统尺寸, i 为格点坐标, n 为迭代次数, a 是局部映射(Tent 映射)的分形参数且 $0<a<1$, 边界条件为 $x_0(n)=x_L(n)$, $x_{L+1}(n)=x_1(n)$ 。

TDCML 映射在 $\varepsilon<0.01$ 时, 各格点序列分布趋于均匀分布, 而其局部映射(Tent 映射)对扰动极为敏感, 微小的扰动在格子间通过扩散而迅速放大, 因此, 在弱耦合情况下($\varepsilon=0.01$), TDCML 映射仍具有良好的时空混沌性态^[4]。另外, 由于局部映射的功率谱是常数, 所以 TDCML 映射各格点序列具有平坦的功率谱。

2.2 混沌噪声的产生

常用于产生高斯分布信号的算法有 Box - Muller 算法和 Wallace 算法等, 这些算法只能产生特定分布的信号, 且有数据间乘法运算^[5], 影响信号的产生速度。文献[6]提出的“接收 - 拒绝”法可以产生任意分布的随机数, 且算法简单, 随机数产生速度快。由此, 本文采用 TDCML 映射和“接收 - 拒绝”法提出了一种产生具有任意分布和平坦功率谱的混沌噪声设计方法, 图 1 为其设计框图。

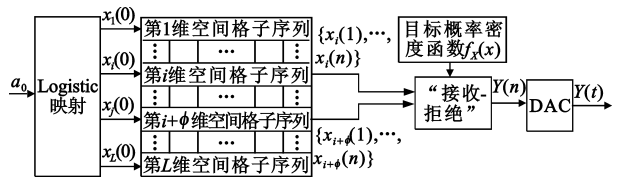


图 1 混沌噪声产生器的设计框图

Fig.1 Design block diagram of chaotic noise generator

在弱耦合情况下, TDCML 映射的各格点序列都满足均匀分布, 为减少数据间的相关性, 选取 TDCML 映射中空间间隔为 ϕ 、长度为 n 的两个格点序列 $\{x_i(1), x_i(2), \cdots, x_i(n)\}$ 和 $\{x_{i+\phi}(1), x_{i+\phi}(2), \cdots, x_{i+\phi}(n)\}$, 通过“接收 - 拒绝”法产生具有任意分布和平坦功率谱的混沌序列 $Y(n)$, 将 $Y(n)$ 经 DAC 后得到混沌噪声 $Y(t)$ 。为便于控制, TDCML 映射的 L 个初始值由 Logistic 映射提供, 这样只要一个 Logistic 映射的初始值 a_0 就可以驱动整个系统运行。

3 混沌噪声的 FPGA 实现

3.1 TDCML 映射的定点运算模型

为降低资源占用率, 提高运算速度, 将式(1)由浮点运算转换为定点运算。经仿真分析, 当 $p=32$ 时 TDCML 序列处于混沌态且性能较好, 所以混沌噪声产生器在 FPGA 上实现时的计算精度取 32 bit。为避免全同步现象^[7], 考虑在降低资源占用率的同时提高序列性能, 系统尺寸 L 取 8。

为产生均匀分布的混沌序列, 同时简化 FPGA 的定点运算, 令 $\varepsilon=2^{-7}=0.007\ 812\ 5$, $a=0.5$ 。此时, TDCML 映射的定点运算模型为

$$\begin{cases} x_i(n+1)=(1-2^{-7})f(x_i(n))+2^{-8}[f(x_{i+1}(n))+f(x_{i-1}(n))] \\ f(x_i(n))=\begin{cases} 2x_i(n), & x_i(n)\in(\underbrace{00\cdots0}_{32}, \underbrace{10\cdots0}_{31}) \\ 2[1-x_i(n)], & x_i(n)\in(\underbrace{10\cdots0}_{31}, \underbrace{11\cdots1}_{32}) \end{cases} \\ x_0(n)=x_L(n), x_{L+1}(n)=x_1(n) \end{cases} \quad (2)$$

该模型中只有移位、加法、减法和判断等简单运算, 所以占用资源少, 信号产生速度快。

3.2 混沌噪声产生器

本文采用 Xilinx 公司的 Spartan 3E 系列的 XC3S1600E 芯片, 以产生具有 Gauss 分布和平坦功率谱的混沌噪声为例来实现本文提出的混沌噪声产生方法。图 2 为该混沌噪声产生器的系统框图。

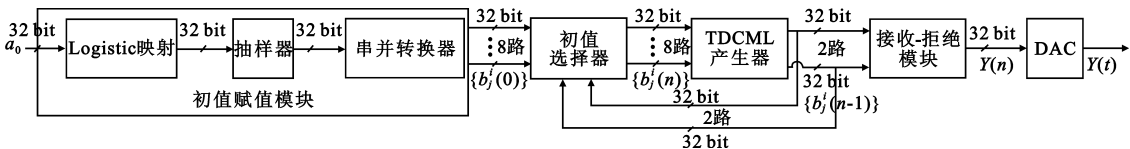


图 2 混沌噪声产生器的系统框图

Fig.2 System block diagram of chaotic noise generator

当 FPGA 的计算精度为 32 bit、TDCML 映射的系统尺寸 $L = 8$ 、耦合系数 $\epsilon = 2^{-7}$ 、分形参数 $a = 0.5$ 时,该系统的工作流程如下。

(1)由于 Logistic 映射的数据产生周期为 3 个时钟周期,为减少相邻数据间的相关性,抽样器每间隔 6 个时钟周期抽取一次数据。

(2)在计数器控制下,串并转换器依次将抽样器输出的 8 个 32 bit 数据存储到寄存器中,到最后一个数据存储到寄存器为止,总共需要 48 个时钟周期,系统在计数器下一次计数时触发 8 个数据同时并行输出。

(3)当初值选择器第一次接收到数据时,将选通串并转换器传来的数据作为 TDCML 产生器的初始值,之后选通 TDCML 产生器传来的数据,让 TDCML 产生器循环迭代产生 TDCML 序列,图 3 为 TDCML 映射的算法流程图。

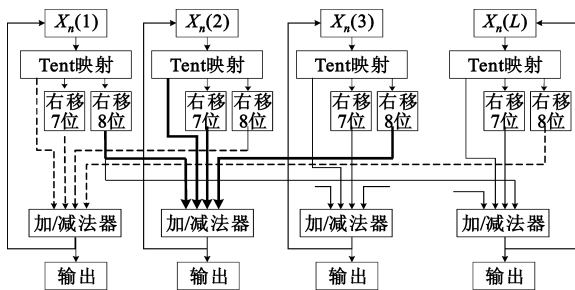


图 3 TDCML 映射的算法流程图

Fig.3 Flow chart of TDCML-map arithmetic

(4)选取 TDCML 映射格点坐标是 3 和 6 的两路 32 bit 数据,将其输出到接收 - 拒绝模块,图 4 为“接收 - 拒绝”模块框图。ROM 中预先存储了 Gauss 分布数据,将第 3 路的高 10 bit 作为地址码读取 ROM 中 1 024 个 32 bit 的分布数据,将其与第 6 路的数据进行比较,当 $a < b$ 时,控制模块使能 FIFO 的 wr_en ,将第 3 路的 32 bit 数据存入 FIFO。当 FIFO 存储一定数据后,在接收数据的同时,控制模块使能 rd_en ,在 clk_out 时钟的控制下将存储的数据输出,得到混沌噪声序列 $Y(n)$,最后通过 DAC 将混沌噪声 $Y(t)$ 输出。

另外,为保证 FIFO 的连续输出,根据“接收 - 拒绝”法原理^[5],若产生 Gauss 分布信号,设定 $clk_out = 1/21\ clk, clk_in = 1/7\ clk$,即在主频 100 MHz 下,混沌噪声的输出速度是 4.76 Msample/s。为更好体现分布数据的分布特点,本文对 Gauss 分布数据采用 μ 律量化后存储到 ROM 中。此外,为提高系统的可控

性,本文设计了一个初值赋值模块,只需一个初始值 a_0 就能驱动整个系统运行。

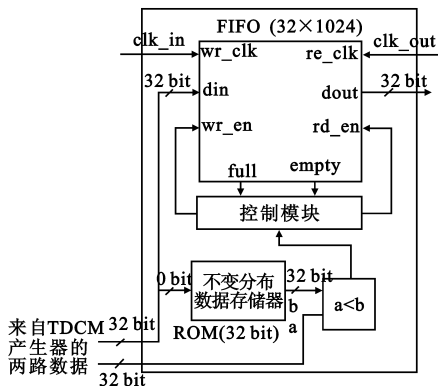


图 4 “接收 - 拒绝”模块框图

Fig.4 Block diagram of “acceptance-rejection” module

利用 ISE Simulator 对混沌噪声产生器进行功能仿真,当初值 $a_0 = 1$ 时,仿真结果如图 5 所示。可见,混沌噪声连续输出且信号产生速度符合设计要求。

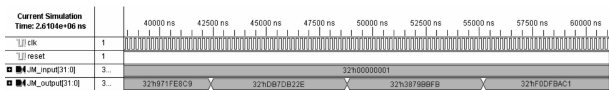


图 5 ISE Simulator 功能仿真结果

Fig.5 Functional simulation result with ISE simulator

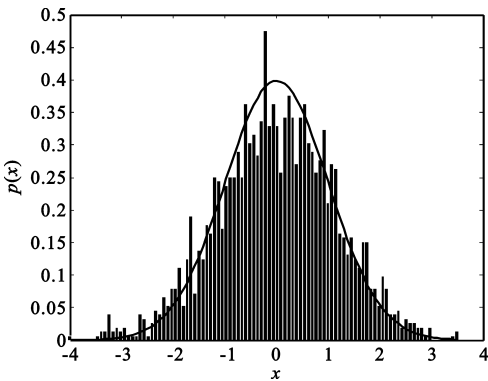
4 性能测试与结论

本节对混沌噪声产生器产生的混沌伪随机序列 $Y(n)$ 进行性能测试^[8-9],主要包括不变分布、功率谱和最大 Lyapunov 指数。本文选取满足 Gauss 分布和 Rayleigh 分布的两种混沌噪声序列进行测试。

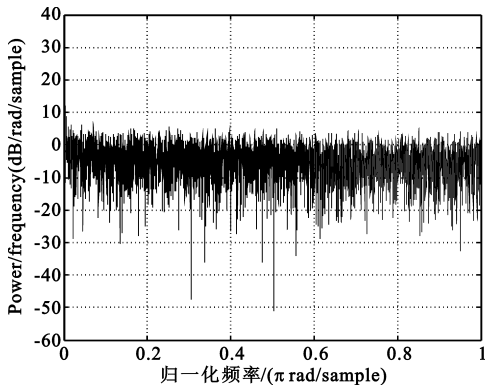
4.1 Gauss 分布混沌噪声序列性能测试

在 ROM 中预存 1 024 个 32 bit 的服从 $N(0,1)$ 分布的数据。设混沌噪声产生器的初始值 $a_0 = 1$,取其产生的 50 000 个样本数据进行不变分布和功率谱测试,图 6 为样本数据的不变分布直方图和功率谱图。

可见,该样本数据的直方图包络很好地逼近标准 Gauss 分布概率密度曲线,其功率谱没有较大的峰值,较平坦,同时计算得到样本数据的均值为 0.001 2,方差为 0.997 1,与标准 Gauss 分布的均值和方差的理论值非常接近。可见混沌噪声产生器能够按照 ROM 中存储的 Gauss 分布数据产生具有相应分布和平坦功率谱的混沌噪声。



(a) Gauss 分布混沌伪随机序列的不变分布



(b) Gauss 分布混沌伪随机序列的功率谱

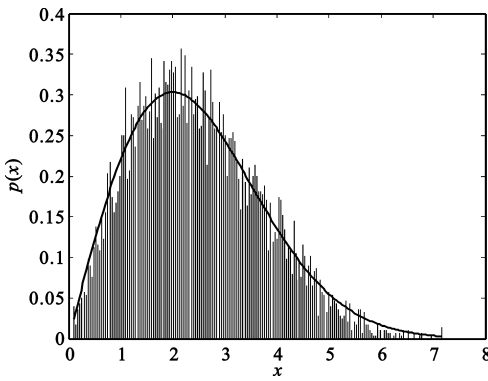
图 6 Gauss 分布混沌伪随机序列的性能测试
Fig.6 Performance testing of chaotic pseudo sequences with Gauss distribution

混沌噪声作为一种类噪声,其随机性是衡量其性能好坏的一个重要指标。混沌信号的随机性通常采用最大 Lyapunov 指数来衡量,最大 Lyapunov 指数越大,随机性越强。

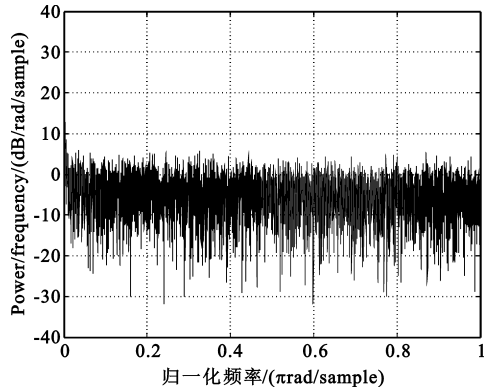
本文采用小数据量法来计算 Gauss 分布混沌伪随机序列的最大 Lyapunov 指数,当嵌入维数 $m = 3$ 、时延 $\tau = 3$ 时, Gauss 分布混沌伪随机序列的最大 Lyapunov 指数为 2.806 9,远远大于低维混沌序列的最大 Lyapunov 指数,所以 Gauss 分布混沌伪随机序列具有良好的随机性。

4.2 Rayleigh 分布混沌伪随机序列性能测试

在 ROM 中预存 1 024 个 32 bit 的 Rayleigh 分布数据,该 Rayleigh 分布服从 $R(2)$ 分布,设混沌噪声产生器初始值 $a_0 = 1$,取其产生的 50 000 个样本数据进行不变分布和功率谱测试,图 7 为样本数据的不变分布直方图和功率谱图。



(a) Rayleigh 分布混沌伪随机序列的不变分布



(b) Rayleigh 分布混沌伪随机序列的功率谱

图 7 Rayleigh 分布混沌伪随机序列的性能测试
Fig.7 Performance testing of chaotic pseudo sequences with Rayleigh distribution

可见,样本数据的直方图包络很好地逼近服从 $R(2)$ 分布的 Rayleigh 分布概率密度曲线,其功率谱没有较大的峰值,较平坦。计算得到样本数据的均值为 2.456,方差为 1.732,与理论上的均值 $\sqrt{2\pi}$ 和方差 $8 - 2\pi$ 很接近。同样,混沌噪声产生器能够按照 ROM 中存储的 Rayleigh 分布数据产生具有相应分布和平坦功率谱的混沌噪声。

当嵌入维数 $m = 3$ 、时延 $\tau = 3$ 时, Rayleigh 分布混沌噪声序列的最大 Lyapunov 指数为 2.840 9,远远大于低维混沌序列的最大 Lyapunov 指数,所以 Rayleigh 分布混沌噪声序列具有良好的随机性。

综上所述,混沌噪声产生器能够按照 ROM 中的分布数据产生具有相应分布和平坦功率谱的混沌噪声,且该信号具有较强的随机性。

4.3 设计方法比较

采用 XC3S1600E 芯片,在 100 MHz 主频下,以产生 Gauss 分布混沌噪声为例,将本文的混沌噪声产生器的设计方法与文献[1]中两种基于 Logistic 映射产生混沌噪声的设计方法进行比较,结果如表 1 所示。

表 1 设计方法比较
Table 1 Comparison of design methods

设计方法	信号输出 速度/ (Msample/s)	输出 路数	占用资源				分布特性	
			Slice	Slice Flip Flop	4 input LUTs	MULT 18 × 18	均值	方差
设计方法 1 ^[1]	33.33	1 路	49%	24%	48%	222.2%	0.001 3	0.997 5
设计方法 2 ^[1]	1.67	1 路	5%	4%	4%	11%	0.001 7	0.998 2
本文方法	4.76	多路	26%	18%	17%	11%	0.001 2	0.997 1

由表 1 可见,设计方法 1 资源占用较多,几乎是本文方法的 2 倍,特别是乘法器已经超过芯片资源的 1 倍,但是其最大输出速度是本文方法的近 7 倍;本文方法的最大输出速度是设计方法 2 的近 3 倍,但资源占用是其近 5 倍;3 种方法产生的 Gauss 分布的分布特性基本相同;本文方法最多能产生 4 路混沌噪声,而设计方法 1 和 2 只能产生 1 路信号。

参考文献:

[1] 张家树,冯海涛.基于混沌的最佳压制干扰噪声源设计[J].电波科学学报,2006,21(5):701-707.
ZHANG Jia - shu, FENG Hai - tao. Chaos - based optimal radar jamming noise sources design [J]. Chinese Journal of Radio Science, 2006, 21(5): 701 - 707. (in Chinese)

[2] Hu Hanping, Xu Ya, Zhu Ziqi. A method of improving the properties of digital chaotic system [J]. Chaos Solitons and Fractals, 2008, 38(2): 439 - 446.

[3] Ping Li, Zhong Li, Wolfgang A Halang, et al. A multiple pseudorandom - bit generator based on a spatiotemporal chaotic map [J]. Physics Letters A, 2006, 349(6): 467 - 473.

[4] 刘建东,付秀丽.基于耦合帐篷映射的时空混沌单向 Hash 函数的构造[J].通信学报,2007,28(6):30-38.
LIU Jian - dong, FU Xiu - li. Spatiotemporal chaotic one - way Hash function construction based on coupled tent maps[J]. Journal on Communications, 2007, 28(6): 30 - 38. (in Chinese)

[5] 杜学峰,武杰.基于 FPGA 的任意分布高速伪随机数发生器[J].中国科学技术大学学报,2006,36(9):990-994.
DU Xue - feng, WU Jie. Arbitrary distribution high - speed pseudo - random number generator based on FPGA [J]. Journal of University of Science and Technology of China, 2006, 36(9): 990 - 994. (in Chinese)

[6] Mao Y, Liu C, Liu W. Design and FPGA implementation of a pseudo - random bit sequence generator using spatiotemporal chaos [C]//Proceedings of 2006 International Conference on Communications, Circuits and Systems. Guilin: IEEE, 2006: 2114 - 2118.

[7] 曹骝,毛耀斌,刘文波,等.时空混沌伪随机比特发生器及其 FPGA 实现[J].系统工程与电子技术,2008,30(9):1606-1610.
CAO Liu, MAO Yao - bin, LIU Wen - bo, et al. Pseudo - random bit generator based on spatio - temporal chaos and its FPGA implementation [J]. Systems Engineering and Electron-

ics, 2008, 30(9): 1606 - 1610. (in Chinese)

[8] 杨瑛,邓鹏飞,刘春泉.混沌噪声调频信号对 UWB - SAR/ISAR 成像的干扰[J].电讯技术,2008,48(9):75-78.
YANG Ying, DENG Peng - fei, LIU Chun - quan. Chaotic Noise FM signal jamming on UWB - SAR/ISAR Imaging [J]. Telecommunication Engineering, 2008, 48(9): 75 - 78. (in Chinese)

[9] 吕波,张晓发,袁乃昌.数字噪声宽带干扰源设计[J].军械工程学院学报,2008,20(1):54-57.
LV Bo, ZHANG Xiao - fa, YU Nai - chang. Design of digital noise FM broadband jamming source [J]. Journal of Ordnance Engineering College, 2008, 20(1): 54 - 57. (in Chinese)

作者简介:

王喜风(1986—),男,浙江嘉善人,2008 年于解放军电子工程学院获学士学位,现为硕士研究生,主要研究方向为非线性信号处理和数字系统设计;
WANG Xi - feng was born in Jiashan, Zhejiang Province, in 1986. He received the B.S. degree from Electronic Engineering Institute of PLA in 2008. He is now a graduate student. His research interests include nonlinear signal processing and digital system design.
Email: wangxifeng815@163.com

王可人(1957—),男,江苏镇江人,1986 年于解放军理工大学获硕士学位,现为教授、博士生导师,主要研究方向为无线通信信号的分析 and 处理;
WANG Ke - ren was born in Zhenjiang, Jiangsu Province, in 1957. He received the M.S. degree from PLA University of Science and Technology in 1986. He is now a professor and also the Ph.D. supervisor. His research interests include wireless communication signal analysis and processing.

冯 辉(1978—),男,山东荣城人,2009 年于解放军电子工程学院获博士学位,现为讲师,主要研究方向为通信信号处理;
FENG Hui was born in Rongcheng, Shandong Province, in 1978. He received the Ph.D. degree from Electronic Engineering Institute of PLA in 2009. He is now a lecturer. His research direction is communication signal processing.

田上成(1985—),男,河北故城人,2008 年于合肥工业大学获学士学位,现为硕士研究生,主要研究方向为通信信号处理、卫星通信技术。
TIAN Shang - cheng was born in Gucheng, Hebei Province, in 1985. He received the B.S. degree from Hefei University of Technology in 2008. He is now a graduate student. His research interests include communication signal processing and satellite communication technology.