

面向随机数的布尔混沌带宽增强研究

刘海芳¹
LIU Haifang

摘要

布尔混沌系统是由逻辑器件互耦合连接组成的数字混沌电路,可以产生混沌信号,对电路中噪声进行非线性放大进而输出不可预测的混沌序列,结构简单、易于集成,在随机数产生领域获得了广泛的关注。但受限于输出布尔混沌序列的带宽,随机数提取速率难以提高。而逻辑器件是布尔混沌系统的唯一非线性元件,文章通过理论模拟研究逻辑器件响应特性对布尔混沌信号带宽的影响,使布尔混沌系统每个非线性器件均可输出混沌信号,并通过控制变量法,观察单独调节任一器件响应特性以及协调多元器件响应特性时布尔混沌任一输出的变化情况,最终确定关键器件以及参数优化方案。结果表明,随着器件的响应速度增大,混沌信号的带宽指数增强,其中协调减小系统中多个器件的响应特性参数布尔混沌熵源复杂度和带宽增强效果最显著,自反馈结构可以增强器件响应特性减小的带宽,为布尔混沌系统设计中器件的选择和参数设计提供了理论基础。

关键词

布尔混沌; 带宽; 器件响应特性; 随机数

doi: 10.3969/j.issn.1672-9528.2026.02.019

0 引言

随着网络的高速发展,信息安全越来越重要,随机数可以对信息进行加密,是保证信息安全的关键^[1]。混沌是一种无周期的复杂的序列,具有初值敏感性,微小的变化可以导致混沌序列轨迹分离为完全不同的轨迹,因此具有长期不可预测性,这种特性与随机数的不可预测性高度一致,因此在随机数产生领域获得了成功的应用^[2-3]。

2018年,Zhang等^[4]在实验室使用逻辑器件耦合连接硬件实现了自治布尔网络,并观察到混沌现象,并命名为布尔混沌。布尔混沌电路结构简单,其带宽优于传统的电路混沌系统,且其输出具有二值化特征易于提取量化,在随机数领域获得了广泛的应用^[5-8]。但是基于布尔混沌熵源的随机数产生速率普遍约为100 Mbit/s。为了提高随机数速率,2013年,Rosin等^[9]使用128个布尔混沌系统作为熵源并行实现了12.8 Gbit/s的随机数。单路布尔混沌熵源产生随机数速率仍然为100 Mbit/s,通过128个熵源并行速率提高的方法使器件数量成百倍增加,增加系统功耗。2015年,Park等^[10]对随机数提取量化方法进行改进,使用双阈值量化实现了

300 Mbit/s的随机数产生。该方法通过对采样时刻的混沌序列值进行双阈值量化得到两位随机数的方法提高随机数速率,但是双阈值量化的方法增加了随机数熵源的后处理步骤,带来随机数0-1偏置,同时增加系统复杂度。2020年,刘峰^[11]设计了一种66节点的布尔混沌系统,并使用延迟异或后处理电路消除偏置,最终实现了10 Gbit/s的随机数发生器。该方法同样存在节点数量大幅增加,需要器件数量成倍增长,且增加了异或后处理结构,进一步增加了系统的复杂度。

混沌的带宽是限制随机数提取速率的本质原因。逻辑器件是布尔混沌系统的唯一非线性元件,通过理论模拟研究逻辑器件响应特性对输出布尔混沌信号带宽的影响。使用控制变量法,分别研究布尔混沌系统中多个逻辑器件中任一逻辑器件的响应特性以及协调控制多个器件的响应特性时,所有器件的输出状态的变化情况,确定影响布尔混沌熵源带宽的关键器件,最终提出优化方案增强布尔混沌带宽。

1 理论模型

布尔混沌系统结构图如图1所示,该布尔混沌由3个二输入二输出节点按照图中所示方式相互连接组成,其中节点2执行异或非操作在硬件实现中由异或非逻辑门实现,节点1和3执行异或操作在硬件实现中由异或逻辑门实现,连接线箭头方向为信号传输方向, τ_{ij} 表示节点 j 的信号传输到节点 i 的传输延时。

1. 山西工程科技职业大学 山西太原 030024

[基金项目] 山西省基础研究计划自由探索类青年科学基金项目(202303021222283); 山西省教育厅科技创新项目(2023L423)

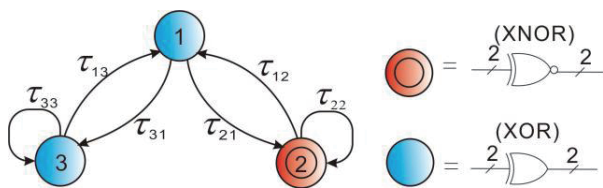


图1 布尔混沌系统结构示意图

数学模型如式(1)~(2)所示,分段线性微分方程是布尔混沌系统的经典数学模型,微分项可以模拟逻辑器件的响应过程^[12-13]。

$$\begin{cases} \tau_{lp,1} \frac{dx_1(t)}{dt} = -x_1(t) + X_2(t-\tau_{1,2}) \oplus X_3(t-\tau_{1,3}) \\ \tau_{lp,2} \frac{dx_2(t)}{dt} = -x_2(t) + X_1(t-\tau_{2,1}) \odot X_3(t-\tau_{2,3}) \\ \tau_{lp,3} \frac{dx_3(t)}{dt} = -x_3(t) + X_1(t-\tau_{3,1}) \oplus X_2(t-\tau_{3,2}) \end{cases} \quad (1)$$

式中:微分项 dx_1/dt 、 dx_2/dt 、 dx_3/dt 分别为模拟逻辑门1、2、3的响应过程;微分项系数 $\tau_{lp,1}$ 、 $\tau_{lp,2}$ 、 $\tau_{lp,3}$ 为器件响应特性参数可以调节相应逻辑门的响应速度,参数值越小逻辑门响应越快; $x_1(t)$ 、 $x_2(t)$ 、 $x_3(t)$ 分别为节点1、2、3的输出信号,并经过相应的延时后作为相连节点的输入,收到输入信号的节点在执行逻辑运算前会对输入信号进行量化,得到布尔值“0”或“1”,再对量化结果进行逻辑运算。

$$X_i(t) = \begin{cases} 1, & x_i(t) > x_{th} \\ 0, & x_i(t) < x_{th} \end{cases} \quad (2)$$

式中: $x_{th}=0.5$ V,表示阈值电压。

2 实验结果与分析

图1中布尔混沌系统的每个节点都可以产生混沌输出,实验中首先以节点1的输出作为系统的输出进行研究,实验中延时参数取值如表1所示。

表1 延时参数表

单位: ns					
τ_{12}	τ_{13}	τ_{21}	τ_{22}	τ_{31}	τ_{33}
0.2	0.07	2.02	0.97	0.19	0.21

逻辑器件是布尔混沌系统的唯一非线性元件,逻辑器件的非线性响应是系统产生混沌的根本原因,分岔图是一种常用的混沌分析方法,使用分岔图研究器件响应特性参数 τ_{lp} ($\tau_{lp} = \tau_{lp,1} = \tau_{lp,2} = \tau_{lp,3}$)对系统输出的影响,结果如图2所示。图中横坐标 τ_{lp} 取值范围为0.01~3

ns,步进为0.007 ns,纵坐标为混沌序列中相邻两个上升沿之间的距离 Δt 。图中可以看出随着参数 τ_{lp} 减小,输出在混沌和周期之间交替出现,参数 τ_{lp} 越小,周期窗口越小混沌窗口越大,最终进入混沌。表明器件响应特性参数可以作为混沌分岔参数,使系统产生混沌信号。

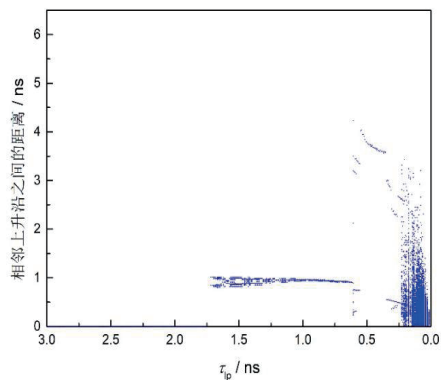


图2 布尔混沌熵源节点1的输出随响应特性参数 τ_{lp} 变化的分岔图

为直观地展示不同取值时系统输出的状态,分别观察了 $\tau_{lp}=0.63$ ns、0.305 ns、0.05 ns时系统输出时序,如图3所示。显然 $\tau_{lp}=0.63$ ns时输出为单倍周期信号, $\tau_{lp}=0.305$ ns时输出更加复杂,当 $\tau_{lp}=0.05$ ns时输出演变为非周期的混沌信号。

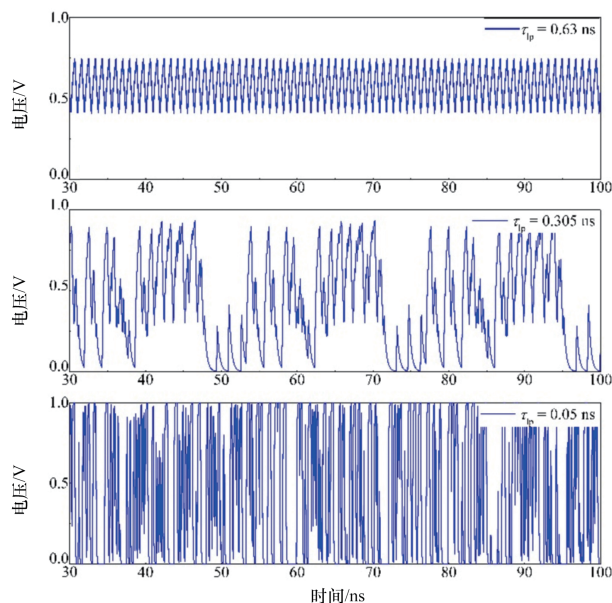


图3 布尔混沌熵源在 $\tau_{lp} = 0.63$ ns, 0.305 ns, 0.05 ns时的输出时序

带宽是混沌的重要特征之一,大的带宽有利于高速随机数的提取,研究了器件响应特性参数对输出布尔混沌带宽的影响,实验中延时参数取值如表1所示,除变化的器件响应特性参数其余取值均为0.1 ns。如图4所示为节点1的输出信号的带宽(-10 dB)随着 τ_{lp} 、 $\tau_{lp,1}$ 、 $\tau_{lp,2}$ 、 $\tau_{lp,3}$ 的变化情况, τ_{lp} ($\tau_{lp} = \tau_{lp,1} = \tau_{lp,2} = \tau_{lp,3}$)表示同时调节3个逻辑器件的响应特性参数。可以看出, τ_{lp} 的变化趋势最明显,协调控制系统中3个器件的响应特性参数对输出信号的混沌带宽调节范围最大,当值小于0.1 ns时,随着 τ_{lp} 的减小混沌信号的带宽呈指数增大, $\tau_{lp,1}$ 的调节范围次之, $\tau_{lp,2}$ 和 $\tau_{lp,3}$ 基本没有调节效果。

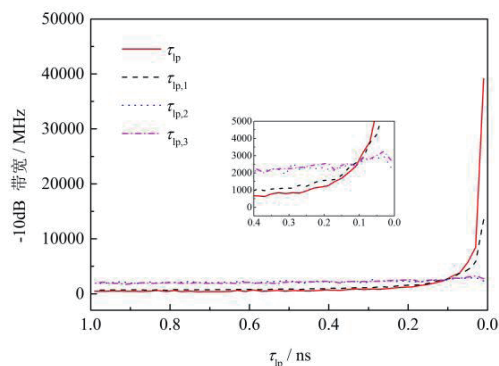


图4 布尔混沌熵源节点1的输出的带宽(-10 dB)随着器件响应特性参数的变化

为了得到更详细全面的结果,进一步观察了节点2和3的输出信号带宽随 τ_{lp} 、 $\tau_{lp,1}$ 、 $\tau_{lp,2}$ 、 $\tau_{lp,3}$ 的变化,如图5~6所示。

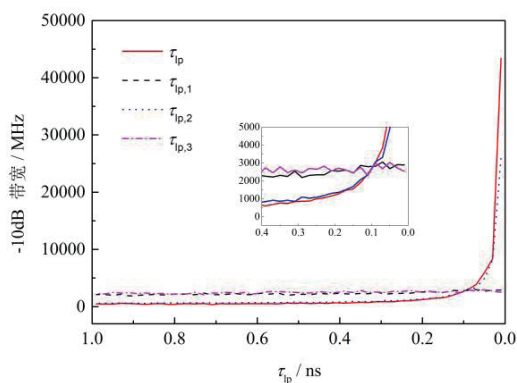


图5 布尔混沌熵源节点2的输出的带宽(-10 dB)随着器件响应特性参数的变化

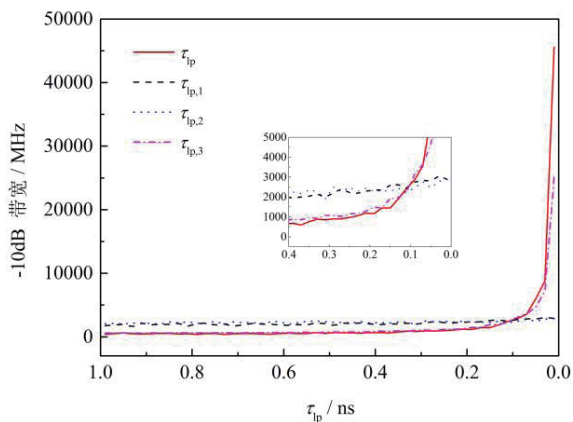


图6 布尔混沌熵源节点3的输出的带宽(-10 dB)随着器件响应特性参数的变化

图5~6中可以看出与图4中相同的是 τ_{lp} 的变化范围最大,表明同时调节3个器件的响应特性参数时系统中任意一个节点的输出混沌信号带宽呈指数增大。不同的是在图5中 $\tau_{lp,2}$ 的调节范围次之,图6中 $\tau_{lp,3}$ 的调节范围次之,表明单独减小任一器件响应特性只能增强该器件本身输出的混沌信号的带宽,同时受限于其他器件响应特性参数为0.1 ns,带宽

增强效果较小。对比分析图4中 $\tau_{lp,1}$ 、图5中 $\tau_{lp,2}$ 、图6中 $\tau_{lp,3}$ 可以看出,图4中 $\tau_{lp,1}$ 的调节范围较小,而图5中 $\tau_{lp,2}$ 和图6中 $\tau_{lp,3}$ 的调节范围较大且一致。结合图1可知,节点2和3有自反馈结构,而节点并没有。分析表明,节点增加自反馈,可以增强节点本身的器件响应特性参数,减小对自身输出混沌信号带宽的增强效果。

3 结论

使用分段线性微分方程模型对布尔混沌系统进行理论仿真研究,观察了非线性器件的响应特性对布尔混沌系统输出状态的影响;分岔图表明随着器件响应特性参数的减小,即器件响应速度增大,系统输出在混沌和周期之间交替,且混沌空间越来越大,周期空间越来越小,最终进入混沌。分析表明快的器件响应速度有利于产生混沌。分别研究了系统中各个器件单独调节时,不同节点输出混沌信号的带宽变化曲线,结果表明单独减小任一器件的响应特性参数可以增强自身输出混沌信号的带宽,对其他节点输出基本没有影响;其中带有自反馈结构的器件响应特性参数减小带宽增强效果最显著;当系统中所有非线性器件的响应特性参数同时减小,所有节点的输出混沌信号带宽均指数增大。上述研究结果为布尔混沌系统硬件设计与实现提供了理论指导。

参考文献:

- [1]YU F, LI L X, TANG Q, et al. A survey on true random number generators based on chaos[J/OL]. Discrete dynamics in nature and society, 2019[2025-09-12].<https://onlinelibrary.wiley.com/doi/10.1155/2019/2545123>.
- [2]张卓宇,蒋林,陈博阳,等.基于深度学习的光电振荡混沌系统建模及FPGA应用[J].光学学报,2024,44(19):117-127.
- [3]NAWWAR O, MINOSHIMA K, KUSE N. Parametric study of chaotic combs for high-rate random number generation[J]. IEEE photonics technology letters, 2025, 37(3): 153-156.
- [4]ZHANG R, GAO Z, GAUTHIER D J, et al. Boolean chaos[EB/OL].(2018-10-15)[2025-09-12].<https://arxiv.org/pdf/0906.4124>.
- [5]ZHOU H L, YAO L, FENG Y K, et al. Lightweight high-throughput TRNG based on single- node boolean chaotic structure[J]. International journal of circuit theory and applications, 2025, 53(5): 2983-2995.
- [6]张琪琪,张建国,李璞,等.基于布尔混沌的物理随机数发生器[J].通信学报,2019,40(1):201-206.
- [7]张鑫.基于随机布尔网络的真随机数发生器设计[D].西安:西安电子科技大学,2017.

基于三尺度鉴别器的水下图像运动模糊去除算法研究

石沈青¹
SHI Shenqing

摘要

在水下环境中,由于光照条件不足以及拍摄设备与场景间的相对运动,图像会呈现出不同程度的模糊,这一问题严重影响了基于视觉的海洋探测任务的开展。基于此,文章提出了一种三尺度鉴别器网络模型TC-DGAN,用于恢复水下运动模糊图像。该网络模型在AT-DGAN网络模型全局和局部尺度的基础上,引入中间尺度构成三尺度鉴别器,中间尺度只针对图像过渡区域模糊进行处理,从而弥补对水下图像的运动模糊的处理集中在全局和局部区域。此外,引入色彩一致性损失函数,用于解决水下图像去运动模糊时引起的颜色失真问题,保持去除模糊前后图像色彩一致。实验结果表明,所提改进算法相较于其他同类型算法,在图像恢复性能有所提升的同时有效控制了图像颜色失真。

关键词

水下运动模糊;三尺度鉴别器;色彩一致性损失函数;颜色失真

doi: 10.3969/j.issn.1672-9528.2026.02.020

0 引言

海洋蕴含着丰富的自然资源,涵盖渔业资源、油气矿产等战略储备。近年来,自主水下航行器搭载高分辨率成像系统,实现对海洋环境的数据采集,从而为基于视觉的海洋探索提供关键数据支撑^[1-2]。

然而,在实际的水下环境中,除了光的色散和衰减导致能见度低和光线不足外,水下图像和视频的获取通常由水下航行器、自主水下航行器和潜水员完成,其中运动伪影、模糊和抖动也会降低图像的质量^[3-4]。这些问题严重影响后续目标检测、三维重建等任务的精度与可靠性。因此,去除运动

模糊以提高图像质量具有重要意义。

目前图像去运动模糊主要分为传统方法和深度学习方法。传统方法在模糊核已知的情况下,将图像去模糊看作是一个反卷积问题^[5]。近年来,除利用卷积神经网络来估计模糊核^[6]的方法外,端到端的无核神经网络方法也得到了发展。Kupyn等^[7]改进了DeblurGAN,提出了DeblurGAN-v2。该模型通过引入特征金字塔网络结构作为核心构建模块,能够灵活地与各种骨干网络配合使用,从而在性能和效率之间取得平衡。Yu等^[8]进一步改进DeblurGAN-v2为AT-DGAN,引入自注意力机制弥补部分损失信息,同时为提高网络训练效率,将铰链损失函数引入到图像去模糊任务中。自然图像的去除运动模糊的方法直接应用于水下,会忽视运动模

1. 武汉轻工大学电气与电子工程学院 湖北武汉 430023

[8]MUNOZ-PACHECO J M, GARCIA-CHAVEZ T, GONZALEZ-DIAZ V R, et al. Two new asymmetric boolean chaos oscillators with no dependence on incommensurate time-delays and their circuit implementation [J]. Symmetry-based,2020,12(4): 506.

[9]ROSIN D P, RONTANI D, GAUTHIER D J. Ultrafast physical generation of random numbers using hybrid Boolean networks[J]. Physical review E,2013,87(4): 040902(R) .

[10]PARK M, RODGERS J C, LATHROP D P. True random number generation using CMOS Boolean chaotic oscillator[J]. Microelectronics journal,2015,46(12): 1364-1370.

[11]刘锋.10Gbps 物理随机数发生器及其采集存储系统的设

计与实现 [D]. 太原:太原理工大学,2020.

[12]龚利爽.面向物理随机数发生器的自治布尔网络研究 [D]. 太原:太原理工大学,2020.

[13]ROSIN D P. Dynamics of complex autonomous boolean networks[EB/OL].[2025-09-12].<https://link.springer.com/book/10.1007/978-3-319-13578-6>

【作者简介】

刘海芳(1989—),女,山西晋中人,博士,讲师,研究方向:混沌熵源和随机密钥的产生研究。

(收稿日期:2025-06-06 修回日期:2026-01-26)