



新型混沌电路与系统的设计原理及其应用

禹思敏 著



科学出版社

国家科学技术学术著作出版基金资助出版

新型混沌电路与系统的设计原理及其应用

禹思敏 著

科学出版社

北京

内 容 简 介

本书详细论述了新型混沌电路与系统的设计原理及其在多媒体混沌保密通信中的应用与技术实现,共19章。其中,第1~3章介绍混沌的基本概念、李氏指数的数值计算方法与应用、离散时间混沌系统。第4~8章介绍高维连续时间超混沌系统的设计,包括具有多个正李氏指数的连续时间超混沌系统、耗散系统与保守系统中的无筒并高维连续时间超混沌系统、无筒并高维连续时间超混沌系统的平均特征值准则、具有多控制器的无筒并高维连续时间超混沌系统、可配置任意多个正李氏指数的连续时间超混沌系统。第9~11章介绍整数域和数字域混沌系统,包括单个随机位迭代更新的1维整数域混沌系统、多个随机位迭代更新的1维整数域混沌系统、高维整数域和数字域混沌系统。第12~19章介绍新型混沌电路与系统在多媒体混沌保密通信中的应用,包括定点算法和状态机控制的通用FPGA混沌信号发生器、视频混沌保密通信系统的设计与FPGA实现、广域网传输实时远程视频混沌保密通信与ARM实现、多核多进程与H.264选择性加密的视频混沌保密通信、多核多线程与H.264编码后加密的视频混沌保密通信、视频混沌保密通信的手机实现、组播多用户和广域网传输的语音混沌保密通信、高维混沌映射单向Hash函数。

本书可作为电子科学与技术、信息与通信工程、控制科学与工程及相关专业的研究生教材或教学参考书,也可供自然科学和工程技术领域的高校教师 and 研究人员参考。

图书在版编目(CIP)数据

新型混沌电路与系统的设计原理及其应用 / 禹思敏著. —北京:科学出版社, 2018.11

ISBN 978-7-03-059216-3

I. ①新… II. ①禹… III. ①混沌理论-应用-电路设计 IV. ①TM02

中国版本图书馆CIP数据核字(2018)第244260号

责任编辑:裴育 纪四稳 / 责任校对:张小霞

责任印制:师艳茹 / 封面设计:蓝正

科学出版社出版

北京东黄城根北街16号

邮政编码:100717

<http://www.sciencep.com>

河北鹏润印刷有限公司印刷

科学出版社发行 各地新华书店经销

*

2018年11月第一版 开本:720×1000 1/16

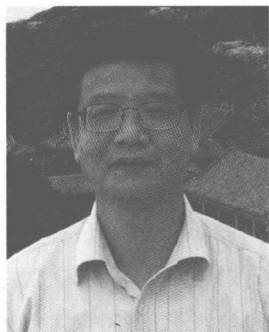
2018年11月第一次印刷 印张:34 1/2

字数:670 000

定价:198.00元

(如有印装质量问题,我社负责调换)

作者简介



禹思敏 1957年5月出生,2001年毕业于华南理工大学电路与系统专业,获工学博士学位。广东工业大学自动化学院二级教授、博士生导师,广东省攀峰重点学科、一级学科博士点“控制科学与工程”学术带头人,国家自然科学奖二等奖、教育部自然科学奖一等奖、广东省科学技术奖二等奖获得者,广东省南粤优秀教师,广东省优秀博士论文、优秀硕士论文指导教师。兼任中国密码学会混沌保密通信专业委员会委员、中国电子学会电路与系统分会混沌与非线性电路专业委员会第一届委员会副主任委员、德国施普林格出版社非线性电路 Brief 丛书编委会委员等学术职务。主持和承担国家及省部级科研项目18项,其中主持国家自然科学基金面上项目4项,承担国家自然科学基金重点项目1项、国家重点研发计划子课题1项。在 *IEEE Transactions*、《中国科学》等国内外期刊上发表SCI收录论文80多篇,*IEEE Transactions* 论文13篇,被SCI引用1800多次,H指数25,ESI高被引论文6篇;出版教材3部、学术专著3部;申请和授权国家发明专利20项。在非线性电路系统理论与技术,多涡卷和多翅膀等复杂拓扑结构混沌吸引子的生成、实现与应用,混沌电路与系统的设计,连续时间系统与切换系统的反控制,混沌密码理论与应用,多媒体混沌保密通信研发等方面取得了一系列有价值的成果。

前 言

本书以若干新型混沌电路与系统的设计原理及其在多媒体混沌保密通信中的应用与技术实现作为主要研究对象,归纳和总结了近年来作者在上述研究领域中取得的一系列科研成果。

本书第一部分重点叙述无简并高维超混沌系统的设计。无简并高维超混沌系统具体是指正李氏指数的个数 L^+ 能够达到可能的最大个数的一类高维超混沌系统。对于 n 维连续时间自治系统,设正李氏指数的个数为 L_c^+ , 负李氏指数的个数为 L_c^- , 零李氏指数的个数为 L_c^0 , 它们之间满足 $n = L_c^+ + L_c^- + L_c^0$ 。如果正李氏指数的个数达到了可能的最大个数,即满足 $L_c^+ = n - 2$, 则称为无简并高维连续时间超混沌系统。如果正李氏指数个数仅满足 $L_c^+ = n - 2 - d$, 则称为有简并高维连续时间超混沌系统,其中 $d > 0$ 为正李氏指数的简并度,是衡量正李氏指数个数减少的一个量化指标, d 越大,正李氏指数个数减少的程度也越大。对于 n 维离散时间自治系统,如果正李氏指数的个数达到了可能的最大个数,即满足 $L_d^+ = n$, 则称为无简并高维离散时间超混沌系统。但如果正李氏指数的个数仅满足 $L_d^+ = n - d$, 则称为有简并高维离散时间超混沌系统。通常情况下将连续系统和离散系统的正李氏指数是否发生简并的两种情况统称为无简并高维超混沌系统或有简并高维超混沌系统。对于连续时间混沌系统,必须有一个零指数和至少一个负指数,而离散系统则无此要求。

在简并无法消除的情况下,正李氏指数的个数不能随着系统维数的拓展而增加,这种单纯通过拓展系统维数而不能增加正李氏指数个数的高维系统设计方法并无实质性的研究意义。例如,一个 3 维离散混沌系统和一个 10 维离散混沌系统,如果这两个系统都只有一个正李氏指数,除维数上的差异之外,其他动力学性质并没有本质上的区别。但如果后者是无简并的,有 10 个正李氏指数,那么,两者的动力学性质将会出现较大的差异。这种差异具体体现在混沌的统计特性能否通过严格的 TestU01 测试和度量混沌系统统计特性的 KS 熵值大小。众所周知,这些指标是混沌加密算法安全性所需的必要条件。

无简并高维超混沌系统和有简并高维超混沌系统在维数相同的条件下,从动力学行为、混沌化的程度以及统计特性等多个方面来进行比较,它们之间都存在一定的差异。根据混沌理论,混沌系统的本质特征由混沌轨道的拉伸折叠变换决

定。只有一个正李氏指数的混沌系统,相邻轨道之间只有一个方向上的拉伸折叠变换和发散度(即指数分离度),而多个正李氏指数的混沌系统具有多个不同方向上的拉伸折叠变换和发散度。在混沌系统全局有界条件下,如果正李氏指数的个数 L^+ 越多,并且正李氏指数的值 LE^+ 越大,则系统具有更大强度的以及更多不同方向上的拉伸折叠变换,且整个系统的行为更复杂,从而导致无简并系统与有简并系统的动力学性质出现较大的差异。

为了解决正李氏指数发生简并的问题,本书第一部分重点介绍一种无简并高维超混沌系统设计的新方法,其适用范围是用一致有界的控制器对渐近稳定的标称系统实施反控制来构造无简并高维超混沌系统,通过控制器的闭环极点配置,使得当受控系统在两类鞍焦平衡点处对应的特征值的正实部个数分别满足 $n-1$ 和 $n-2$ 时,正李氏指数的个数能够达到 $L^+=n-2$ 。但在实际情况中,混沌系统的解 $\mathbf{x}(t)$ 遍历地分布在整个相空间中,设混沌系统的状态方程为 $\dot{\mathbf{x}}=f(\mathbf{x})$,对应的雅可比矩阵为 $\mathbf{J}(\mathbf{x})=\partial f(\mathbf{x})/\partial \mathbf{x}$,则雅可比矩阵 $\mathbf{J}(\mathbf{x})$ 也是状态变量 $\mathbf{x}$ 的函数,根据 $\mathbf{J}(\mathbf{x})$ 计算得到的特征值 $\lambda_i(\mathbf{x})$ ($i=1,2,\dots,n$)也是随着 $\mathbf{x}$ 的变化而变化的。仅考虑在两类鞍焦平衡点处对应的特征值的正实部个数分别满足 $n-1$ 和 $n-2$,虽然能解决维数不是很高情况下正李氏指数的无简并问题,但这只是一个必要条件,对于 $n>12$ 的高维系统,可以举出许多反例说明,即便满足这个必要条件,正李氏指数的个数也不一定能够满足 $L^+=n-2$,存在简并度 $d>0$ 的情况。但如果进一步考虑在控制器的一个周期内所有雅可比矩阵对应的平均特征值的正实部个数满足 $n-2$,就有可能进一步解决这个问题。

本书第二部分主要介绍满足 Devaney 混沌定义的整数域和数字域混沌系统的设计。改善或补偿数字域中混沌动力学退化的各种方法以及提出在数字域上构造混沌的新理论是近年来国内外关注的一个热点课题。目前,人们虽然采用了多种不同的改善或补偿数字域中混沌动力学退化的方法来研究这个问题,但更为重要的是另辟蹊径,提出在数字域上构造混沌的新理论与新方法来解决这个问题。

众所周知,混沌严格的数学定义,如 Devaney 混沌定义和 Li-Yorke 混沌定义等,都是针对“无限时间”和“无限精度”的条件而言的。混沌特性的数学定义都是渐近的,如李氏指数是用极限定义的、功率谱是用无穷傅里叶级数表示的。由于计算机和数字器件都是“有限精度”,人们无法实现严格数学定义的混沌,只能在“有限时间”和“有限精度”的“数字域”中实现“数字混沌”。在没有外部控制的条件下,对于一个数字域上的“自治混沌系统”本身而言,在整数域或数字域上的状态数为有限的情况下,它不可能具有数学意义上真正的混沌特

性。因此,解决问题的根本途径是必须引入某种外部的控制方法来解决数字域混沌的建模问题。例如,采用外部随机序列控制的单个随机位或多个随机位迭代更新的方法,构造满足 Devaney 混沌定义的 1 维和高维整数域或数字域混沌系统。

本书第三部分主要介绍多媒体混沌保密通信及其在 ARM、FPGA 和手机等硬件平台上的应用与技术实现。混沌密码不能总是停留在理论分析与设计的阶段,最终必须走向实际应用。这就需要解决两个重要的瓶颈问题:一是如何保证整个系统的安全性,二是如何获得硬件设计与实现的可行性。混沌密码的硬件设计与实现则是多媒体混沌保密通信走向实际应用的一项重要研究工作,其科学意义体现在“实践是检验真理的标准”。经过严格密码分析检测的混沌密码是否具有实用性,在很大程度上取决于该混沌密码设计算法在硬件实现方面的实际可行性,硬件实现是检验混沌密码合理性的重要实验手段和事实依据。

目前,国内外通常采用计算机数值仿真的方法来检验混沌密码算法和多媒体混沌保密通信。相对于数值仿真,硬件实现具有更大的技术难度,需要更高的实验手段。由于技术原因,现有的混沌密码及其保密通信方案,绝大多数仅给出了计算机数值仿真结果,而硬件实现结果的报道偏少。特别是,包括发送端、接收端和实际传输信道在内的整个多媒体混沌保密通信系统的硬件实现结果尤为偏少。文献统计分析表明,只有少量混沌加密相关论文附有硬件实现,这在很大程度上归咎于硬件实现通常比数值仿真技术难度更大。

与数值仿真不同,硬件实现还需要考虑整个系统的硬件资源、硬件实现条件、实际信道环境和实时性受限等一系列实际问题。现有许多混沌密码方案,尽管数值仿真容易实现,但在硬件资源和实时性受限的情况下,硬件实现则很难甚至无法获得实验结果。因此,人们需要统筹兼顾各方面的因素,提出既能保证安全性又能保证硬件实现的优选方案。在此基础上,进一步从硬件设计与实现的角度解决广域网传输的实时远程视频、语音、图像等多媒体混沌保密通信的应用问题,并针对不同应用业务、应用环境和应用平台进行优化和融合,使混沌密码从理论分析与设计走向实际应用。

多年来,作者的研究工作在很大程度上受益于国家和省部级科研项目的连续资助。借此机会,衷心感谢国家自然科学基金面上项目(61172023、61671161)、国家自然科学基金重点项目(61532020)、国家重点研发计划子课题(2016YFB0800401)的资助。衷心感谢香港城市大学陈关荣院士、中国科学院数学与系统科学研究院吕金虎研究员。作者在从事研究过程中得到了许多同行的支持和帮助,其中的许多结果是作者与合作者共同完成的,在此表示衷心感谢。衷心感谢家人的长期支

持和理解。衷心感谢科学出版社的大力支持和帮助。

由于作者水平有限，书中难免存在疏漏或不足之处，热诚期待广大同行和读者批评指正。

禹思敏

2017年10月于广州

目 录

前言

第 1 章 混沌的基本概念	1
1.1 混沌的基本特征	1
1.1.1 动力系统的基本概念	1
1.1.2 发现混沌之前人们对动力系统的认识	3
1.1.3 混沌的基本性质	4
1.2 基于反控制的“全局有界+正李氏指数”混沌的生成方法	11
1.2.1 基于反控制的无简并高维连续时间超混沌系统的设计	13
1.2.2 基于反控制的无简并高维离散时间超混沌系统的设计	14
1.3 混沌的基本定义	15
1.3.1 Li-Yorke 混沌定义	15
1.3.2 Devaney 混沌定义	18
1.3.3 有关混沌定义的几点说明	19
1.4 通向混沌的道路	20
1.4.1 倍周期分岔道路	20
1.4.2 阵发混沌道路	21
1.5 混沌动力系统的分类与表示方法	22
1.5.1 混沌动力系统的分类	22
1.5.2 相图、分岔图和迭代图	23
1.5.3 自治系统与非自治系统	26
1.5.4 保守系统与耗散系统	27
1.6 拓扑共轭	28
1.6.1 拓扑共轭的基本概念	28
1.6.2 拓扑共轭的意义	31
1.7 符号动力系统、帐篷映射、马蹄映射与 Henon 映射	31
1.7.1 符号动力系统	31
1.7.2 帐篷映射	35
1.7.3 马蹄映射	35
1.7.4 Henon 映射	43

1.8	Shilnikov 定理与 Melnikov 方法	46
1.8.1	Shilnikov 定理	46
1.8.2	Shilnikov 定理在切换系统中的应用	48
1.8.3	Melnikov 方法	52
1.9	动力系统的定性分析方法	55
1.9.1	平衡点	55
1.9.2	同宿轨道和异宿环	63
1.9.3	解的唯一性问题讨论	69
1.10	回归排斥子和 Marotto 定理	70
1.10.1	回归排斥子	70
1.10.2	Marotto 定理	71
第 2 章	李氏指数的数值计算方法与应用	79
2.1	离散时间混沌系统李氏指数数值计算的几个定义	79
2.2	基于 QR 正交分解的离散时间混沌系统李氏指数数值计算方法	81
2.3	基于 SVD 正交分解的离散时间混沌系统李氏指数数值计算方法	83
2.4	离散时间混沌系统李氏指数数值计算的几个应用实例	84
2.4.1	Henon 映射	84
2.4.2	基于 Chen-Lai 算法的 4 维离散时间混沌系统	86
2.4.3	基于 Wang-Chen 算法的 9 维离散时间混沌系统	87
2.5	连续时间混沌系统李氏指数数值计算的相关定义和 QR 正交分解算法	89
2.6	李氏指数与特征根之间定性关系的分析和讨论	96
2.7	高维连续时间系统反控制的李氏指数计算实例	98
2.7.1	6 维线性系统反控制的李氏指数计算	98
2.7.2	9 维线性系统反控制的李氏指数计算	101
第 3 章	离散时间混沌系统	104
3.1	矩阵范数	104
3.1.1	矩阵范数的定义	104
3.1.2	矩阵范数与谱半径的关系	105
3.2	圆盘定理与几个引理和推论	105
3.2.1	圆盘定理	105
3.2.2	几个引理和推论	107
3.3	离散时间系统的混沌判据	110
3.4	Chen-Lai 算法	110

3.4.1	Chen-Lai 算法的表述	110
3.4.2	基于 Chen-Lai 算法的 1 维线性离散时间系统的混沌化	111
3.4.3	基于 Chen-Lai 算法的 n 维线性离散时间系统的混沌化	112
3.4.4	基于 Chen-Lai 算法的 1 维非线性离散时间系统的混沌化	113
3.4.5	基于 Chen-Lai 算法的 n 维非线性离散时间系统的混沌化	115
3.5	Chen-Lai 算法的推广形式	117
3.5.1	模函数为正弦函数的 1 维线性受控系统	117
3.5.2	模函数为正弦函数的 n 维线性受控系统	118
3.5.3	模函数为锯齿波函数的 1 维线性受控系统	123
3.5.4	模函数为锯齿波函数的 n 维线性受控系统	124
3.6	Chen-Lai 算法总结	127
3.7	Wang-Chen 算法	128
3.7.1	Wang-Chen 算法的表述	128
3.7.2	基于 Wang-Chen 算法的 1 维非线性离散时间系统的混沌化	129
3.7.3	基于 Wang-Chen 算法的 n 维非线性离散时间系统的混沌化	130
3.7.4	基于 Wang-Chen 算法的 1 维线性离散时间系统的混沌化	131
3.7.5	基于 Wang-Chen 算法的 n 维线性离散时间系统的混沌化	132
3.8	Wang-Chen 算法的推广形式	133
3.9	Wang-Chen 算法总结	136
3.10	两个应用实例	137
第 4 章	具有多个正李氏指数的连续时间超混沌系统	139
4.1	问题的提出	139
4.2	超混沌系统设计的一种新方法	141
4.3	几个典型的超混沌系统设计实例	145
4.3.1	具有 2 个正李氏指数的 4 维超混沌系统	145
4.3.2	具有 3 个正李氏指数的 5 维超混沌系统	147
4.3.3	具有 4 个正李氏指数的 6 维超混沌系统	149
4.3.4	具有 5 个正李氏指数的 7 维超混沌系统	152
4.4	超混沌系统的电路设计与实现	155
第 5 章	耗散系统与保守系统中的无简并高维连续时间超混沌系统	159
5.1	问题的提出	159
5.2	n 维标称系统的设计	161
5.3	n 维耗散与保守超混沌系统的设计	163
5.3.1	n 维受控系统的设计	163

5.3.2	平衡点与雅可比矩阵	166
5.3.3	基于单参数控制的耗散系统与保守系统的统一模型	167
5.4	几个实例	167
5.4.1	具有 8 个正李氏指数的 10 维耗散超混沌系统	167
5.4.2	具有 9 个正李氏指数的 11 维耗散超混沌系统	171
5.4.3	具有 8 个正李氏指数的 10 维保守超混沌系统	174
5.4.4	具有 9 个正李氏指数的 11 维保守超混沌系统	177
第 6 章	无简并高维连续时间超混沌系统的平均特征值准则	181
6.1	问题的提出	181
6.2	简并问题的描述	183
6.3	构造无简并高维超混沌系统的平均特征值准则与步骤	186
6.3.1	几个相关的引理	186
6.3.2	基于对称正定矩阵的李氏指数计算公式	189
6.3.3	李氏指数与平均特征值之间的关系	190
6.3.4	构造无简并高维超混沌系统的平均特征值准则	192
6.3.5	无简并高维超混沌系统的设计步骤和参数选取算法	195
6.4	两个典型设计实例	202
6.4.1	设计具有 23 个正李氏指数的无简并 25 维超混沌系统	203
6.4.2	设计具有 24 个正李氏指数的无简并 26 维超混沌系统	204
第 7 章	具有多控制器的无简并高维连续时间超混沌系统	207
7.1	具有多控制器的无简并高维超混沌系统设计与平衡点分析	207
7.1.1	无简并高维超混沌系统的结构设计	207
7.1.2	无简并高维超混沌系统的平衡点分析	209
7.2	具有多控制器的无简并高维超混沌系统的设计准则与步骤	211
7.2.1	无简并高维超混沌系统的分析	211
7.2.2	具有多控制器的无简并高维超混沌系统设计准则	213
7.2.3	具有多控制器的无简并高维超混沌系统的设计步骤	214
7.3	两个典型的设计实例	215
7.3.1	具有 4 控制器的无简并 12 维超混沌系统	215
7.3.2	具有 3 控制器的无简并 13 维超混沌系统	217
第 8 章	可配置任意多个正李氏指数的连续时间超混沌系统	219
8.1	问题的提出	219
8.2	基于参数控制的 n 维耗散和保守超混沌系统的统一模型	220
8.2.1	统一模型的提出	220

8.2.2	耗散系统和保守系统	222
8.3	动力学分析	223
8.3.1	n 维耗散超混沌系统的情况	223
8.3.2	n 维保守超混沌系统的情况	228
8.3.3	耗散系统和保守系统平衡点和特征值分布的主要差异	230
8.3.4	正李氏指数个数与方程维数的关系	230
8.4	几个实例	233
8.4.1	18 维耗散超混沌系统	233
8.4.2	21 维耗散超混沌系统	235
8.4.3	21 维保守超混沌系统	236
第 9 章	单个随机位迭代更新的 1 维整数域混沌系统	239
9.1	基于单个随机位迭代更新的 1 维整数域混沌系统的基本概念	239
9.2	基于单个随机位迭代更新的 1 维整数域混沌迭代方程及其混沌存在性证明	241
9.2.1	度量空间 (X, d) 中映射 $G_f: X \rightarrow X$ 的数学表达式	241
9.2.2	基于单个随机位迭代更新的 1 维整数域混沌迭代方程的一般形式	242
9.2.3	度量空间 (X, d) 中距离的定义	242
9.2.4	单边无穷随机整数序列中 $\sigma: s \rightarrow s$ 的连续性	244
9.2.5	Devaney 混沌定义	245
9.2.6	周期点稠密的证明	245
9.2.7	拓扑传递性的证明	246
9.2.8	迭代的输入与输出的关系	248
9.3	基于单个随机位迭代更新的 1 维整数域混沌电路设计与硬件实现	250
9.3.1	均匀噪声信号生成电路	250
9.3.2	噪声电平转换电路	250
9.3.3	采样保持电路	251
9.3.4	译码电路	251
9.3.5	迭代方程的电路	253
9.3.6	D/A 转换电路	254
9.3.7	总电路设计与实现	255
第 10 章	多个随机位迭代更新的 1 维整数域混沌系统	257
10.1	具有多个随机位迭代更新的 1 维整数域混沌系统的基本概念	257
10.2	迭代图及其连通性	259
10.2.1	$N = 3$ 时的迭代图及其连通性	260

10.2.2	$N=4$ 时的迭代图及其连通性	261
10.3	强连通情况下混沌存在性的证明	263
10.4	具有多个随机位迭代更新的整数域混沌系统的统计特性	265
10.5	硬件设计与实现	267
10.5.1	电路设计	267
10.5.2	FPGA 设计与硬件实现	268
第 11 章	高维整数域和数字域混沌系统	270
11.1	高维整数域和数字域混沌系统中距离的定义与证明	270
11.1.1	距离的基本性质	270
11.1.2	向量范数及其三角不等式	270
11.1.3	高维整数域和数字域混沌系统中距离的定义	272
11.1.4	高维整数域和数字域混沌系统中距离的证明	272
11.2	高维整数域和数字域混沌系统的特点与定义	274
11.2.1	基本概念	274
11.2.2	1 维整数域的情况	276
11.2.3	1 维数字域的情况	277
11.2.4	m 维整数域的情况	278
11.2.5	m 维数字域的情况	280
11.3	m 维数字域混沌系统的描述	282
11.3.1	度量空间	282
11.3.2	高维整数域和数字域混沌系统的迭代方程	283
11.3.3	度量空间中的距离	284
11.4	实数域、整数域和数字域混沌系统的性能比较	285
11.5	数字域混沌系统状态空间的网络分析	287
11.6	m 维整数域混沌系统的混沌存在性证明	289
11.6.1	周期点稠密的证明	290
11.6.2	拓扑传递性的证明	292
11.7	m 维整数域混沌系统的李氏指数计算公式	294
11.7.1	迭代值和随机序列的十进制表示	294
11.7.2	$\partial g(y_1, y_2, \dots, y_m) / \partial y_k$ 的数学表达式	297
11.7.3	李氏指数的计算公式	298
11.7.4	讨论	299
11.8	高维整数域混沌系统的 FPGA 实现及其在图像保密通信中的应用	301
11.8.1	3 维整数域混沌系统的 FPGA 实现	301

11.8.2 基于 3 维整数域混沌系统图像保密通信系统的 FPGA 设计与实现	303
第 12 章 定点算法和状态机控制的通用 FPGA 混沌信号发生器	305
12.1 问题的提出	305
12.2 FPGA 技术与开发平台介绍	306
12.2.1 FPGA 简介	306
12.2.2 FPGA 的应用	307
12.2.3 FPGA 的开发流程	309
12.2.4 FPGA 开发工具	310
12.2.5 Virtex II Pro 硬件开发平台	312
12.3 连续时间混沌系统的 Verilog HDL 定点算法设计	315
12.4 基于 Verilog HDL 定点算法的状态分配与状态机控制方法	317
12.5 网格 9 涡卷 Chua 系统的 Verilog HDL 定点算法设计	318
12.6 网格 9 涡卷 Chua 系统的 FPGA 硬件实现	320
12.7 离散时间混沌系统的 Verilog HDL 定点算法设计	322
12.8 6 维离散时间混沌系统的 FPGA 硬件实现	325
第 13 章 视频混沌保密通信系统的设计与 FPGA 实现	329
13.1 问题的提出	329
13.2 离散时间混沌系统的设计	330
13.2.1 离散时间实数域混沌系统	330
13.2.2 离散时间整数域混沌系统	334
13.3 视频混沌保密通信系统的设计原理与硬件实现	340
13.3.1 视频混沌保密通信系统的设计原理	340
13.3.2 视频采集系统设计	347
13.4 发送端和接收端硬件系统的工作流程	354
13.5 系统的时序验证	356
13.6 FPGA 硬件实现	356
13.7 安全性能分析	358
13.7.1 统计分析	358
13.7.2 差分分析	359
13.7.3 NIST 测试	361
13.7.4 TestU01 测试	363
13.7.5 有效密钥失配的雪崩效应	372
13.7.6 密码分析的四种基本方法与安全性能的改进措施	374
第 14 章 广域网传输实时远程视频混沌保密通信与 ARM 实现	381
14.1 广域网的 TCP 和 UDP 传输原理	381

14.2	基于 TCP 的地址端口映射	383
14.2.1	路由器的设置	383
14.2.2	基于 TCP 的地址端口映射原理	385
14.3	视频格式及其转换	390
14.4	n 维混沌映射的构造及其基本性质	394
14.4.1	n 维混沌映射的构造	394
14.4.2	基本性质	397
14.5	像素位置置乱加密和解密算法	398
14.5.1	算法的工作原理	398
14.5.2	视频加密算法	401
14.5.3	视频解密算法	402
14.5.4	密钥空间的大小	402
14.6	像素值的混沌序列密码加密和解密算法	403
14.6.1	8 维离散时间混沌系统的设计	403
14.6.2	混沌序列密码算法设计	404
14.7	基于 ARM 平台的视频混沌保密通信系统设计	409
14.8	视频混沌保密通信的 ARM 硬件实现	412
第 15 章	多核多进程与 H.264 选择性加密的视频混沌保密通信	414
15.1	H.264 视频压缩编码技术	414
15.1.1	H.264 的编解码框架	414
15.1.2	H.264 的关键编码技术	416
15.2	H.264 编解码器的工作原理	418
15.2.1	H.264 编解码器的工作原理描述	418
15.2.2	H.264 编解码器的工作过程描述	419
15.2.3	当前帧为第 1 帧的情况	421
15.2.4	当前帧为第 2 帧的情况	421
15.2.5	帧内预测的四种模式	421
15.3	基于非线性标称矩阵的 6 维离散时间超混沌系统的设计	423
15.4	H.264 选择性加密与解密算法	426
15.4.1	H.264 选择性加密对象的选择	426
15.4.2	基于软件编码库的 H.264 选择性加密和解密算法	427
15.4.3	发送端的 H.264 选择性加密算法	427
15.4.4	接收端的 H.264 选择性解密算法	432
15.4.5	H.264 选择性加密和解密算法对视频文件的测试	436

15.5	视频混沌保密通信系统的设计	437
15.5.1	软硬件开发平台介绍	437
15.5.2	Linux 操作系统的多线程及多进程处理模式	438
15.5.3	视频混沌保密通信系统的软件整体设计方案	441
15.6	ARM 嵌入式平台上的硬件实现	445
15.6.1	通信系统硬件结构及开发环境的构建	445
15.6.2	广域网远程传输实验	446
15.7	安全性分析与测试	449
15.7.1	相关性分析	449
15.7.2	TestU01 统计测试	449
15.7.3	密钥失配灵敏度	450
15.7.4	破译密钥参数的复杂度	451
第 16 章	多核多线程与 H.264 编码后加密的视频混沌保密通信	452
16.1	H.264 硬件和软件编解码的视频混沌保密通信方案概述	452
16.2	三种加密方案耗时和传输帧率的测试及分析	455
16.3	方案 3 的具体设计	459
16.3.1	总体设计方案	459
16.3.2	混沌流密码的设计及其 H.264 的数据格式保护	461
16.3.3	位置置乱混沌加密的设计及其自适应内存选择	463
16.4	混沌流密码的设计	464
16.4.1	基于非线性矩阵的正李氏指数无简并的离散时间混沌系统设计	464
16.4.2	混沌流密码及其工作原理	467
16.5	硬件实验	470
第 17 章	视频混沌保密通信的手机实现	472
17.1	2 维双尺度和高维多尺度混沌映射及其算法	472
17.1.1	2 维双尺度混沌映射及其算法	472
17.1.2	高维多尺度混沌映射及其算法	475
17.2	基于 MJPG-Steamer 和 ARM 平台的视频混沌加密算法	476
17.3	基于 Android APP 和智能手机的视频混沌解密算法	479
17.4	广域网传输的实时远程视频混沌保密通信的手机实现	480
第 18 章	组播多用户和广域网传输的语音混沌保密通信	482
18.1	问题的提出	482
18.2	组播多用户 Wi-Fi 通信系统	483
18.2.1	组播多用户的工作原理	483