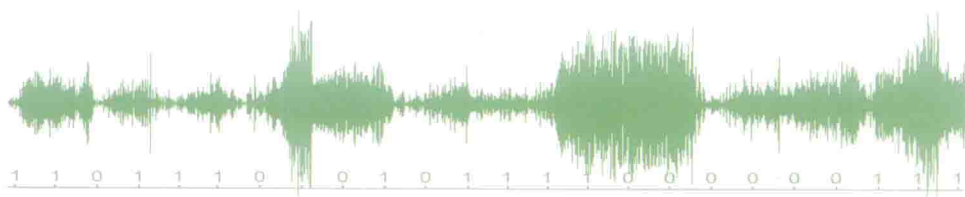


PRINCIPLE AND TECHNOLOGY OF CHAOTIC SECURE
COMMUNICATION

混沌保密通信 原理与技术

孙克辉 著
Sun Kehui



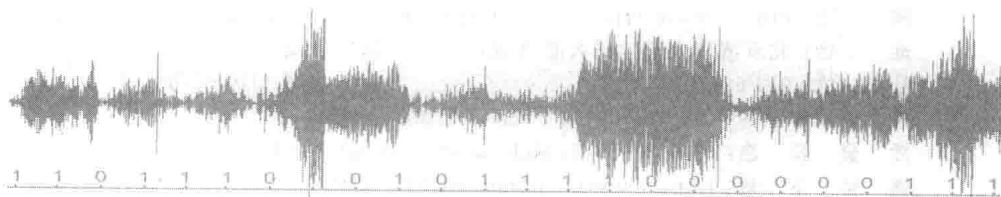
清华大学出版社

电子信息与电气

PRINCIPLE AND TECHNOLOGY OF CHAOTIC SECURE
COMMUNICATION

混沌保密通信 原理与技术

孙克辉 著
Sun Kehui



清华大学出版社

内 容 简 介

本书在阐述了混沌理论与应用研究进展、混沌研究分析方法和典型混沌系统的基础上,着重研究了混沌保密通信系统所涉及的基本技术与方法,包括混沌同步控制技术、混沌保密通信方案、混沌加密系统原理与设计、混沌电路的设计与实现技术等,作者还总结了分数阶混沌系统的分析方法、仿真技术与最新研究进展。

本书是作者近几年从事混沌理论及其保密通信应用研究的一个总结,书中包含作者十多年来的研究工作成果。

本书可作为电子信息工程、自动化等专业本科生与研究生的教材或参考书,或供理工科大学的师生阅读,也可供自然科学和工程技术领域的研究人员参考。

本书封面贴有清华大学出版社防伪标签,无标签者不得销售。

版权所有,侵权必究。侵权举报电话:010-62782989 13701121933

图书在版编目(CIP)数据

混沌保密通信原理与技术/孙克辉著.--北京:清华大学出版社,2015

电子信息与电气工程技术丛书

ISBN 978-7-302-38627-8

I. ①混… II. ①孙… III. ①混沌理论—应用—保密通信 IV. ①TN918.6

中国版本图书馆 CIP 数据核字(2014)第 276490 号

责任编辑:盛东亮

封面设计:李召霞

责任校对:焦丽丽

责任印制:王静怡

出版发行:清华大学出版社

网 址: <http://www.tup.com.cn>, <http://www.wqbook.com>

地 址:北京清华大学学研大厦 A 座 邮 编:100084

社总机:010-62770175 邮 购:010-62786544

投稿与读者服务:010-62776969, c-service@tup.tsinghua.edu.cn

质 量 反 馈:010-62772015, zhiliang@tup.tsinghua.edu.cn

课 件 下 载: <http://www.tup.com.cn>, 010-62795954

印 装 者:北京鑫海金澳胶印有限公司

经 销:全国新华书店

开 本:185mm×260mm

印 张:17.75

字 数:420 千字

版 次:2015 年 2 月第 1 版

印 次:2015 年 2 月第 1 次印刷

印 数:1~2000

定 价:49.00 元

产品编号:061153-01

自从1963年气象学家 Lorenz 发现混沌现象以来,混沌得到了广泛而深入的研究,混沌理论被誉为20世纪继相对论、量子理论后的第三大科学理论革命。特别是1990年美国海军实验室的 Pecora 和 Carroll 发现混沌同步后,便掀起了混沌保密通信的研究热潮,经过二十多年的研究和发展,混沌保密通信技术正成为信息技术领域中高新技术新的生长点。一方面,混沌的应用将不断促进人们对混沌本质的深刻认识;另一方面,混沌应用提出的新问题也将进一步引领混沌研究的深入。虽然混沌保密通信技术离实际应用还有较长的路要走,但混沌在保密通信领域的应用为我们展示了诱人的前景。

全书共分9章。第1章综述了混沌研究的历史,介绍了混沌发展中的重要人物与趣事,评述了混沌同步控制技术和混沌保密通信方法的研究进展;第2章阐述了非线性系统的混沌特性分析方法;第3章简略介绍了典型混沌动力学系统模型;第4章通过实例讨论了混沌系统的同步控制原理与技术;第5章重点讨论了基于混沌同步的保密通信技术与方案;第6章讨论了基于混沌序列的数据加密技术;第7章研究了基于混沌的音视频实时加密通信技术;第8章研究了分数阶混沌系统的最新研究进展、动力学特征分析与仿真方法;第9章研究了混沌电路的设计与实现技术。为了方便读者掌握书中的重要知识点,作者在每章的最后列出了为数不多的思考题,为教师安排课后训练提供便利。为了方便读者查找相关文献和将研究成果及时发表,特地将混沌研究领域期刊作为本书的附录A;此外,为了方便广大读者迅速掌握混沌研究方法,作者把课题组研究积累的有关分析程序进行了整理,作为本书的附录B。

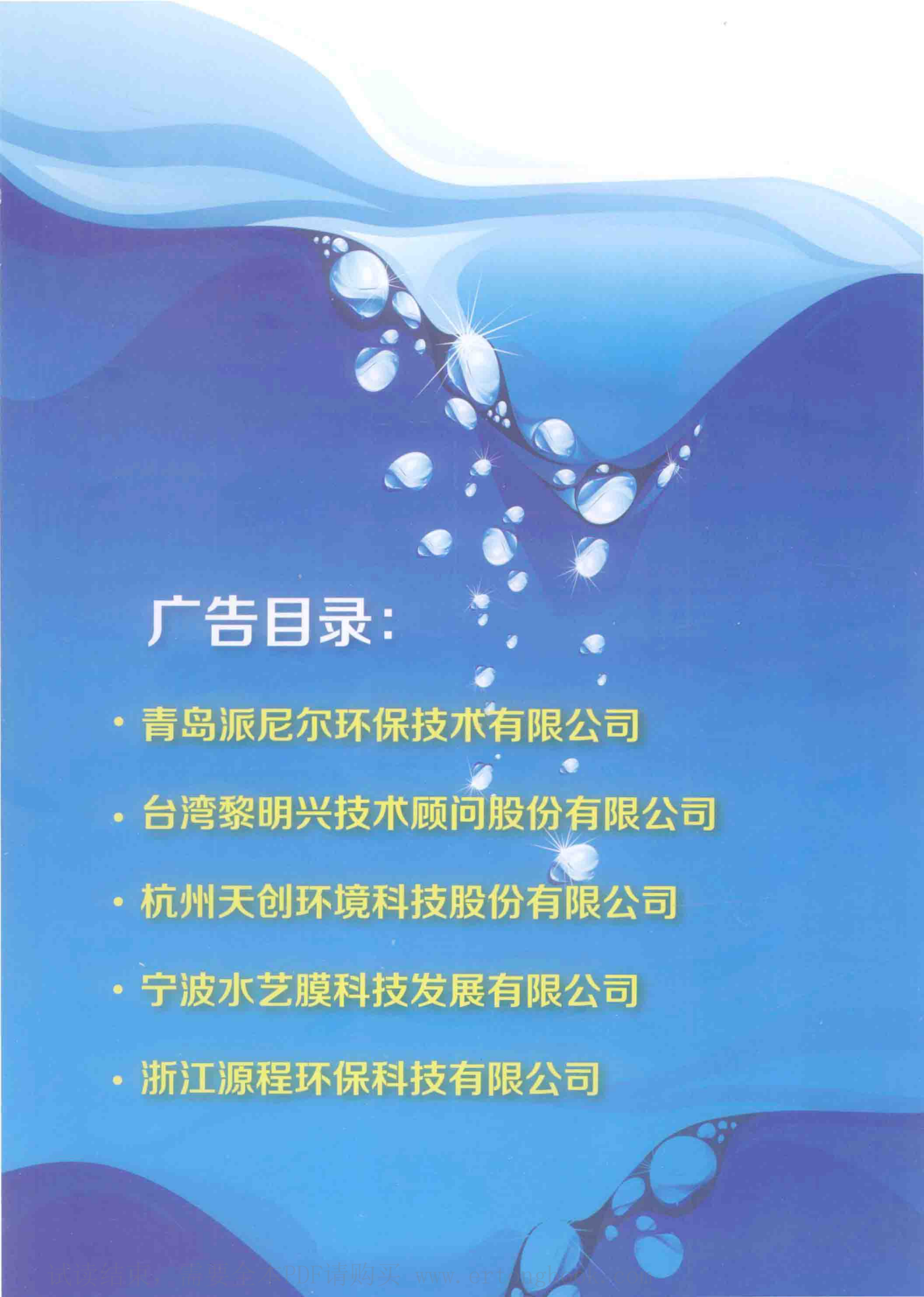
本书是作者在总结从事该领域研究成果的基础上,参阅大量国内外相关文献资料,经过反复修改而写成的。

在作者从事该领域的研究过程中,先后得到了美国威斯康星大学 J C Sprott 教授,华南理工大学丘水生教授,广东工业大学禹思敏教授,杭州电子科技大学王光义教授,中南大学张泰山教授、盛利元教授和朱从旭教授的指导和启发,作者对以上诸位先生的关怀和指导表示诚挚的谢意!在本书的编写过程中,还得到历届研究生牟俊、周家令、谈国强、任建、尚芳、王霞、包善琴、杨静利、程巍、刘璇、贺少波、王会海、王艳丽、汪艳、左婷和艾星星等同学的大力支持,在此表示衷心感谢!

由于作者水平有限,书中难免有不妥之处,敬望读者不吝赐教。

孙克辉

2015年1月于长沙



广告目录:

- 青岛派尼尔环保技术有限公司
- 台湾黎明兴技术顾问股份有限公司
- 杭州天创环境科技股份有限公司
- 宁波水艺膜科技发展有限公司
- 浙江源程环保科技有限公司

ISO9001认证企业 大型臭氧发生器制造工厂

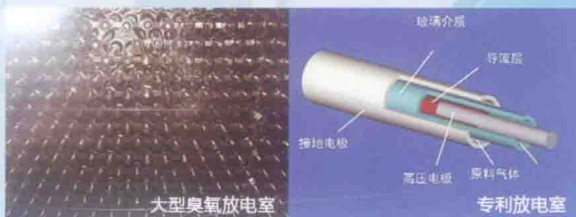
青岛派尼尔环保技术有限公司坐落于青岛市城阳区，是一家立足于臭氧发生器技术产品研发、生产制作的专业化生产工厂。

公司拥有大型臭氧发生器制造技术的专业人才，在臭氧发生器单元的技术研发、产品生产、系统调试以及售后服务等部门均为具有核心竞争力的技术团队，为臭氧发生器系统在用户现场稳定运行及服务做出保障。

公司所生产的臭氧发生器设计制造标准，严格依据中华人民共和国城镇建设行业标准CJ/T 322—2010《水处理用臭氧发生器》的标准，保证臭氧发生系统能够稳定的连续运行。

目前公司臭氧发生器的制造能力为单台100kg/h，臭氧系统的运行参数均达到国际先进水平。

我们会不断的提高公司团队的核心竞争力；我们能够提供优质的臭氧系统为用户服务；我们终将致力于我们的环保产业！



全国服务电话：400-0532-608

青岛派尼尔环保技术有限公司
中国·山东 青岛市城阳区东蓝家庄工业园

电话：+86(532)89080190 / 80965895

总经理：陈勇

手机：13356852676 / 15863088188

传真：+86(532)84937068

网址：www.pioneerrep.com

邮箱：pioneer@pioneerrep.com

江浙沪总代理：浙江源程环保科技有限公司

http://www.zjyckj.com

咨询热线：0579-85628555

新颖脱氮技术

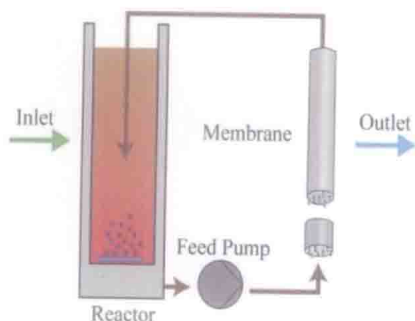
红菌-厌氧氨氧化

SNAD, Greater Energy Savings for High Strength Ammonia Wastewater

黎明興技術顧問股份有限公司

www.leaderman.com.tw

MBR 结合红菌技术



- 高脱氮效率
- 占地小
- 节省 60%运行成本
- 适用性广
- 可既有设备提标改造
- 温室气体减排 80%
- 无需额外投加碳源
- 低污泥产量



TianChuang
天创

改善 水生态 循环 水资源
创造 绿色健康财富

关于天创 >>

杭州天创环境科技股份有限公司成立于1997年，总部位于杭州，是一家集科研、设计、制造、销售、服务和系统集成于一体的高新技术企业。以“改善水生态，循环水资源，创造绿色健康财富”为使命，致力于膜分离技术在工业水处理领域的研究和应用，为客户提供水资源循环利用的整体解决方案。

专注膜分离技术的研发和应用

国内极少数能开发、生产、销售全系列水处理膜产品的厂家之一

MBR工艺的优点：

- 出水水质好，膜过滤孔径小于0.4微米，能够高效的进行固液分离，MBR产水水悬浮物和浊度 < 1NTU；
- 抗负荷冲击能力强，MBR对微生物的高效截留，使的内微生物浓度高，难降解的物质在反应器中不断反应、降解。
- MBR系统省去了二沉池单元，因此可大幅减少污水处理占地面积，节省土建投资；
- MBR工艺产生污泥量少，污泥性质稳定，该工艺的污泥量是传统污水处理工艺的1/3；
- MBR系统实现PLC/DCS控制，操作、维护管理便简。

天创自主开发的MBR膜设备特点：

【优越的膜材料性能】：PVDF 膜丝柔韧性高、不易断丝、化学稳定性好

【浸没式膜，高品质过滤】：能应付高悬浮物与有机物的进水，对水质不稳定的进水有较强的抗冲击能力

【模块化膜组件，方便扩展】：膜组件装配式设计，拆装、维护方便灵活

案例展示 >>



天创服务号

杭州天创环境科技股份有限公司

地址：杭州市余杭区仓前工业园海曙路16号

电话：0571-8698 9170/9172

欢迎登陆天创官方网站：<http://www.hztianchuang.com>查询相关信息

邮编：311121

传真：0571-8862 0836

水艺 SHUIYI

Reinforced PVDF Hollow Fiber Membrane Modules-MBR

MBR增强型中空纤维 帘式膜组件



SMU-30A

SMU-18A

产品简介

水艺MBR用中空纤维帘式膜组件采用编织管增强型PVDF中空纤维膜，具有高强度、高亲水性、小孔径等特点，耐污染性强，产水水质稳定。以水艺MBR中空纤维帘式膜组件为基础的膜装置结构紧凑，填充密度大，安装使用方便。

水艺MBR膜系统用于市政及工业污水处理，可以避免传统沉降分离工艺中的悬浮物泄露问题，并去除大肠杆菌、隐孢子虫等微生物，膜系统产水可直接或者添加少量消毒剂作为中水回用。

产品特点

机械强度高，不断丝

采用编织管增强型结构，膜丝断裂力达300N以上，可以有效防止组件长期运行中的膜丝断裂问题。

剥离强度高，不脱皮

水艺中空纤维膜的分离层与编织管支撑层结合紧密，瞬时剥离强度可达700 kPa以上，可以经受频繁的反冲洗运行，不会出现中空纤维膜脱皮现象，系统运行稳定。

膜孔径小且分布均匀，产水优质

水艺MBR膜组件采用PVDF超滤膜，平均孔径约0.06 μm ，孔径分布均匀，可有效去除悬浮物、细菌、胶体、病毒等污染物，出水水质优良。

高通量，过滤压力小，节省能耗

水艺PVDF中空纤维膜纯水通量达1500 $\text{L}/\text{m}^2 \cdot \text{h} \cdot 0.1\text{MPa}$ ，具有低压大通量的特点。根据原水水质情况，跨膜压差约10~50 kPa，典型运行通量可达到15~40 $\text{L}/\text{m}^2 \cdot \text{h} \cdot 0.1\text{MPa}$ 。

膜亲水性强，抗污染性能好

基于水艺专有的亲水改性生产工艺，水艺增强型PVDF中空纤维膜具有永久亲水性，大大提升了膜的抗污染性，减少了清洗要求，延长了膜的使用寿命。

耐药性好，易于清洗恢复

采用独特配方的PVDF膜材质，在保证优异亲水性的同时有很好的耐药性，使得膜元件可以适用于条件苛刻的工业污水处理环境，可以使用氧化剂、无机酸或有机酸清洗，保证膜系统的稳定运行。

模块化设计，安装简单

水艺MBR膜系统采用模块化方式设计，便于各种大型污水处理工程的改建、扩建分期进行，土建可以按最终的设计流量进行，而膜系统的膜元件数量可根据工程要求的处理量分阶段增加。

应用领域

市政污水处理
工业污水处理
中水回用
高浓度有机废水处理
零排放系统

我们的产品
即将更名为
Uniqua Membrane
敬请关注！

宁波水艺膜科技发展有限公司

Ningbo Shuiyi Membrane technology Development Co., Ltd

地址：宁波市杭州湾新区兴慈一路368号

邮编：315336

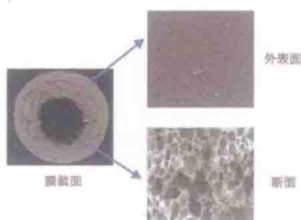
电话：0574-63937223

传真：0574-63073633

www.shuiyigroup.com



电镀下膜丝截面图



MC-100系列中空纤维膜专用清洗化学剂

Membrane Cleaning Specialist



MC-100系列



清洗前



清洗后

主要成分：日本品质MC-100系列食品添加剂等专用药剂组成；

使用方法：5~10%浓度，25℃以上浸泡3~6个小时零推荐；

回复效果：90%以上回复率（药洗后，无需特殊排水处理）；

适用范围：PVDF, PE, PVC, PES, PS等水处理中空纤维膜；

工程业绩：防止膜的永久堵塞，（日本某企业用户）连续使用，
可以使膜丝的寿命达10年之久。



浙江源程环保科技有限公司

ZHEJIANG WATER SOURCE PROGRAM GREEN ENVIROTECH CO. LTD

<http://www.zjyckj.com/>

咨询热线：0579-85628555

18072350101@163.com

第 1 章 绪论	1
1.1 线性、非线性与混沌	1
1.2 混沌研究历程	2
1.3 混沌发展中的重要人物与趣事	4
1.4 混沌的定义与特征	8
1.5 混沌同步方法研究综述	9
1.5.1 现有混沌同步方法及其特点	9
1.5.2 其他同步方法与问题	11
1.6 混沌在保密通信中的应用研究综述	12
1.6.1 混沌模拟通信	12
1.6.2 混沌数字通信	13
1.6.3 基于混沌序列的加密通信	14
1.7 混沌研究方法 with 主要研究内容	14
思考题	15
参考文献	16
第 2 章 非线性系统的混沌特性分析方法	19
2.1 相轨线(相图)分析法	19
2.2 自功率谱分析法	20
2.3 Poincaré 截面法	21
2.4 Lyapunov 特征指数法	23
2.4.1 Lyapunov 指数的定义	23
2.4.2 Lyapunov 指数谱	24
2.4.3 Lyapunov 指数的物理意义	24
2.4.4 条件 Lyapunov 指数	25
2.5 分数维分析法	26
2.6 0-1 测试法	26
2.6.1 0-1 测试算法	27
2.6.2 改进的 0-1 测试算法	27
2.6.3 0-1 测试法应用	28
2.7 分频采样法	29
2.8 赝相空间法	30
2.9 复杂度测度法	30
2.9.1 谱熵复杂度算法	31

目录

2.9.2 C_0 复杂度算法	32
思考题	33
参考文献	33
第3章 典型混沌动力学系统	35
3.1 离散混沌映射系统	35
3.1.1 Logistic 映射	35
3.1.2 Tent 映射	37
3.1.3 Hénon 映射	37
3.1.4 TD-ERCS 映射	38
3.2 连续混沌系统	39
3.2.1 Duffing 振子	39
3.2.2 van der Pol 振子	40
3.2.3 Lorenz 系统	41
3.2.4 Rössler 系统	41
3.2.5 蔡氏电路	42
3.2.6 Chen 系统	45
3.2.7 Lü 系统	47
3.2.8 统一混沌系统	47
3.2.9 简化 Lorenz 系统	49
3.2.10 新混沌系统的建议标准	53
3.3 超混沌系统	53
3.3.1 Rössler 超混沌系统	53
3.3.2 Chen 超混沌系统	54
思考题	55
参考文献	55
第4章 混沌系统的同步原理与方法	57
4.1 混沌同步定义	57
4.2 混沌同步系统的性能指标	58
4.3 反馈同步控制原理与性能	59
4.3.1 连续混沌系统的多变量驱动反馈同步	59
4.3.2 离散混沌系统的线性与非线性反馈同步	62
4.4 基于 Pecora-Carroll 同步判据的参数自适应同步	69
4.4.1 自适应同步原理	69
4.4.2 控制律与控制参数的选择	70

4.4.3	控制常数边界与范围的确定	70
4.4.4	系统仿真与结果讨论	71
4.5	基于 Lyapunov 稳定性理论的自适应同步	73
4.5.1	确定参数的自适应同步	73
4.5.2	不确定参数的自适应同步	74
4.6	间歇反馈同步	77
4.6.1	不同系统间的间歇同步	77
4.6.2	同步仿真与性能分析	79
4.7	基于状态观测器方法的同步	81
4.7.1	状态观测器设计原理	81
4.7.2	统一混沌系统的状态观测器设计	82
4.7.3	仿真与结果讨论	83
4.8	混沌观测器同步	84
4.8.1	混沌观测器设计原理	84
4.8.2	统一混沌系统的混沌观测器设计	85
4.8.3	同步仿真与性能分析	86
4.9	投影同步	88
4.9.1	比例投影同步原理与仿真	89
4.9.2	函数投影同步原理与仿真	91
4.9.3	自适应函数投影同步与仿真	94
4.10	混沌同步存在问题与研究热点	100
	思考题	100
	参考文献	100
第 5 章	基于混沌同步的保密通信技术	102
5.1	混沌掩盖通信	103
5.2	混沌键控通信	106
5.2.1	COOK	106
5.2.2	CSK	107
5.2.3	DCSK	112
5.2.4	FM-DCSK	112
5.2.5	QCSK	113
5.3	混沌调制通信	116
5.4	混沌扩频通信	118
5.4.1	混沌直接序列扩频通信原理	119

目录

5.4.2 混沌扩频码的产生	120
5.4.3 多用户混沌扩频系统仿真模块设计	122
5.4.4 基于 Rake 接收的多用户混沌扩频系统的设计与仿真	126
5.4.5 基于 Rake 接收的多用户混沌扩频系统的性能分析	128
思考题	130
参考文献	130
第 6 章 基于混沌序列的数据加密技术	132
6.1 混沌密码学	132
6.1.1 传统密码体制	132
6.1.2 混沌密码与传统密码的关系	133
6.1.3 混沌序列加密原理	134
6.2 基于混沌序列的数据加密算法	135
6.2.1 混沌加密算法的基本要求	135
6.2.2 Logistic 混沌系统及其统计特性	137
6.2.3 混沌序列加密模型与算法	137
6.2.4 基于混沌序列的数据加密算法实现	138
6.2.5 系统调试与性能分析	140
6.3 基于混沌映射的二值水印图像加密算法	143
6.3.1 混沌伪随机序列发生器的改进	143
6.3.2 基于 TD-ERCS 混沌映射的二值水印图像加密算法	144
6.3.3 加密算法的性能分析	145
6.4 基于混沌映射和小波变换的彩色图像水印算法	148
6.4.1 小波变换算法及其应用	148
6.4.2 水印嵌入与提取算法的设计与实现	152
6.4.3 数值仿真与性能分析	155
6.5 混沌图像加密算法	160
6.5.1 混沌图像加密技术	160
6.5.2 混沌图像加密新方案	162
思考题	167
参考文献	167
第 7 章 音视频混沌加密通信技术	170
7.1 实时语音加密通信原理	170
7.1.1 数字加密通信系统原理	170
7.1.2 实时语音加密通信系统	171

7.1.3 密码同步技术	172
7.2 实时数据流加密算法	173
7.2.1 3DES 加密算法	173
7.2.2 3DES 与混沌映射相结合的加密算法	174
7.2.3 网络同步方法研究	175
7.2.4 实时语音加密通信系统的安全性能分析	177
7.3 实时语音加密通信系统的实现	178
7.3.1 实时语音加密通信系统结构	178
7.3.2 实时传输协议及其数据结构	179
7.3.3 基于自适应通信环境的 RTP 协议实现	180
7.3.4 系统调试与性能测试	182
7.4 基于混沌序列的 MPEG 视频加密算法	183
7.4.1 混沌加密系统的设计原则	184
7.4.2 MPEG 视频数据加密原理与步骤	185
7.4.3 基于混沌的流密码设计	186
7.4.4 基于混沌的置乱算法设计	188
7.4.5 加密实验与效果分析	188
7.4.6 MPEG 视频加密系统性能分析	189
7.5 基于混沌的 H.264 视频加密算法	191
7.5.1 基于 TD-ERCS 的混沌流密码的构造	191
7.5.2 H.264 视频加密方案	192
7.5.3 视频加密性能分析	194
思考题	195
参考文献	195
第 8 章 分数阶混沌系统的分析与仿真	197
8.1 分数阶混沌系统的研究现状	197
8.2 分数阶微积分定义及其物理意义	199
8.3 分数阶混沌系统的求解方法	201
8.3.1 分数阶混沌系统的频域近似求解方法	201
8.3.2 分数阶混沌系统的时域近似求解方法	205
8.4 分数阶混沌系统仿真方法	209
8.4.1 分数阶混沌系统动态仿真方法	209
8.4.2 分数阶混沌系统电路仿真方法	211
8.4.3 分数阶混沌系统数值仿真方法	213

目录

8.4.4	仿真方法对比与特点分析	215
8.5	基于频域法的分数阶统一系统动力学特性分析	216
8.5.1	分数阶统一混沌系统模型	216
8.5.2	分数阶统一混沌系统的动态仿真	217
8.5.3	参数固定时分数阶统一系统的动力学特性	219
8.5.4	参数变化时分数阶统一系统的动力学特性分析	221
8.6	基于时域法的分数阶非耗散 Lorenz 系统的动力学特性	223
8.6.1	分数阶非耗散 Lorenz 系统模型	223
8.6.2	分数阶非耗散 Lorenz 系统的混沌特性	224
8.6.3	系统控制参数 R 不同时的分岔特性分析	224
8.6.4	分数阶阶数不同时的分岔特性	225
8.6.5	方程微分阶数不同时的分岔特性	227
	思考题	228
	参考文献	228
第 9 章	混沌系统的仿真与硬件实现	231
9.1	混沌系统的动态仿真	231
9.1.1	Simulink 动态仿真步骤	231
9.1.2	仿真结果分析与性能改善	232
9.2	混沌系统的电路仿真	233
9.3	混沌模拟电路设计	233
9.3.1	混沌模拟电路设计步骤	233
9.3.2	混沌电路模块化设计	234
9.3.3	混沌电路的基本组成及元器件选型	235
9.4	混沌电路的改进型模块化设计	237
9.4.1	基于 OA 器件的多涡卷 Jerk 电路设计	237
9.4.2	基于 CC 器件的多涡卷 Jerk 电路设计	238
9.4.3	多涡卷 Jerk 电路实现	240
9.5	混沌系统的 DSP 设计与实现	241
9.5.1	混沌系统的 DSP 实验平台	241
9.5.2	整数阶混沌系统的 DSP 实现	244
9.5.3	分数阶混沌系统的 DSP 实现	245
	思考题	247
	参考文献	247
附录 A	混沌研究领域的主要学术期刊	249
附录 B	混沌特性分析 MATLAB 源程序	250

经过几十年的发展,人们对混沌已不再陌生,但如何正确认识、理解和研究混沌及其应用,仍然是学界的主要任务。众所周知,混沌是非线性的,而我们所拥有的和熟知的知识是线性的,它们是什么关系呢?讨论就先从这里开始。

1.1 线性、非线性与混沌

“线性”与“非线性”常用于区别函数 $y=f(x)$ 对自变量 x 的依赖关系,线性函数即一次函数,其图像为一条直线;其他函数则为非线性函数,其图像不是直线。更具体地说,线性是指量与量之间按比例、成直线的关系,在空间和时间上代表规则和光滑的运动;而非线性则指不按比例、不成直线的关系,代表不规则的运动和突变,如两个眼睛的视敏度是一个眼睛的几倍?很容易想到的是两倍,可实际是 6~10 倍,这就是非线性,即 $1+1$ 不等于 2。

非线性关系虽然千变万化、较为复杂,但还是具有某些不同于线性关系的共性。线性关系是互不相干的独立贡献,而非线性则是相互作用,而正是这种相互作用,使得整体不再是简单地等于部分之和,而可能出现不同于“线性叠加”的增益或亏损。如激光的产生就是非线性的,当外加电压较小时,激光器犹如普通电灯,光向四面八方散射;而当外加电压达到某一定值时,会突然出现一种全新现象:受激原子好像听到“向右看齐”的命令,发射出相位和方向都一致的单色光,这就是激光。又如线性关系保持信号的频率成分不变,而非线性则使频率结构发生变化,只要存在非线性,哪怕是任意小的非线性,就会出现和频、差频、倍频等成分。非线性是引起行为突变的原因,对线性的微小偏离,一般并不引起行为突变,而且可以从原来的线性情况出发,用修正的线性理论去描述和理解;但当非线性达到一定程度时,系统行为就可能发生突变。非线性系统往往在一系列参量阈值上发生突变,每次突变都伴随着某种新的频率成分,系统最终进入混沌状态。

从非线性的上述特点可以看到,若系统出现混沌现象,则系统必定是一个非线性系统。非线性系统进入混沌状态是一种突变行为,如何判断系统是否进入混沌状态,即如何区分系统是否呈现长周期现