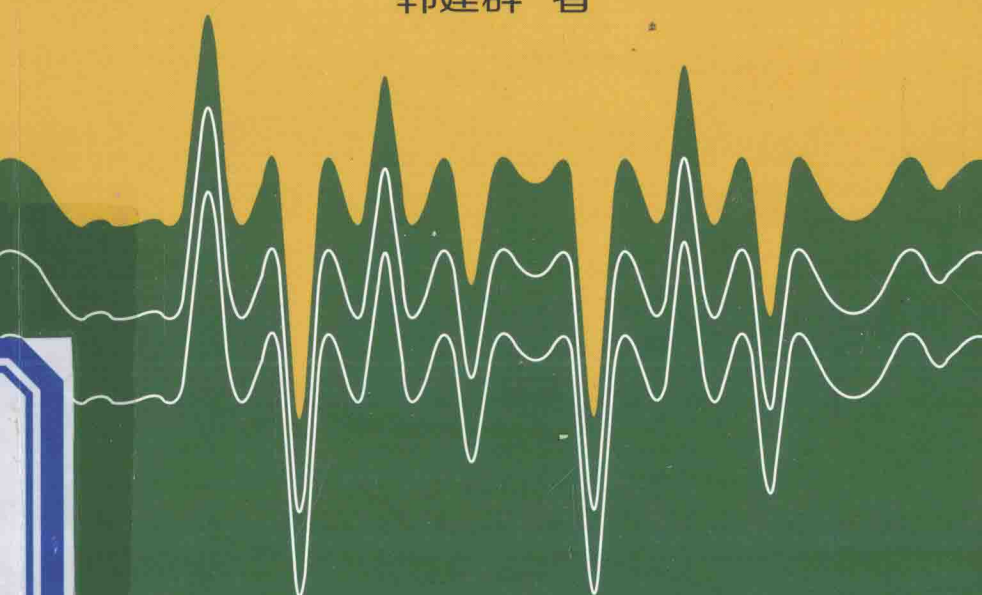
本书由国家自然科学基金项目（No.51277011）资助出版

混沌保密通信及其弱信号检测特性应用研究

韩建群 著



大连海事大学出版社

本书由国家自然科学基金项目（No.51277011）资助出版

混沌保密通信及其弱信号检测特性应用研究

韩建群 著

大连海事大学出版社

图书在版编目（CIP）数据

混沌保密通信及其弱信号检测特性应用研究 / 韩建群著. — 大连：大连海事大学出版社，2013.3

ISBN 978-7-5632-2850-8

Ⅰ. ①混… Ⅱ. ①韩… Ⅲ. ①混沌理论—应用—保密通信—研究 ②混沌理论—应用—信号检测—研究 Ⅳ. ①TN918.6 ②TN911.23

中国版本图书馆 CIP 数据核字（2013）第 050834 号

大连海事大学出版社出版

地址：大连市凌海路 1 号 邮编：116026 电话：0411-84728394 传真：0411-84727996

http://www.dmupress.com E-mail: cbs@dmupress.com

大连美跃彩色印刷有限公司印装 大连海事大学出版社发行

2013 年 3 月第 1 版 2013 年 3 月第 1 次印刷

幅面尺寸：140 mm×203 mm 印张：5.5

字数：118 千 印数：1～500 册

责任编辑：姜建军 华云鹏 版式设计：晓 江

封面设计：王 艳 责任校对：华云鹏

ISBN 978-7-5632-2850-8 定价：20.00 元

前 言

混沌理论是继相对论、量子力学后，20世纪人类认识世界和改造世界的最富有创造性的科学领域的第三次大革命。近年来，作为非线性科学重要内容的混沌理论，在混沌应用技术方面取得了长足进步。混沌理论与计算机科学理论等领域相结合，使人们对一些久悬未解的基本难题的研究取得了突破性进展，在探索、描述及研究客观世界的复杂性方面发挥了巨大作用。其中，关于混沌系统的控制及在保密通信中的应用问题更是引起了人们的广泛关注，并且日益成为研究的热点和难点，相关的文献和成果，也在不断丰富之中。混沌用于强噪声背景下的有效信号检测是一个热点课题，其应用领域包括气象学、生物学、电子学、自动控制、数量经济学、地学和军事学等。

本书是作者几年来就混沌系统在混沌控制、混沌保密通信以及混沌微弱信号检测等方面从事科研工作的基本总结。对该研究工作提供支持的科研项目是国家自然科学基金项目“飞机整体驱动发电机内部故障特征提取及诊断方法研究（项目编号：51277011）”，辽宁省教育厅科学研究项目“基于Duffing混沌系统的数字信号解调器研究（项目编号：L2010005）”。这些项目的研究成果发表在《电子学报》、《电子与信息学报》、《系统工程与电子技术》、《计算机科学》等学术刊物上，经进一步总结提炼构成本书的主要内容。

本书共分7章，第1章回顾了混沌理论的发展历程和混沌运

动的独特特征，简要综述混沌保密通信及其弱信号检测特性研究的现状。第2章介绍了混沌的数学定义和混沌通信研究中几种常用的动力系统，并且着重阐述了混沌吸引子的特征量——李雅普诺夫指数和分数维。第3章论述了混沌系统的控制和同步过程，首先介绍了混沌控制的OGY控制方法、自适应控制方法和滑模变结构方法，提出了Lorenz混沌系统滑模控制简化方法；然后论述了混沌同步的定义和驱动—响应同步、主动—被动同步及观测器同步等几种方法，最后基于模糊控制理论分析了时变信道混沌同步通信的方法。第4章首先介绍了传统的掩盖通信原理，然后通过对二维Duffing混沌系统进行变量分解建立了三维Duffing系统数学模型，并证明了Duffing系统实现掩盖通信方法，最后提出了利用数字信道实现混沌掩盖通信的方法，并给出了数学仿真结果。第5章对当前最有发展前途的混沌差分键控通信进行了阐述，详细介绍常规的差分混沌移相键控（DCSK）和调频差分混沌移相键控（FM-DCSK）方法，并在此基础上论述改进的FM-DCSK，得到了提高FM-DCSK调制传输效率方法。第6章对混沌系统用于强噪声背景下信号检测进行理论分析，研究断续正弦信号参数占空比和角频率对Duffing系统检测状态的影响，并利用Duffing混沌系统实现了移频键控信号检测。最后通过分析Duffing混沌系统阻尼参数对断续正弦信号检测的影响，证明了通过增加阻尼参数值可缩小断续正弦信号频率范围，从而提高系统的检测精度的方法。第7章结论与展望，总结了本文的主要

创新点以及未来混沌通信研究的发展方向。

在本书的写作过程中，得到大连海事大学朱义胜导师的指导，为今后的学术发展打下了坚实的基础。另外，渤海大学工学院于忠党教授、伦淑娴教授、巫庆辉副教授、韩志艳博士、王巍博士等提出了许多有价值的建议，郭艳东老师、孙宏老师在手稿书写、整理、仿真实验和校对书稿等方面做了大量的工作，在此向他们表示由衷的感谢。

由于作者水平有限，书中不足之处在所难免，热诚欢迎读者与同行不吝赐教。

韩建群

2012 年 11 月于渤海大学

目 录

第1章 绪 论

1.1 混沌概述

所谓混沌，粗略地说是一种在确定系统中所表现出来的类似随机而无规则运动的动力学行为。通过对混沌确定系统的内在随机现象研究有助于人们对客观世界的正确认识和把握，揭示自然界及人类社会中普遍存在的复杂性，反映世界上无序和有序之间、确定性与随机性之间的辩证统一关系。目前，研究人员用已有的混沌理论成功地解释了许多原来无法理解的现象。

最先对混沌的研究可以追溯到19世纪，公认为真正发现混沌的第一位学者是法国数学、物理学家H. Poincare，他是在研究太阳系的三体运动时发现混沌的。20世纪70年代，这是混沌科学发展史上光辉灿烂的年代，混沌学作为一门新兴的学科正式诞生了。1971年，法国的数学物理学家D. Ruelle和荷兰的F. Takens发表了著名论文《论湍流的本质》，在学术界首次提出用混沌来描述湍流形成机理的新观点，并为耗散系统引入了“奇怪吸引子”这一概念。进入20世纪80年代，混沌研究已发展成为一个具有独特的概念体系和方法论框架的新学科。如今，混沌的发现被认为是20世纪物理学三大成就之一，可以说“相对论消除了关于绝对空间与时间的幻想；量子力学消除了关于可控测量过程的牛顿式的梦；而混沌则消除了拉普拉斯关于决定论式可预测性的幻想”。

国家自然科学基金项目（No. 51277011）资助出版

混沌研究主要有三个方面的内容，一是研究系统从有序到混沌态的过渡，即探讨系统进入混沌状态的机制与途径；二是研究混沌中的有序行为，即探讨混沌中的普适性和标度不变性；三是研究如何有效地控制混沌或主动地利用混沌。

混沌运动是确定非线性系统所特有的复杂运动形式，出现在某些耗散系统、不可积Hamilton保守系统和非线性离散映射系统中。从运动轨迹上看，混沌是一种不稳定的有限定常运动，即为全局压缩和局部不稳定运动，或除了平衡、周期和准周期以外的有限定常运动，因此混沌运动的两个主要特征是不稳定性和有限性。

混沌运动的独特特征主要有：

（1）动力学特性极端敏感地依赖于初始条件。这是混沌区别于其他运动体制的本质特征，这一特征意味着混沌是不可预测的。这里所说的不可预测性是指混沌系统长期行为是不可预测的，而短期行为是完全确定的。

（2）确定性方程中的内在随机性。凡随机现象都表现出某些统计确定性，遵循统计规律，混沌运动都表现出某种统计确定性；然而，混沌运动所产生的随机性与通常所说的随机系统中的随机性有着本质的区别，通常所说的随机性是通过运动方程中加入随机外作用力或随机系数或随机初始条件等三种方式表现出来的，应称为外在随机性。混沌系统的动力学方程是确定的，既没有随机外力，也没有随机系数或随机初值，随机性完全是在系统自身演化的动力学过程中由于内在非线性机制作用而自发产生出来的，是确定的。

（3）普适性。所谓普适性，是指系统运动状态在趋向混沌

国家自然科学基金项目（No. 51277011）资助出版

时所表现出来的共同特征，它不随着具体的系数以及系统的运动方程而变化。通常提到的普适性有两种，即结构的普适性和测度的普适性。前者是指趋向混沌过程中轨线的分岔情况与定量特征不依赖于该过程的具体内容，只与它的数学结构有关；后者是指同一映象或迭代在不同测度层次之间嵌套结构的相同，结构的形态指依赖于非线性函数幂级数展开时的幂次。

（4）具有丰富的层次和自相似结构。混沌所在的区域中具有很丰富的内涵，在趋向混沌时，把标尺缩小或放大，看到的仍然是相似的“几何结构”。混沌区内有窗口（稳定的周期解），窗口里面还有混沌……有序运动和无序运动相互结合，相互转换，这种结构无穷多次重复，并具有各态历经和层次分明的特性。

（5）混沌具有伸长和折叠的特性。这是形成敏感初始条件的主要机制，伸长是指系统内部局部不稳定所引起的点之间距离的扩大；折叠是指系统整体稳定因素（有界、耗散等）作用下所形成的点之间距离的限制。经过多次的伸长和折叠，轨道被搅乱了，形成了混沌。

（6）非周期定态。因为混沌是非周期的，所以它不能被细分或不能被分解为两个互不影响的子系统（两个不变的开子集合），也就是说，混沌系统具有拓扑可传递性。

（7）遍历性。混沌运动在有限区域内轨道永不重复，运动性态极为复杂。

混沌理论具有广泛的发展领域，从20世纪80年代中后期开始，混沌学便与其他学科相互渗透、相互促进，不仅在生物学、生理学、心理学、数学、物理学、电子学、信息科学，而且在天

国家自然科学基金项目（No. 51277011）资助出版

文学、气象学、经济学，甚至在音乐、艺术等领域都得到了广泛的应用。20 世纪 90 年代以来，国际上混沌保密通信技术及其应用的研究，为高新科技的发展开辟了一个新的生长点。随着混沌通信论著的推出，混沌在保密通信领域的理论和应用研究，已经成为现代信息科学的重要分支。混沌理论的创立和发展，使得原来看似互不相关的学科之间建立了密切的联系；同时，对于混沌的研究，反过来又促进了各个具体研究领域的发展。

1.2 混沌保密通信研究现状

现代保密通信是随着军事、外交及商业需要发展起来的一种通信方法。在因泄密、窃听、破译而失密的事件中，已经给一些国家在军事、经济上造成了重大的损失，甚至导致了战争的失败和人员的重大伤亡，后果是非常严重的。随着保密通信技术的发展，情况虽有所改善，但还没有杜绝失密现象，因此世界各国都非常重视保密通信方法的研究。伴随着现代通信技术的发展，特别是计算机和各种通信网络的日益普及，保密通信已经得到很大的发展，新的加密、解密方法层出不穷。目前，保密通信已经成为计算机通信、网络、应用数学、微电子等有关学科的研究热点。

保密通信的需要激发了人们将混沌应用于通信的热情，自从 1987 年 Fujisaka 和 Yamata 以及 1990 年 Pecora 和 Carroll 对混沌同步研究取得了突破性的进展后，混沌应用于通信领域已成为可能，该理论开创了混沌同步加密的新阶段。混沌同步加密是一种动态加密方法，实际上是先将信息信号调制到近乎完全随机的混沌信号中，再经过信道传送到接收端，接收机只有被调整到与发

国家自然科学基金项目（No. 51277011）资助出版

射机参数相同或很小一个范围内时，两者才能达到同步，也只有这样，信息才能被还原出来，这种加密方法与其他加密方法相比，具有很高的保密度。混沌同步加密既可以用于实时信号加密处理，也可以用于静态加密的场合，由于其处理速度与密钥长度无关，因此这种加密方法的计算效率很高。尽管目前这项新技术的研究尚处于实验室阶段，但是由于这种加密方法实时性强、保密性高、运算速度快，所以可以预见，混沌加密是具有极高理论研究和实际应用价值的，在保密通信中，它必将具有强大的生命力和深远的应用前景。

目前，混沌通信分为有线通信和无线通信。混沌有线通信因为在理想信道中传输信号，基于混沌同步的通信比较容易实现，而混沌无线通信的难度则比混沌有线通信大得多。混沌无线通信又分为无线模拟通信和无线数字通信。基于模拟混沌电路系统的无线混沌通信保密系统，其核心问题是同步技术，关键为数字混沌序列的生成、收发双方的混沌同步、混沌信号编码以及利用群同步等。

按照目前国内国际的研究内容，混沌通信可以主要划分为四大类：混沌扩频、混沌键控、混沌参数调制及混沌掩盖[1]。信息学界围绕这四大类混沌通信体制已经进行了广泛的理论分析、仿真和实验研究。

1.2.1 混沌扩频通信

混沌扩频通信就是以混沌序列代替目前扩频通信中的伪随机序列作地址码，它利用了混沌系统对初始条件的敏感依赖性，

通过演化可以产生大量相关特性良好的扩频序列[2-6]。从理论上讲，利用混沌非线性映射产生的混沌序列是非周期序列，其概率统计特性与白噪声相似，自相关为 δ 函数，互相关为 0，而且混沌映射的初始条件不同，混沌序列就不同，同时这些序列可利用混沌系统的确定性重复产生。利用混沌序列良好的统计特性，对于实现混沌扩频码分多址通信是非常有效的。此外，混沌映射便于产生数目众多的相互正交序列，对混沌正交序列的研究有望为扩频通信提供无限多的地址码，解决目前码源有限的问题。

混沌扩频通信的关键在于混沌扩频序列的选择。混沌扩频要求的混沌序列是确定性的、易于实现的、可用序列的数目多、有好的相关特性，并且对加性高斯白噪声和其他信道干扰有较强的鲁棒性，同时由于混沌序列随初始状态的不同而不同，从而可以方便地增加通信系统的安全性。

在利用混沌序列进行扩频通信中存在一个重要的问题，那就是有限精度效应。虽然从理论上讲混沌系统产生的码序列是随机的，但是由于实际上产生混沌码的数字硬件设备精度是有限的，这种情况导致了理论上的非周期序列在实现过程中总是趋于周期序列。对于周期序列来讲，序列的周期越长，其安全性以及相关性越理想，但是提高硬件的精度则相应地提高了硬件电路复杂度和运算代价。如何经济地克服硬件设备的有限精度效应，产生具有逼近于高斯白噪声统计特性的混沌扩频序列是实现混沌扩频通信的重要研究课题。目前，混沌扩频序列主要是利用 Logistic 混沌映射或者其改进型产生，如何进一步寻找数量众多、周期任意、产生简便和性能优良的混沌扩频序列仍然是研究方向。

国家自然科学基金项目（No. 51277011）资助出版

混沌数字码分多址的研究刚刚起步，还只是处于尝试性的探索阶段[7~9]。由于混沌序列基本上不是整数序列，无法直接进行二进制转换，因此不能直接用来取代传统的二进制伪随机码或正交码。近年来，Yang Tao 等提出的混沌数字码分多址$(CD)^2MA$，直接传送伪随机混沌扩频载波[7, 8]。在$(CD)^2MA$ 中，所有移动站的混沌电路都相同，当两个用户接通时，基站分给它们一样的混沌电路初始条件。由于混沌电路往往是低频电路，一般要将其频谱搬移到兆赫（MHz）级，在频谱扩展的同时还要加上密钥信号扰频，以增加保密性。$(CD)^2MA$ 的同步方式采用冲击式同步，即通过系统状态变量间歇性的采样值来实现两个混沌系统的同步，这样既减少了发送信号的冗余，也增强了系统的保密性能。混沌序列作为$(CD)^2MA$ 信道或用户接入码，它的自相关性与互相关性是十分重要的，因为自相关性意味着码是否具有自同步性，而互相关性则决定不同用户或信道之间的互相干扰程度。就目前来说，还没有很好的码序列可以同时提供好的自相关性和互相关性，只能根据实际需要有所侧重地选取，例如基于 IS-95 标准的实用 CDMA 个人通信系统的前向链路是以同步的互相关性好的 Walsh 正交码作为扩谱序列来区分不同的用户接入信道，而在反向链路中是使用自相关性好的小m伪随机码来作为信道分隔的接入序列和扩谱序列。在$(CD)^2MA$ 中，尚未有成熟的理论来证明或确定混沌序列之间的正交性，事实上，迄今为止所发现的各种混沌序列集是非正交的，但是，由于混沌系统所具有的两个显著特点使它成为替代现有伪随机码的一个选择，这两个特点是：对初始条件的高度敏感性和在混沌状态下一个区间内均匀分布的随机性。目

国家自然科学基金项目（No. 51277011）资助出版

前$(CD)^2MA$ 还停留在实验室阶段，有关的仿真结果表明，$(CD)^2MA$的系统容量相当于CDMA的两倍，达到香农极限的1/3，其误码率与CDMA相当。

1.2.2 混沌键控通信

在混沌数字通信中，混沌键控占据重要的地位，具有比较广阔的发展前景与较高的应用价值。主要包括：COOK（混沌开关键控）[10~12]、CSK（混沌移相键控）[13~15]、DCSK（差分混沌移相键控）[16~18]和 FM-DCSK（调频差分混沌移相键控）[19~21]等四种调制方式。其解调方式有相干解调与非相干解调两种[11, 13]。在2000年左右，有关文献给出了混沌键控的噪声性能仿真结果，其中包括相干双极性CSK、相干COOK、非相干COOK以及DCSK等通信方案的噪声性能曲线，并与常规的BPSK、FSK等做了性能对比。比较结果是：从理论上讲，相干双极性CSK能达到常规相干BPSK的噪声性能，但有两个前提，一是码元能量要求保持恒定；二是要有鲁棒性相当好的同步。如果在接收端混沌载波不能精确地得到恢复，则COOK的噪声性能优于CSK，但其判决门限依赖于信噪比。当使用两个混沌信号源时，尽管相干解调的COOK在理论上能达到常规相干FSK的噪声性能，但是因为混沌信号实际上很难同步，所以实际性能达不到理论上的结果。当不能同步时，较理想的调制方式是使用非相干DCSK，其判决门限不依赖于信噪比（恒为0），而且由于经过同一信道传输参考信号和携带信息的信号，故这种调制方式对信道畸变不敏感，在参数随时间慢变的信道中具有较好的性能。如果再加上FM调制，

国家自然科学基金项目（No. 51277011）资助出版

则变成 FM-DCSK，其调制过程是：先使 FM 调制器输出具有均匀功率谱密度的带限信号，从而使每个码元传输的能量保持不变，相关器的输出具有零方差，再进行 DCSK 调制。

相干解调具有保密性，而且抗噪声性能优于非相干解调，但当传输信道的信噪比较低时，相干解调所需的同步难以建立，此时适合使用非相干解调。如果信道条件能够满足混沌同步的建立，则宜用混沌相干解调，此时混沌通信的噪声性能可以达到与常规通信相类似的水平，由于混沌载波的恢复总比周期载波难，因此一般来讲混沌相干解调的噪声性能比常规通信差一些。如果信道条件比较差，不能建立同步，就应当改用非相干解调。非相干解调已经得到了学术界广泛的关注，从 1996 年开始至今，有许多关于非相干通信的方案设计与系统性能测试的报道。从有关文献报道上看，FM-DCSK 通信方案趋于肯定，最具有实用性和发展前途，而且已经被欧洲有关委员会列入长期研究计划。FM-DCSK 能提供最优的噪声性能，它的最大优点是在多径信道下性能衰减远远好于常规方案，特别适合于无线局域网、室内无线通信、移动通信等对多径干扰敏感的场合，以及其他一些因信道恶劣而不能同步或发射功率密度要求足够低而不能影响其他设备的场合。

目前研究表明，混沌键控可以应用于超宽带（UWB）通信。超宽带技术来源于军事需求，其信号形式类似于雷达，它通过发送超短的冲激脉冲信号作为载波，在很宽的带宽范围内完成通信，也称冲激无线电。2002 年美国 FCC（Federal Communications Commission，联邦通信委员会）开放超宽带频谱，具有频谱重用和传输信号格式多样化的双重优点。因为 UWB 具有极大的信号

国家自然科学基金项目（No. 51277011）资助出版