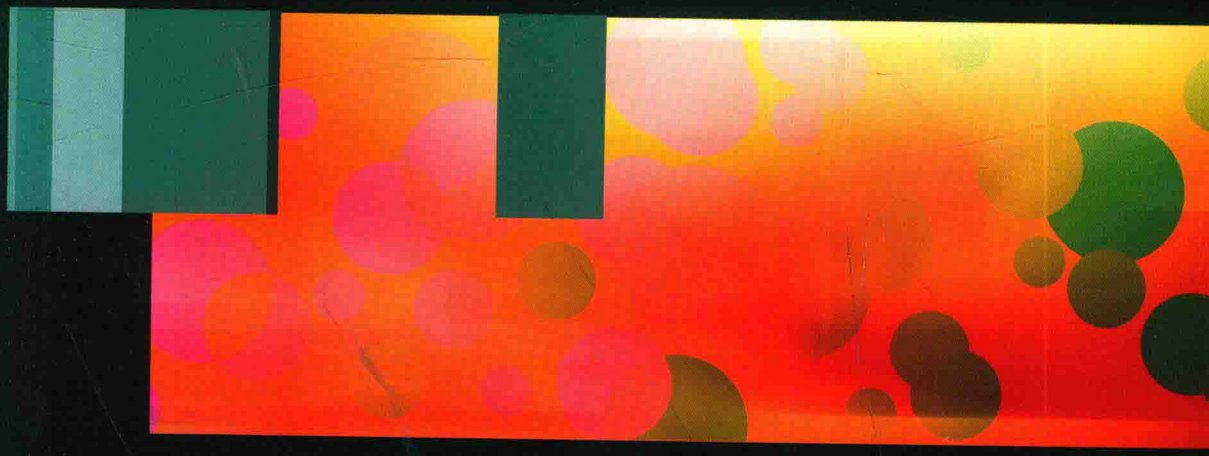
# 基于混沌的数据安全与应用

■ 李锦青 底晓强 祁 晖 何 巍 毕琳 著



# Data Security and Application Based on Chaos

国防工业出版社
National Defense Industry Press

# 基于混沌的数据安全与应用

## Data Security and Application based on Chaos

李锦青　底晓强　祁　晖　何　巍　毕　琳　著



国防工业出版社
·北京·

# 内容简介

本书以当今信息安全需求为着眼点，利用混沌理论，结合当前的研究热点，从加密解密、身份认证、安全防护技术以及保密通信方法入手，以混沌细胞神经网络和量子细胞神经网络超混沌系统为基础，对混沌同步控制方法、混沌图像加密技术进行深入研究，理论结合实际，深入分析了混沌在数据加密及网络安全通信中的应用。本书可作为从事混沌技术、数据加密和网络安全研究的师生和科研人员参考用书。

**图书在版编目(CIP)数据**

基于混沌的数据安全与应用/李锦青等著. —北京：国防工业出版社，2017.12

ISBN 978-7-118-11537-6

Ⅰ.①基… Ⅱ.①李… Ⅲ.①计算机网络-安全技术 Ⅳ.①TP393.08

中国版本图书馆 CIP 数据核字(2018)第 016213 号

※

国防工业出版社出版发行

(北京市海淀区紫竹院南路 23 号 邮政编码 100048)

天津嘉恒印务有限公司印刷

新华书店经售

*

**开本** 710×1000 1/16 **印张** 6¼ **字数** 109 千字

2017 年 12 月第 1 版第 1 次印刷 **印数** 1—2000 册 **定价** 60.00 元

**(本书如有印装错误，我社负责调换)**

国防书店：(010)88540777 发行邮购：(010)88540776

发行传真：(010)88540755 发行业务：(010)88540717

# 前　言

随着互联网技术的快速发展和信息化程度的不断提高，其越来越广泛的应用，深刻影响着政治、经济、文化等各个方面。然而，人们在享受计算机和网络带来便利的同时，也承担着巨大的风险，危害信息安全的事件不断发生。

美国麻省理工学院教授、混沌学开创人之一 E. N. 洛伦兹(Lorenz)1963 年发表一篇名为《决定论的非周期流》[1] 的论文，提出了著名的 Lorenz 方程。Lorenz 经过研究发现，当这个方程组的参数取某些值的时候，轨线运动会变的复杂和不确定，具有对初始条件的敏感依赖性，也就是初始条件最微小的差异都会导致轨线行为的无法预测，提出“混沌理论”的概念。1972 年 12 月 29 日，洛伦兹在美国科学发展学会第 139 次会议上发表了题为《蝴蝶效应》的论文，提出一个貌似荒谬的论断：在巴西一只蝴蝶翅膀的拍打能在美国得克萨斯州产生一个龙卷风，并由此提出了天气的不可准确预报性。时至今日，这一论断仍为人们津津乐道，更重要的是，它激发了人们对混沌学的浓厚兴趣。今天，伴随着计算机等技术的飞速进步，混沌学已发展成为一门影响深远、发展迅速的前沿科学。

混沌不是偶然的、个别的事件，而是普遍存在于宇宙间各种各样的宏观及微观系统的，万事万物，莫不混沌。混沌也不是独立存在的科学，它与其它各门科学互相促进、互相依靠，由此派生出许多交叉学科，如混沌气象学、混沌经济学、混沌数学等。混沌学不仅极具研究价值，而且有现实应用价值，能直接或间接创造财富。这使得混沌控制问题引起了国际上非线性动力系统和工程控制专家的极大关注，成为非线性科学研究的热点之一。混沌的发现和混沌学的建立，同相对论和量子论一样，是对牛顿确定性经典理论的重大突破，为人类观察物质世界打开了一个新的窗口。所以，许多科学家认为，20 世纪物理学永放光芒的三件事是相对论、量子论和混沌学的创立。

混沌系统所具有的对参数和初值非常敏感的基本特性和密码学的天然关系在 Shannon 1949 年发表的经典论文《Communication Theory of Secrecy Systems》中就有提到。

本书共分六章。

“第一章、绪论”。简要介绍了本书研究背景和意义，以及混沌与混沌图像加密的基本概念。

“第二章、混沌神经网络图像加密算法研究”。阐述了当前图像加密算法的

常见机制；对混沌和神经网络的特性进行总结，分析了以细胞神经网络作为模型设计图像加密方法的主要优点；给出了两种基于复合混沌映射和6阶细胞神经网络以及Hopfield混沌神经网络的彩色图像加密解密算法；最后分别对这两种加密算法的安全性能进行了详细的仿真实验和数值分析，对算法的安全性、可靠性进行了证明。

“第三章、量子细胞神经网络混沌同步控制方法的研究”。对于量子细胞神经网络的混沌特性进行分析计算，分别以2-cell和3-cell耦合构成混沌振荡器，绘制其超混沌吸引子计算其Lyapunov指数，分析其超混沌特性。最后设计给出了这两种超混沌系统不同的同步控制规则和参数更新规律，并利用实验仿真，证明该同步方法快速有效。

“第四章、量子细胞神经网络混沌同步的保密应用研究”。以第二章和第三章的研究结果为基础，在第四章中，我们以2-cell的量子细胞神经网络为基础，利用其同步控制方法设计了一套多进制数字保密通信系统，并通过数值仿真验证了它的有效性和可扩展性；此外，结合当前不同的数字图像加密方法的优缺点，设计了一种新型半对称量子细胞神经网络超混沌图像加密算法，并通过仿真实验对该算法的安全性进行了全面分析。

“第五章、混沌加密网络安全应用”。结合第一章中所介绍的人们所面临的信息安全威胁，从身份认证的角度出发，结合超混沌加密技术，设计了一种分布式跨域身份认证方案；提出了一种基于量子细胞神经网络的弱密码超混沌加密方法，该密码方案将量子细胞神经网络的超混沌特性和人脑模式识别的优势相结合，使用较少的密码位数，极大降低了加密过程中的计算量，达到了较高的安全水平，该方法具有安全性高，用户记忆便捷的特点。

“第六章、量子细胞神经网络超混沌系统在光学图像加密中的应用”。从现有光学加密系统非线性程度不足的角度出发，利用量子细胞神经网络超混沌系统对光学图像进行加密解密，由于量子细胞神经网络的超混沌特性，弥补了传统双随机相位编码光学加密技术的线性特征的不足，令该加密方法具有密钥空间大，抗攻击能力强的安全特点。

作者希望本书能对计算机和信息安全等专业的本科高年级学生、研究生和相关研究人员了解相关理论的发展、从事相关的研究工作提供一定的参考价值。

由于作者水平有限，并受到科研水平及所做工作的局限性影响，书中难免存在不妥之处，敬请读者批评指正。本书部分研究内容得到了吉林省省级产业创新专项资金项目“基于混沌的视频加密技术研究与应用”(2016C087)的资助。

李锦青

2017年7月

# 符号、缩略语说明

| 序　号 | 符号、缩略语 | 说　明 |
|---|---|---|
| 1 | CNN(Cellular Neural Network) | 细胞神经网络 |
| 2 | QCNN(Quantum Cellular Neural Network) | 量子细胞神经网络 |
| 3 | TLM ( Tent-Logist Compound Chaos Map) | 复合混沌映射 |
| 4 | Lyapunov 指数 | 李亚普诺夫指数 |
| 5 | $H$ | 信息熵 |
| 6 | NPCR(Number Pixels Change Rate) | 像素变化率 |
| 7 | UACI(Unified Average Change Intensity) | 统一平均变化强度 |
| 8 | $r_{xy}$ | 像素的相关系数 |
| 9 | QCA(Quantum-Dot Cellular Automata) | 量子点细胞自动机 |
| 10 | $\hbar$ | 普朗克常量 |
| 11 | $\gamma$ | 量子点间隧穿能 |
| 12 | $E_k$ | 静电损耗 |
| 13 | $P_k$ | 相邻量子细胞自动机极化率 |
| 14 | $\overline{P}_k$ | $P_k$ 的加权代数和 |
| 15 | $\phi_k$ | QCA 量子相位 |
| 16 | TCP(Trusted Computing Platform ) | 可信计算平台 |
| 17 | Do | 可信域 |
| 18 | DCAC(Distributed Certificate Arbitration Center) | 分布式证书仲裁中心 |
| 19 | AIK(Attestation Identity Key) | 平台身份密钥 |
| 20 | CRPM(Chaotic Random Phase Mask) | 混沌随机相位模板 |

# 目　录

# 第一章 绪 论

网络空间已被视为继陆、海、空、天之后的第五空间，网络战已成为所谓的“第五空间战争”，随之，网络空间的安全问题，已经上升到国家战略安全的层次。2014 年 2 月 27 日，中央网络安全和信息化领导小组宣告成立，并在北京召开了第一次会议。中共中央总书记、国家主席、中央军委主席习近平亲自担任组长，明确提出要建设坚固可靠的国家网络安全体系。《中华人民共和国网络安全法》也在 2017 年 6 月 1 日颁布实施。

计算机网络把人类社会从工业时代带进了信息时代，人类在工作、生活和学习等方方面面已经无法摆脱对网络的依赖，但在网络服务给人们提供了极大便利的同时，对于信息系统的非法入侵和破坏活动正以惊人的速度在全世界蔓延，同时带来了巨大的经济损失和安全威胁，据统计，每年全球因网络安全问题导致的损失已经达到数万亿美元。因此网络信息安全问题已引起各国政府的高度重视。这种重视也明显体现在了国家教育发展的规划上。2011 年，国务院学位办编写的《计算机科学与技术一级学科简介》（征求意见稿）将信息安全从计算机软件与理论二级学科中划分出来，与从计算机系统结构二级学科中剥离出来的计算机网络放在一起，设置了新的二级学科：计算机网络与信息安全；2012 年，国家教育部对本科专业目录调整时在计算机专业类中明确设置了信息安全专业，并可授工学或理学或管理学学士学位。

随着互联网应用，特别是电子商务、电子政务、电子金融的普及，以及云计算、大数据时代的到来，信息安全已经成为国家战略安全的重要组成部分，同时，网络攻防技术成为大国间经济、政治、文化、军事博弈的利器。2016 年 11 月在浙江乌镇召开的第三届互联网大会上，中共中央总书记、国家主席习近平着重强调了网络安全对于网络空间命运共同体的重要性。回顾近年来国内外网络安全大事件，“315 晚会曝光公共 WIFI 漏洞，20 万儿童信息泄露或打包出售，准大学生徐玉玉遭电信诈骗后死亡，超 3200 万 Twitter 账户密码泄露，2.7 亿 Gmail、雅虎和 Hotmail 账号遭泄露，MySpace 出现史上最大规模数据泄露事件”等一系列电信诈骗、病毒攻击、数据泄密安全事件频发，且愈演愈烈，使我们清晰地认识到解决网络信息安全问题还任重而道远。

## 1.1 混沌简介

混沌(Chaos)也作浑沌,指确定性系统产生的一种对初始条件具有敏感依赖性的回复性非周期运动。浑沌与分形(fractal)和孤子(soliton)是非线性科学中最重要的三个概念。浑沌理论隶属于非线性科学,只有非线性系统才能产生浑沌运动。据1991年出版的《浑沌文献总目》统计,已收集到与浑沌研究有直接关系的书269部、论文7157篇。到1996年底,还不断有新的浑沌研究成果发表[3]。

混沌确定系统是1903年庞加莱在研究三体问题时第一次发现的。典型的Duffing动力学方程和VDP动力学方程奠定了混沌动力学基础。1954年,苏联数学家A. N. Kolmogorov发现了哈密尔顿函数微小变化时条件周期运动的持续,从而揭示了不仅耗散系统有混沌,保守系统中也有混沌。1963年,Lorenz给出了三个变量的Lorenz方程。这些都为混沌的发展奠定了基础。20世纪70年代,特别是1975年以后,是混沌科学发展史上光辉灿烂的年代。在这一时期,作为一门新兴学科——混沌学正式诞生了。1971年,法国数学物理学家Ruelle和荷兰学者Takens一起发表了《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,通过严密的数学分析,独立地发现了动力系统存在"奇怪吸引子",他们形容为"一簇曲线,一团斑点,有时展现为光彩夺目的星云或烟火,有时展现为非常可怕和令人生厌的花丛,数不清的形式有待探讨,有待发现。"1973年,日本京都大学的Y. Ueda在用计算机研究非线性振动时,发现了一种杂乱振动形态,称为Ueda吸引子;1975年,李天岩(T. Y. Li)和J. A. Yorke在他们的论文《周期3意味着混沌》中,给出了闭区间上连续自映射的混沌定义,在文中首先提出Chaos(混沌)这个名词,并为后来的学者所接受。1977年夏天,物理学家J. Ford和G. Casati在意大利组织了关于混沌研究的第一次国际科学会议,进一步营造了混沌研究的氛围;1978年,M. J. Feigenbaum用手摇计算机彻夜工作,发现了一类周期倍化通向混沌的道路中的普遍常数;1979年,P. J. Holmes作了磁场曲线中曲片受简谐激励时的振动试验,发现激励频率和振幅超过某个特定值之后,就出现混沌振动;1980年,意大利的V. Franceschini用计算机研究流体从平流过渡到湍流时,发现周期倍化现象,验证了费根鲍姆(Feigenbaum)常数;1981年,美国麻省理工学院的P. S. Linsay第一次用实验证明了Feigenbaum常数;1989年,美苏混沌讨论会召开;1990年,在德国专门设立

了分岔与混沌研讨会;1991 年 4 月,在日本由联合大学与东京大学共同召开了“混沌对科学与社会的影响”的国际会议;1991 年 10 月,在美国召开了首届混沌试验研讨会。这些会议的召开促进了混沌学研究世界性热潮的到来[3,4]。

近年来,混沌科学更是与其他科学相互渗透,无论是在生物学、生理学、心理学、数学、物理学、电子学、信息科学,还是天文学、气象学、经济学,甚至在音乐、艺术等领域,混沌都得到了广泛的应用[3]。例如 Kaos 公司在 1995 年主办了混沌芝加哥艺术节,把混沌理论的意义和内容带到了装饰术中。M. S. Baptista 在 1998 年提出了一种基于搜索机制的混沌密码算法,可以使用简单的低维和混沌逻辑方程的遍历属性来加密消息(由某些字母组成的文本)。2000 年 S. S. GE 提出了一种用于构建反馈控制律和相关 Lyapunov 函数的混沌系统设计方法,2005 年,A. Argyris 对混沌载波在光混沌通信系统中同步的能力在光谱域分析下进行了实验研究。2007 年,Francis C. Moon 修订流体和固体混沌振动现象,反映了这个快速变化主题的最新发展。2008 年,Behnia 等人提出了基于耦合混沌映射的对称图形加密算法;2010 年,J Hizanidis 等人提出了一种结合以前研究的全光学和电光学方案的光混沌通信的新架构,2012 年,Zhang 等人首次提出了基于 PDE 的图像加密技术;2013 年,Wu 等阐述了离散分数逻辑映射,其是在左侧卡普托离散增量的意义上提出;2014 年,F. Krahmer 等人提出了一个基于链接方法的一组矩阵索引的特殊类型混沌过程的上限的新界限;2015 年,M. Sciamanna 讨论了支撑激光二极管混沌的基础物理学以及将其用于潜在应用的机会。Meng 等人在 2016 年发表的论文中研究开发了基于 Einthoven 原理的 ECG 过程。使用 LabVIEW 将电路和 DAQ 卡并入人机界面,以检测 ECG 中的 PQRST 点,并显示测试对象的经处理的 ECG 信号。使用主从混沌系统将保存的 ECG 数据绘制成混沌动态误差动力学图。选择混沌眼作为特征,并使用元素模型构建身份数据库,通过使用扩展方法分类来识别个人身份。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”。正如混沌科学的倡导者之一,美国海军部官员 M. Shlesinger 所说的那样:“20 世纪科学将永远铭记的三件事,那就是相对论、量子力学和混沌”,它在整个科学中所起的作用相当于微积分学在 18 世纪对数理科学的影响[4]。混沌学的创立,将在确定论和概率论这两大科学体系之间架起桥梁,它将揭开物理学、数学乃至整个现代科学发展的新篇章[3,4]。

国外的混沌研究成果倍出,以洛伦茨(Lorenz)吸引子、费根鲍姆(Feigenbaum)普适常数、KAM 定理、阿诺德(Arnold)扩散、斯梅尔(Smale)马蹄

理论为标志,取得了重大的突破;国内的学者也取得了一系列成果,涌现出了蔡少棠、郝柏林、陈关荣等一大批混沌学专家[3,4]。

将量子理论与神经计算相结合是美国路易斯安那州立大学 Subhash Kak 教授的创举,他在 1995 年发表的《On Quantum Neural Computing》[5]一文首次提出量子神经计算的概念,开创了该领域的先河。同年 6 月,英国 Sussex 大学的 Ronald L. Chrisley 提出了 Quantum Learning[6]的概念,并给出非叠加态的量子神经网络模型和相应的学习算法。

1995 年 11 月,英国 Exeter 大学的 Mark Moore 和 Ajit Narayanan 在本校的技术报告中发表了有关量子衍生计算《Quantum-Inspired computing》的学术论文[7];同年 12 月,Menneer 和 Narayanan 又发表了量子衍生神经网络《Quantum-Inspired Neural Networks》的相关论文[8];1996 年,Narayanan 和 Moore 又在 IEEE 的 Evolutionary Computation 国际会议上发表了一篇关于量子衍生遗传算法《Quantum-Inspired Genetic Algorithms》的文章[9];1998 年,Menneer 完成了题目为《Quantum Artificial Neural Networks》的博士论文[10],文中讨论了如何将量子计算引入人工神经网络,并证实了对于分类问题量子神经网络要比传统神经网络更为有效。

1996 年,美国 Wichita 州立大学的 Behrman 博士等人在《InterJournal Complex Systems》杂志上发表了一篇名为《A Quantum Dot Neural Networks》的文章,文中提出了量子点神经网络模型[11]。

1997 年,美国 Brigham Young 大学的 Dan Ventura 博士和 Tony Martinez 教授初步给出了具有量子力学特性的人工神经元模型,并在 2000 年发表的《Quantum Associative Memory》一文中给出有关量子联想的概念[12]。

1999 年,毕业后在 Penn 州立大学工作的 Ventura 博士在 IEEE Intelligent System 7/8 月专刊上正式提出量子计算智能(Quantum Computational Intelligence)的定义,并在 2000 年 3 月召开的第四届国际计算智能和神经科学会议上主持了量子计算与神经量子信息处理的专题会议《The Special Sessions on Quantum Computation and Neuro-quantum Information Processing》。

此外巴西 Brasilia 大学的李伟钢(Li Weigang)博士在 1998 年发表了有关量子并行 SOM 算法的文章《A Study of Parallel Self-Organizing Map》[13],并应用于卫星遥感图像的识别;1999 年,他在文章《A Study of Parallel Neural Networks》中讨论了量子的隐形传态(Teleportation)问题,初步构造了纠缠神经网络模型[14]。

由于量子论是现代物理学的基石。量子论给我们提供了新的关于自然界的表述方法和思考方法。量子论揭示了微观物质世界的基本规律,它具有更普遍

更本质的特征。量子神经网络是传统神经计算系统的自然进化，量子计算的巨大威力势必会大幅提升神经计算的信息处理能力。

1993 年，Lent 等利用量子点提出的量子点细胞自动机（Quantum - doc Cellular Automata，QCA）[15]已经引起学术界的广泛关注。采用量子计算的方法有很多优点，如计算是在纳米结构尺度上，因此具有超高集成密度和低功耗等特点[16]。学者们还利用 QCA 构造了细胞局部耦合的网络——量子细胞神经网络（Quantum Cellular Neural Network，QCNN）[17-21]。这些量子点细胞以其规则结构及局部耦合排列的网络与蔡氏细胞神经网络非常类似。以薛定谔方程为基础的 QCNN 量子力学方程，也表现出与蔡氏细胞神经网络动力学特性类似的形式。由于量子点之间的量子相互作用，可从每个细胞的极化率获得复杂的动力学特性。Fortuna 等在文献[22]中介绍了量子细胞神经网络的混沌现象，并在 2004 年发表了文章[23]，介绍了由 QCNN 构造的纳米级混沌振荡器。西安交通大学的蔡理和王森发表了多篇关于量子细胞神经网络超混沌特性及其相关应用的学术论文[16, 24-28]。近年来，国内外的研究者以量子细胞神经网络为基础，针对不同的混沌同步方法展开了深入的研究[29-34]。2009 年，KS Sudheer 利用自适应方法研究了双细胞量子-CNN 混沌振荡器的功能投影同步；2010 年，Yang 等人利用非线性自适应控制器研究了两单元量子 CNN 混沌振荡器的功能投影同步；XK Yang 等在研究了具有不确定系统参数的量子细胞神经网络和 Lorenz 超混沌系统的功能投影同步；CH Yang 通过可变结构控制和脉冲控制，研究了量子 CNN 混沌系统的混沌同步和混沌控制；ZM Ge 提出了一种新的模糊模型来模拟量子细胞神经网络纳米系统（称为 Quantum-CNN 系统）；2011 年 CH Yang 提出了通过 GYC 部分区域稳定性实现混沌广义同步的新策略；2016 年，Luca 等人发表的《从量子混沌和本征态热化到统计力学和热力学》对本征态热化假说（ETH），其基础及其对统计力学和热力学的影响进行了教学性的介绍。

## 1.2 混沌图像加密简介

数字图像是目前最流行的多媒体形式之一，在政治、经济、国防、教育等方面均有广泛应用。对于某些特殊领域，如军事、商业和医疗，数字图像还有较高的保密要求。为了实现数字图像保密，实际操作中一般先将二维图像转换成一维数据，再采用传统加密算法进行加密。与普通的文本信息不同，图像和视频具有时间性、空间性、视觉可感知性，还可进行有损压缩，这些特性使得为图像设计更

加高效、安全的加密算法成为可能。自20世纪90年代起,研究者利用这些特性提出了多种图像加密算法。

混沌图像加密技术是近年来应用非常普遍的一种数字图像加密技术,由于近年来兴起的混沌理论在加密数字图像上的应用表现出了良好的特性,并且为数字图像加密提供了一种新的有效途径,从而使得混沌图像加密的相关研究受到国内外的广泛重视。混沌现象是指在确定性系统中的貌似随机的不规则运动,在一个确定性理论描述的系统中,其行为却表现为不确定性、不可重复、不可预测的类似随机的过程,混沌动力学在此基础上得到迅猛发展,这使得混沌可以用来作为一种新的密码体系,可以给声音、图像数据以及文本文件加密。由于混沌系统对初始条件和参数的敏感性及其类噪声特性,使得混沌理论越来越多地被应用到保密通信系统的设计中,专家学者们先后提出了许多基于混沌系统的加密算法[35-50]。

对基于混沌的图像加密模式做进一步研究具有非常重要的理论意义和应用价值。1997年,Fridrich首次将混沌加密方法应用到图像加密中[35],随后,混沌图像加密技术成为数字图像加密技术研究的热点。2010年,Faridnia以混沌函数和图论为基础,提出了一种图像加密方法[36]。同年,Ahmad Musheer等,在文献[37]中设计了一种多层次的块置乱图像加密方案。Singh Narendra和Sinha Aloka在文献[38,39]中分别介绍了基于混沌映射的光学图像加密算法和数字水印。2011年,Kumar提出了一种扩展的替代扩散的基于混沌标准映射的图像加密方法[40]。Ahmad Musheer和Farooq Omar在文献[41]中给出了一种基于混沌和离散小波变换的安全的卫星图像传输方案。2012年,文献[42]介绍了一种基于改进的混沌序列的图像加密方案。Mirzaei Omid等提出了一种并行子图像超混沌加密算法[43]。文章[44]给出了基于混沌加密的分形图像编码方案。Abdullah等在文献[45]中提出了一种混合遗传算法和混沌函数模型的图像加密算法。Seyedzadeh介绍了基于耦合二维分段混沌映射的快速彩色图像加密算法[46]。文献[47]阐述了一种基于延迟分数阶Logist混沌的图像加密方法。2013年,文献[48]中介绍了一种使用离散Chirikov标准映射和混沌分数随机变换的双光学图像加密方法。Tong在文章中阐述了多混沌映射的图像加密方案设计思想[49]。Rasul提出了一种加权离散帝国主义竞争算法(WDICA)结合混沌映射的图像加密算法[50]。2014年,Khan等人提出了利用分数洛伦兹混沌系统的仿射变换的新的数字图像加密方案,J. S. 提出了一种基于线性多项式方程(LDE)的快速生成大排列和扩散密钥的一轮加密方案,在很大程度上克服了混沌图像加密耗时耗材的问题。2015年,Khan, M. & Shah提出了一种构建图像

加密应用中使用的非线性分量的算法。zhao 等人基于数字图像加密和高维混沌序列的特点,提出了一种新的 improper 分数阶混沌系统的对称数字图像加密算法。2016 年,R. Guesmi 等人提出了一种基于脱氧核糖核酸(DNA)掩蔽的混合模型,安全散列算法 SHA-2 和 Lorenz 系统的新型图像加密算法,研究使用 DNA 序列和操作以及混沌 Lorenz 系统来加强密码系统。A Belazi 提出了基于 SP 网络和混沌的 61A 新型图像加密方法;2017 年,A Belazi 提出了一种基于混沌系统和线性分数变换(LFT)构建的基于替代盒(S-box)的基于混沌的部分图像加密方案;A. Roy 等使用自由运行的垂直腔表面发射激光器(VCSEL)中的偏振动力学同步来研究彩色图像的加密和解密过程。

# 第二章　混沌神经网络图像加密算法研究

## 2.1　引　　言

近年来，安全通信方式中的数据加密机制受到了全世界研究者的广泛关注。最常见的图像加密机制为置乱—扩散机制。采用该机制的图像密码系统通常包含两个阶段：置乱阶段主要是用于将图像的信息次序打乱，将 a 像素移动到 b 像素的位置上，b 像素移动到 c 像素的位置上等，用于掩盖明文、密文和密钥之间的关系，使其变换成杂乱无章、难以辨认的图像，使密钥和密文之间的统计关系尽可能复杂，导致密码攻击者无法从密文推理得到密钥；扩散阶段是使明文的任意一位像素均能影响密文中多位的值，将明文冗余度分散到密文中，以便隐藏明文的统计结构。将置乱—扩散过程重复循环一定次数，以保证达到相应的安全水平。在这种机制中，密钥和控制参数的生成是算法安全性与复杂性的决定性要素之一。

一个良好的加密算法应该是对密钥敏感的，并且密钥空间应该足够大以抵抗暴力攻击。混沌系统所具有的对参数和初值非常敏感的基本特性和密码学的天然关系在 Shannon 的经典文章[51]中就有提到。当前，文献中大量的基于混沌系统的加密方法被提出，使用混沌系统生成密钥及参数已成为安全通信领域一项非常重要的课题[52-55]。由于神经网络的复杂性和时变结构使其作为信息保护的另一选择被广泛的应用，包括对数据的加密、认证、入侵检测等[56-59]。

混沌神经网络结合了神经网络与混沌二者的特性，较传统的混沌系统而言具有更为复杂的时空复杂度，其良好的置乱和扩散特性已经成功用于密码设计。混沌神经网络应用于密码设计的研究引来越来越多学者的关注[60-66]。Huang[60]提出了一种四个神经元的 Hopfield 神经网络结构，并对其混沌特性进行了分析。Bigdeli 根据文献[60]讨论的混沌神经网络模型设计了一种图像加密算法[61]，并对其安全性进行分析。Li[62]对一种细胞神经网络模型的混沌现象进行了分析。Peng[63]设计了一种基于文献[62]的图像加密算法；Gao 依照该

模型提出一种图像识别算法[64]；文献[66]介绍了使用细胞神经网络模型设计的公钥水印算法。

以细胞神经网络(CNN)作为模型设计图像加密方案，其优点主要有[60]：

(1) 细胞神经网络状态方程形式简单，但在很大的参数范围内具有混沌吸引子，具有复杂的动力学行为；

(2) 细胞神经网络状态方程中参数较多，可以设计出密钥空间较大的加密方案；

(3) 细胞神经网络状态方程能直接产生随机性较好的随机矩阵，使得二维图像加密方案的设计更加方便；

(4) 细胞神经网络易于在超大规模集成电路中实现。

## 2.2 基于复合混沌映射和混沌细胞神经网络的彩色图像加密算法

基于复合混沌映射和混沌细胞神经网络的彩色图像加密算法使用两个不同初始条件和参数的复合混沌映射[67]分别生成置乱阶段的控制参数和高阶混沌系统的控制参数。在该算法中，六个初始密钥包括：两个复合映射混沌系统的初始条件，两个控制参数以及两个迭代次数。本算法具有极强的敏感性，即便是十分轻微的不匹配都无法解密。这意味着，即使知道密钥的近似值也不能够进行破解。对图像加密算法的安全性分析表明：该加密系统具备鲁棒性，有效性和出色的工作性能。

### 2.2.1 复合混沌映射与细胞神经网络模型

**1. 复合混沌映射 TLM (Tent-logist Compound chaos mapping)**

标准帐篷映射的方程为[69]

$$x_{n+1}=\begin{cases}\mu x_n, & 0<x_n<0.5\\ \mu(1-x_n), & 0.5\leqslant x_n<1\end{cases} \tag{2.1}$$

研究表明，当对 $\mu$ 取不同值迭代，该方程所表现出来的特性是不同的。在 $\mu<1$ 时，式(2.1)处于收敛状态，恒收敛于不动点 0，其收敛速度随着 $\mu$ 增大而减小。当达到临界点 $\mu=1$ 时，方程收敛于初始迭代点。当 $\mu>1$ 时，方程表现为混沌状态，并且混沌带随着 $\mu$ 增大而逐渐扩大。

Logistic 映射的方程为[63]

$$x_{n+1}=\lambda x_n(1-x_n)\quad \lambda\in(0,4),x\in[0,1] \tag{2.2}$$