

光学信息安全导论

彭翔 位恒政 张鹏 著

本书由深圳大学学术著作出版基金资助出版

科学出版社

北京

内 容 简 介

本书主要内容涉及光学信息安全的基本概念和理论。光学信息安全是近年来国际上起步发展的新一代信息安全技术。自从1995年国际上首次提出双随机相位编码光学加密的概念和方法后,光学信息安全在国际上得到了广泛的关注和研究。光学信息安全目前已经成为信息光学研究领域的前沿课题之一。本书所讲述的光学信息安全包括光学密码学、光学密码分析学,以及光学信息隐藏的基本概念和理论基础。

本书可作为光学工程、信息与通信工程(通信与信息系统,信号与信息处理)、控制科学与工程(模式识别与智能系统)、物理学(光学)等专业的大学高年级学生和研究生的教材,也可以作为在上述领域工作的科研人员的参考书。

图书在版编目(CIP)数据

光学信息安全导论/彭翔,位恒政,张鹏著. - 北京:科学出版社,2008
ISBN 978-7-03-021384-6

I. 光… II. ①彭…②位…③张… III. 信息光学-安全技术
IV. O438

中国版本图书馆 CIP 数据核字(2008)第 034471 号

责任编辑:余 丁 杨 然 / 责任校对:陈玉凤

责任印制:刘士平 / 封面设计:耕者

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>

印刷

科学出版社发行 各地新华书店经销

*

2008年4月第 一 版 开本:B5(720×1000)

2008年4月第一次印刷 印张:15 1/4

印数:1—3 000 字数:287 000

定价:45.00 元

(如有印装质量问题,我社负责调换〈环伟〉)

作者简介

彭翔,深圳大学光电工程学院教授,博士生导师,副院长。1982年毕业于天津大学精密仪器与光电子工程学院,1984年和1989年分别在该校获得工学硕士和工学博士学位,1990~1992年作为洪堡研究员在德国斯图加特大学应用光学研究所从事博士后研究,1992~1998年在天津大学精密仪器与光电子工程学院任副教授,1998~2002年任教授、博士生导师。曾在美国休斯敦大学(1985、1986)、加拿大卡尔加里大学(1999.2~1999.10)进行合作研究。2003年1月调入深圳大学,任教授、博士生导师,曾主持完成多项国家自然科学基金项目和省部级项目,现主持国家自然科学基金、广东省自然科学基金及深圳市科技计划项目等多项课题的研究。研究领域涉及三维数字成像及造型、光学信息安全和现代光学测试技术。在上述领域的国内外重要学术期刊上发表研究论文100余篇,获得授权国家发明专利7项,曾获德国洪堡基金会研究奖学金、国家教委科技进步奖、天津市青年科技奖。

位恒政,博士,2008年毕业于天津大学,研究方向为信息安全、数字图像处理、计算机视觉、激光技术等,参与并完成了包括国家自然科学基金、中国科学院微系统与信息技术研究所开放课题、广东省自然科学基金、深圳市科技计划项目在内的多项重要课题的研究,相关成果发表在《物理学报》、《光学学报》、*Optics Letters*等国内外著名学术期刊,其中6篇被SCI收录。

张鹏,博士,2006年毕业于天津大学,研究方向为信息安全、密码学理论、数字信号处理、计算机视觉等。参与并完成了包括国家自然科学基金、中国科学院模式识别国家重点实验室开放课题、教育部985项目、广东省自然科学基金、深圳市科技计划项目在内的多项重要课题的研究。在包括《电子学报》、《物理学报》、《光学学报》、*Optics Letters*、*Optik*等在内的国内外著名学术期刊、国际会议上发表学术论文20余篇,其中9篇被SCI收录,20篇被EI收录,申请国家发明专利7项,已授权3项。张鹏博士现任职于中国建设银行总行电子银行部,主要从事电子银行安全、金融电子化等相关领域的研究。

前 言

光学信息安全是近代光学与信息安全技术相结合而衍生出来的一门新兴交叉学科。信息安全技术已经成为在当今巨大的互联数字信息社会中保护数字信息不受侵害、识别信息用户合法身份的关键技术。基于近代光学理论与方法的数据加密和信息隐藏技术是近十几年来在国际上活跃开展的新一代信息安全理论与技术。信息光学系统具有固有的并行数据处理能力。例如,在光学系统中,一幅二维图像中的每一个像素都可以被同时传播和处理。很明显,光学信息系统的并行能力在处理海量信息时显现出电子信息系统所不能比拟的优势,而且所处理的图像越复杂、信息量越大,这种优势就越明显。同时,光学加密比电子加密具有更多的自由度,信息可以被隐藏在多个自由度空间中。在完成数据加密或信息隐藏的过程中,可以通过计算光的干涉、衍射、滤波、成像、全息等过程对涉及的波长、焦距、振幅、光强、相位、偏振态、空间频率及光学元件的参数等进行多维编码。与传统基于数学的计算机密码学及信息安全技术相比,光学信息安全技术具有多维度、大容量、高鲁棒性以及固有的并行处理性质等诸多优势。因此,光学信息安全技术在国际学术界受到了广泛的关注。近年来,国际光学工程学会(SPIE)和国际电子电气工程师协会(IEEE)等国际学术组织多次召开关于光学信息安全的专题国际会议。国际光学工程学会(SPIE)的官方期刊(*Optical Engineering*)在1996年、1999年、2004年分别三次出版了关于光学信息安全的期刊专辑。与光学信息安全有关的研究报道已经成为国际光学工程学会最热门的主题之一。

自从1995年双随机相位编码的光学加密方法被提出以来,光学信息安全技术从利用联合变换相关器进行身份认证和生物特征识别逐渐发展到利用信息光学原理构造各种密码算法和密码系统。值得注意的是,这些光学密码的原理既可以通过光学手段实现,也可以通过数字手段实现。因此,光学信息安全理论在具体应用上具有普适性。此外,基于信息光学原理的各种数字水印技术和其他信息隐藏技术也被相继提出。经过十几年的发展,光学信息安全已经发展成为一个活跃研究的交叉学科领域。

本书作者在从事这一领域的研究工作和指导研究生的过程中,迫切感到需要一本这方面的专著和教科书。编写此书的目的,一方面旨在为读者介绍这一新兴领域的研究工作和最新取得的进展;另一方面向读者介绍这一新兴交叉学科领域的基础知识,使得那些对这一领域有兴趣的读者可以比较全面和系统地建立起光学

信息安全的有关概念,并掌握与之相关的各种算法的理论基础。

全书共分8章:第1章是绪论,介绍信息的内涵和一些基本概念以及光学信息安全的发展过程和研究现状。第2章介绍光学密码系统的理论基础和一些典型光学密码技术的原理。第3章介绍基于虚拟光学框架的对称密码学。从密码学的观点来看,国际上目前关于光学加密工作的绝大多数报道都属于对称密钥密码系统的范畴,这种系统由于在网络环境下的密钥管理、分发、传输问题尚未得到解决,所以无法与信息安全的国际标准相结合,从而不能嵌入到公钥基础设施(PKI)中。因此,第4章主要介绍基于虚拟光学框架的公钥密码学。信息光学理论除了在密码学研究方面具有很大的发展潜力外,在信息隐藏与数字水印技术方面也表现出极大的潜力。相比于传统的数字水印技术,利用光学理论与方法完成水印的嵌入和提取是一种新的概念和新的技术途径。第5章介绍基于虚拟光学的三维空间数字水印技术。第6章介绍基于计算全息图的半色调图像信息隐藏。密码编码和密码分析是密码学的两个既相互独立又相互关联的研究内容。对光学密码研究而言,目前国际上从密码分析学的角度对光学数据加密系统进行全面的密码分析工作的报道很少,而对光学数据加密系统的密码分析学研究,无论是从光学信息安全理论体系的完整性,还是从实际应用的重要性来看都具有极其重要的价值。第7章讲述光学密码分析的理论基础。第8章介绍双随机相位编码的光学加密系统的各种密码分析方法。在全书的8章内容中,第3、4、5、6、8章包括了本书作者在光学信息安全领域的研究工作。

本书的第1、2章由彭翔撰写;第3、4、5章由彭翔和张鹏撰写,其中4.3节由彭翔和位恒政撰写;第6、7章由彭翔撰写;第8章由彭翔和位恒政撰写。最后由彭翔审校了全书。本书所涉及作者的研究工作得到了国家自然科学基金(60472107)、广东省普通高校自然科学研究重点基金(04Z010)、深圳市科技计划项目(200426)、模式识别国家重点实验室开放课题、中科院微系统与信息技术研究所等科研项目的支持。在此,作者向上述科学基金委员会、所属的政府及科研机构表示感谢。作者还要感谢于斌博士在本书3.3节中部分内容所做出的贡献;感谢研究生崔志勇在第5章中部分内容所做出的贡献,白伟东在第6章中部分内容所做出的贡献,汤红乔在第7章和第8章中部分内容所做出的贡献。本书涉及的诸多理论分析和实验结果都来源于作者学生的学位论文,没有他们的贡献,完成本书是不可能的。

作者在从事光学信息安全领域的研究之初,曾与香港科技大学蔡李隆教授、余凌峰博士进行过卓有成效的讨论与合作。正是通过与他们的讨论,作者获得了很多灵感。在此,作者向蔡李隆教授和余凌峰博士表示诚挚地感谢!

由于作者水平所限,如果书中难免存在不妥之处,敬请读者指正。最后感谢深圳大学学术著作出版基金对本书出版给予的资助。

彭翔

2007.9.15 于深圳大学

通信地址:深圳大学光电工程学院,518060

电话:(0755)26538548

传真:(0755)26538580

电子邮件:xpeng@szu.edu.cn

主页:<http://opto.szu.edu.cn/cn/Member/PengX.htm>

目 录

前言	
第 1 章 绪论	1
1.1 信息安全	1
1.1.1 密码学	1
1.1.2 信息隐藏	4
1.2 光学信息安全技术	6
1.2.1 光学安全认证技术	6
1.2.2 基于光学理论与方法的数据加密	7
1.2.3 基于光学理论与方法的信息隐藏	9
1.2.4 国际学术组织的活动	10
1.2.5 国内的研究进展情况	11
参考文献	11
第 2 章 光学密码系统的理论基础	17
2.1 光学加密系统的相关理论基础	17
2.1.1 传播理论	17
2.1.2 透镜的傅里叶变换性质	21
2.1.3 全息理论	23
2.2 典型的光学密码编码系统	28
2.2.1 基于 $4f$ 系统的双随机相位编码	28
2.2.2 基于菲涅耳变换的双随机相位编码	29
2.2.3 基于分数傅里叶变换的双随机相位编码	30
2.2.4 基于联合变换相关器的双随机相位编码	31
2.2.5 基于数字相移全息的随机相位编码系统	33
2.2.6 基于 POCS 算法的随机相位编码	35
2.2.7 纯相位光学加密系统	37
2.2.8 基于分割合成滤波方法的随机相位编码	43
2.2.9 基于光学“异或”的流密码系统	47
2.2.10 基于光学联合相关器(JTC)的指纹识别系统	53
2.3 光学密码系统特点分析	55
参考文献	56

第 3 章 基于虚拟光学框架的对称密码学	60
3.1 对称密码体制的基本概念	60
3.1.1 对称密码体制概述	60
3.1.2 分组密码的基本原理和设计原则	61
3.1.3 序列密码的基本原理和设计原则	62
3.2 虚拟光学的概念	63
3.3 基于虚拟光学框架的新型分组密码算法	63
3.3.1 基于虚拟成像的多维数据加密技术	64
3.3.2 基于虚拟类全息的多维数据加密技术	66
3.3.3 基于级联相位恢复算法的光学图像加密技术	68
3.4 虚拟光学多维数据加密算法的电子学硬件实现	72
3.4.1 基于并行 DSP 的电子学硬件系统结构	72
3.4.2 TMS320C6701 并行数字信号处理器	73
3.4.3 虚拟光学多维数据加密算法的 DSP 实现详细流程	76
3.4.4 核心加/解密算法的优化	80
3.4.5 实验结果及讨论	83
参考文献	85
第 4 章 基于虚拟光学框架的公钥密码学	87
4.1 公钥密码体制的基本概念	87
4.1.1 公钥密码体制的基本原理	87
4.1.2 公钥密码算法应满足的要求	88
4.1.3 国际上几种经典的公钥密码算法	88
4.2 基于公钥概念的虚拟光学信息安全系统模型	90
4.2.1 公钥基础设施 PKI 与数字证书技术	90
4.2.2 散列函数与数字签名技术	91
4.2.3 基于公钥概念的虚拟光学信息安全系统构架	93
4.2.4 CA 签发接收方的数字证书	95
4.2.5 发送方通过验证证书来验证接收方的公钥	96
4.3 基于虚拟波前编码的光学公钥密码系统	97
4.3.1 波前传感的基本原理	97
4.3.2 基于波前传感编码的公钥密码系统	98
4.3.3 系统密钥的设计	99
4.3.4 灰度图像的非对称加/解密过程	100
参考文献	106

第 5 章 基于虚拟光学的三维空间数字水印技术	108
5.1 数字水印的基本概念	108
5.1.1 数字水印的定义	108
5.1.2 数字水印的特点	109
5.1.3 数字水印的嵌入与提取	109
5.1.4 数字水印的研究现状	110
5.2 基于光学理论与方法的数字水印技术研究现状	112
5.2.1 基于傅里叶变换全息术的数字水印技术	112
5.2.2 基于离散余弦变换域的数字全息水印技术	114
5.2.3 相移数字全息术与双随机相位编码方法相结合的数字水印技术	115
5.3 基于虚拟光学的三维空间数字水印算法	118
5.3.1 虚拟光学三维数字水印系统的理论模型	118
5.3.2 实验结果及分析	120
5.3.3 水印算法应用于数字音频信号	124
5.4 数字水印算法的改进	127
5.4.1 改进后数字水印系统的理论模型	128
5.4.2 改进算法的实验结果及分析	130
参考文献	136
第 6 章 基于计算全息的半色调图像信息隐藏	139
6.1 半色调图像信息隐藏的相关概念	139
6.1.1 印刷与半色调编码	139
6.1.2 应用于印刷品的信息隐藏技术的特性	140
6.2 基于半色调图像信息隐藏的典型方法	141
6.2.1 直接操作半色调网点的信息隐藏方法	141
6.2.2 基于罗曼全息图的半色调图像信息隐藏	141
6.3 基于计算全息图的半色调图像信息隐藏方法	143
6.3.1 基于计算全息图的半色调图像信息隐藏	144
6.3.2 隐藏信息的提取	147
6.3.3 鲁棒性检验	149
6.3.4 抗印刷信息隐藏和提取实验	152
参考文献	160
第 7 章 光学密码分析的理论基础	162
7.1 密码分析的基本概念	162
7.1.1 密码分析的基本假设——Kerckhoffs 假设	162
7.1.2 密码分析的分类	162

7.2	相位恢复技术的基本概念	163
7.3	相位恢复的若干方法	164
7.3.1	GS 算法	164
7.3.2	误差减少算法	165
7.3.3	输入-输出算法	165
7.3.4	杨-顾算法	166
7.3.5	混合投影-反射算法	166
7.3.6	松弛平均交互反射算法	170
7.3.7	差分映射算法	170
7.3.8	迭代角谱算法	171
7.4	相位恢复算法的比较与误差度量	172
7.4.1	算法的比较	172
7.4.2	误差度量	173
7.5	相位恢复的仿真实验	174
7.5.1	复值物体相位恢复	174
7.5.2	非负实值物体相位恢复	177
7.5.3	支撑大小对算法的影响	178
	参考文献	181
第 8 章	光学加密系统的密码学分析	184
8.1	引言	184
8.2	双随机相位加密系统的密码学分析	185
8.2.1	选择密文攻击	185
8.2.2	基于相位恢复的已知明文攻击方法	186
8.2.3	基于模拟退火算法的已知明文攻击	190
8.2.4	选择明文攻击	193
8.2.5	基于线性方程组求解的已知明文攻击	198
8.2.6	唯密文攻击	199
8.3	菲涅耳域双随机相位加密系统的选择明文攻击	206
8.3.1	菲涅耳域的双随机相位编码	206
8.3.2	加密系统的安全性分析	208
8.3.3	加密系统的选择明文攻击	210
8.3.4	仿真实验及分析	213
8.3.5	小结	216
8.4	基于 POCS 算法和 $4f$ 相关器的密码系统的已知明文攻击	216
8.4.1	基于 POCS 算法和 $4f$ 相关器的密码系统的基本原理	216

8.4.2 已知明文攻击过程	217
参考文献	219
附录 1	221
附录 2	223
名词索引	224

第 1 章 绪 论

1.1 信息安全

全球网络化的发展,标志着人类已经进入信息社会,网络和信息系统在人们的生活、工作和学习中发挥着越来越大的作用。随着人们对信息化期望程度的加深,一个不容忽视的新课题已经摆在人们面前,那就是网络与信息的安全问题。

信息安全技术是一门综合的学科,它涉及信息论、计算机科学和密码学等多方面的知识^[1],它的主要任务是研究计算机和通信网络内信息的安全、保密、真实、完整^[2]。随着公众信息系统和商业信息服务功能广泛覆盖于各行各业及各个领域,网络用户来自各个阶层与部门,人们对网络环境和网络信息资源的依赖程度日渐加深,网络信息的安全隐患也越来越明显地表现出来。网络信息安全涉及信息传输的安全、信息存储的安全、传输内容的审计以及对用户的鉴别和授权四个方面。为保障数据传输的安全,需采用数据传输加密技术、数据完整性鉴别技术;为保证信息存储的安全性,需保障数据库安全和终端安全;信息内容的审计是对进出内部网络的信息进行实时内容审计,以防止或追查可能的泄密行为。用户的鉴别是对网络中的主体进行验证的过程,通常有 3 种方法可以验证主体身份:一是只有该主体了解的秘密,如口令、密钥;二是主体携带的物体,如智能卡和令牌卡;三是只有该主体才具有的独一无二的特征或能力,如指纹、声音、视网膜或签字等。

随着我国国民经济和社会信息化建设的推进,金融信息化、电子商务、电子政务的快速发展,急需解决军事、经济、文化等重要领域信息系统的信息安全以提高安全防御能力。而且,任何一个国家的关键基础设施中不可能引进或采用别国的信息安全技术,只能自主开发。为了抵御国外的冲击,必须要有自主研发的信息安全技术和标准。因此,通过自主创新来研制支持信息系统建设的信息安全技术和产品,不仅具有重要的学术价值,而且具有重大的经济和社会效益。

1.1.1 密码学^[3-10]

密码技术是信息安全的核心。密码学是在编码和破译的斗争实践中逐步发展起来的,并随着先进科学技术的发展和应用,已成为一门综合性的尖端技术科学。它与数学、语言学、声学、电子学、信息论、计算机科学等有着广泛而密切的联系。随着计算机网络不断渗透到各个领域,密码学的应用也随之扩大。密码学的研究主要

包括两部分,一部分是基于数学的密码理论与技术,包括公钥密码、分组密码、序列密码、认证码、数字签名、Hash 函数、身份识别、密钥管理和公钥基础设施(PKI)等;另一部分是非数学的密码理论与技术,包括量子密码、基于生物特征识别理论与技术等。

1. 基本概念

密码学由密码编码学和密码分析学两个相互对立又相互促进的分支组成。密码编码技术的主要任务是寻求产生安全性高的有效密码算法,以满足对消息进行加密或认证的要求。密码分析技术的主要任务是破译密码或伪造认证信息,实现窃取机密信息或进行诈骗破坏活动。这两个分支既相互对立又相互依存。正是由于这种对立统一关系,才推动了密码学自身的发展。通常将待加密的消息称为明文,加密后的消息称为密文;加密就是从明文得到密文的过程;合法地由密文恢复出明文的过程称为解密;表示加密和解密过程的数学函数称为密码算法;实现这种变换过程需要输入的参数称为密钥。密钥可能的取值范围称为密钥空间。密码算法、明文、密文和密钥组成密码系统。根据密码算法所使用的加密密钥和解密密钥是否相同,还可将密码体制分为对称密码体制和非对称密码体制。对称密码体制的基本特征是加密密钥和解密密钥相同,其优点是具有很高的保密强度,加密速度快,但密钥必须通过安全可靠的途径传递,密钥管理成为影响系统安全的关键性因素。非对称密码体制的主要特征是加密密钥和解密密钥不同,可以适应开放性的使用环境,密钥管理问题相对简单,可以方便、安全地实现数字签名和验证。

2. 对称密码算法

对称密码算法的特征是加密和解密采用同一个密钥。如图 1-1 所示。按照对明文处理方式的不同,可以分为流密码(又称序列密码)与分组密码。

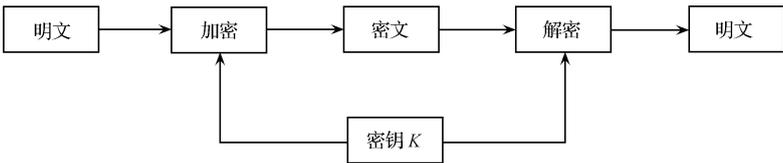


图 1-1 对称密码系统

序列密码属于对称密码体制的一种。设明文流为 $P = p_1 p_2 \cdots p_n$, 密钥流为 $K = k_1 k_2 \cdots k_n$ (密钥流由密钥或种子密钥通过密钥流生成器得到), 通过密钥流与明文流逐位应用“异或”运算得到密文, 表示为 $C = c_1 c_2 \cdots c_n$, 其中 $c_i = E_{k_i}(m_i) (i = 1, 2, \cdots, n)$ 。序列密码具有软件实现简单、便于硬件实现、加/解密处理速度快、没有或只有

有限的错误传播等特点,因此在实际应用中,特别是专用或机密机构中保持着优势,典型的应用领域包括无线通信和外交通信。目前,公开的序列密码算法主要有 RC4、SEAL 等。

对称密码体制中的另一种是分组密码。与序列密码每次加密处理数据流的一位或一个字节不同,分组密码处理的单位是一组明文,即将明文消息编码后的数字序列 $p_0, p_1, p_2, \dots, p_i$ 划分成长为 L 位的组 $P = (p_1, p_2, p_3, \dots, p_L)$, 各个长为 L 的分组分别在密钥 $K = (k_1, k_2, k_3, \dots, k_l)$ 的控制下变换成与明文组等长的一组密文输出 $C = (c_1, c_2, c_3, \dots, c_L)$, L 通常为 64 或 128, 分组密码的模型如图 1-2 所示。

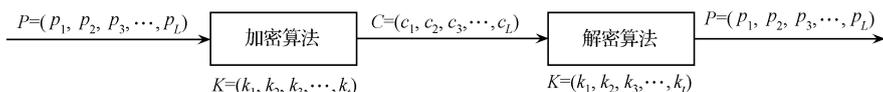


图 1-2 分组密码模型

最著名的对称分组算法是数据加密标准(DES),它是由 IBM 公司提出的,并于 1977 年被采纳为美国联邦标准。作为第一个标准化的加密体制,DES 无疑是密码学历史上的一个里程碑。DES 的基本思想是把二进制序列的明文分为每 64bit 一组,对每组先作初始置换 IP,把置换后的 64bit 的左边 32bit 记为 L_0 ,右边 32bit 记为 R_0 ,然后用 56bit 的密钥作 16 轮替换和换位运算,再经逆初始置换 IP^{-1} 形成密文。DES 的一种改进是 3DES,效果相当于将 DES 密钥长度加倍。目前常使用的另一种对称加密算法是国际数据加密算法(IDEA),密钥长度为 128bit。由于计算机能力的迅速增强,DES 已不能完全适应网络时代信息安全的要求,高级加密标准(AES)成为新一代密码算法标准。

在对称密码体制下,密钥需要经过安全的通道由发送方传递给接受方。这种密码体制的优点是:安全性高,加/解密速度快。缺点是:密钥管理和分发过程十分复杂,代价高;无法实现数字签名。

3. 公钥密码算法

Diffie 和 Hellman 于 1976 年发表了“密码学新方向”一文^[11],提出了公钥密码算法。这是密码学历史上的又一个里程碑。它既有效地克服了对称密码算法的密钥分发问题,又可用于数字签名等功能,为网络时代的信息安全提供了新的理论和技术基础。采用公钥加密体制的系统如图 1-3 所示。公钥密码算法的特点是每个用户有两个密钥,一个公开作为加密密钥,称为公钥;另一个作为用户专用的解密密钥,称为私钥。用抽象的观点来看,公钥密码就是一种陷门单向函数。可以说一个函数 f 是单向函数,即若对它的定义域中的任意 x 都易于计算 $f(x)$,而对 f 的值域中的几乎所有的 y ,即使当 f 为已知时要计算 $f^{-1}(y)$ 在计算上也是不可行的。

若当给定某些辅助信息(陷门信息)时,则易于计算 $f^{-1}(y)$,就称单向函数 f 是一个陷门单向函数。公钥密码体制就是基于这一原理而设计的,将辅助信息(陷门信息)作为私钥。这类密码的安全强度取决于它所依据问题的计算复杂度。目前国际上已经提出了许多种公钥密码体制,但比较流行的主要有两类:一类是基于大整数因子分解问题的方法,其中最典型的代表是 RSA;另一类是基于离散对数问题的方法,比如 ElGamal 公钥密码和椭圆曲线公钥密码。

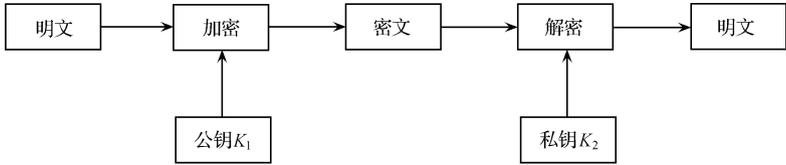


图 1-3 公钥密码系统

公钥密码算法的缺点在于其速度较慢,因此不适合加密数据量大的文件。在实际应用中,人们通常是将对称密码算法和公钥密码算法结合起来使用,用对称密码算法来加密数据文件,而用公钥密码算法来传递对称密码算法所使用的密钥。这样就既能利用对称密码算法的速度,又能有效解决密钥分发的问题。

1.1.2 信息隐藏

信息隐藏是信息安全的另一个重要的核心技术。信息隐藏是将机密信息隐藏在普通的信息之中而不露破绽。信息隐藏不同于传统的密码学技术。密码学技术仅仅隐藏了信息的内容,而信息隐藏不但隐藏了信息的内容而且隐藏了信息的存在。对加密通信而言,可能的监测者或非法拦截者可截取密文并对其进行破译,或将密文进行破坏后再发送,从而影响机密信息的安全;但对信息隐藏而言,可能的监测者或非法拦截者难以从公开信息中判断机密信息是否存在或截获机密信息,从而保证机密信息的安全^[12-16]。

1. 基本概念

通常,人们把希望被秘密隐藏的对象称为嵌入对象(embedded object),它含有特定用途的秘密信息或重要信息。用于隐藏嵌入对象的非保密载体称为载体对象(cover object)。将嵌入对象添加到载体对象中得到隐藏对象的过程称为信息嵌入(information embedding)。从隐藏对象中重新获得嵌入对象的过程称为信息提取(information extracting)。

数字水印是信息隐藏最重要的一个分支,也是目前国际学术界研究的一个前沿热门方向。数字水印为计算机网络上的多媒体产品的版权保护等问题提供了有效的解决方案。它通过在原始数据中嵌入秘密信息(水印)来证实该数据的所有权

嵌入的水印可以是一段文字、标识、序列号等。水印通常是不可见或不可察觉的,它与原始数据紧密结合并隐藏其中,成为源数据不可分离的一部分,并可以经历一些不破坏源数据使用价值或商用价值的操作而存活下来^[17-19]。

信息之所以能够隐藏在多媒体数据中是因为:①多媒体本身存在很大的冗余性。从信息论的角度看,未压缩的多媒体信息是编码效率很低的,所以这些机密信息嵌入到多媒体信息中进行密码传送是完全可行的,并不会影响多媒体信息本身的传送和使用;②人眼或人耳本身对某些信息都有一定的掩蔽效应,比如:人眼对灰度的分辨率只有几十个灰度级;对边缘附近的信息不敏感。利用人的这些特点,可以很好地将信息隐藏而不被察觉。

2. 分类及特点

Petitcolas 等对信息隐藏技术作了较好的分类,如图 1-4 所示^[19]。信息隐藏的主要方法包括在时间域、空间域、变换域的隐藏,另外还有基于文件格式和载体生成技术的隐藏^[20,21]。

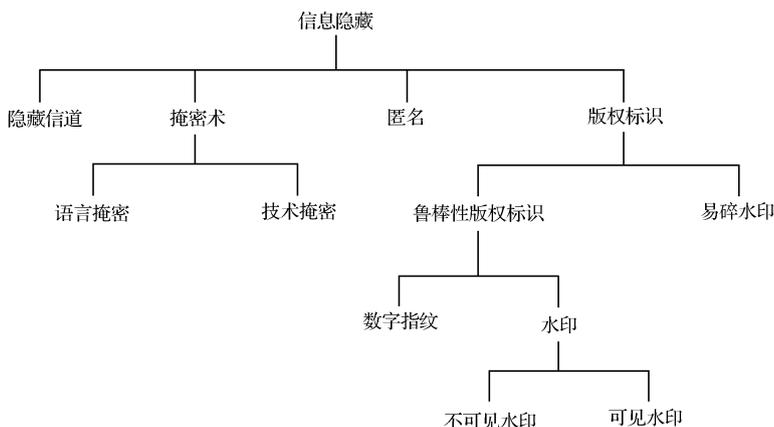


图 1-4 信息隐藏技术分类

信息隐藏技术必须考虑正常的信息操作所造成的威胁,即要使机密资料对正常的的数据操作技术具有免疫力。这种免疫力的关键是要使隐藏信息部分不易被正常的的数据操作(如通常的信号变换或数据压缩)所破坏。根据信息隐藏的目的和技术要求,该技术存在以下特性^[1,12]。

1) 不可感知性:利用人类视觉或听觉系统属性,经过一系列隐藏处理,使隐藏对象没有明显的降质现象,而嵌入对象却无法人为地看见或听见。有些极个别应用场合可能需要使用可见水印。

2) 鲁棒性:指不因隐藏对象通过某种常用信号处理操作而导致嵌入对象丢失

的能力。这里所说的信号处理操作包括滤波、有损压缩、打印、扫描、几何变换、D/A 或 A/D 转换等。

3) 安全性:指隐藏算法具有较强的抵抗恶意攻击能力,即它必须能够承受一定程度的人为攻击,而使嵌入对象不被破坏。与信息加密一样,信息隐藏技术最终也需要把对信息的保护转化为对密钥的保护。因此密码学中对密钥的要求也适用于信息隐藏技术,如必须有足够大的密钥空间等。

4) 不可检测性:指隐藏对象与载体对象需具有一致的特性,如具有一致的统计噪声分布等,从而使得恶意攻击者无法判断隐藏对象中是否有嵌入对象。

5) 自恢复性:经过某些操作和变换后,可能会使隐藏对象产生较大的破坏。如果只从留下的片段数据,仍能恢复嵌入信号,而且恢复过程不需要载体信号,这就是所谓的自恢复性。并不是所有应用场合都需要自恢复性。

6) 对称性:通常信息的隐藏与提取过程具有对称性,包括编码、加密方式,以减少存取难度。

1.2 光学信息安全技术

基于光学理论与方法的数据加密和信息隐藏技术是近年来在国际上开始起步发展的新一代信息安全理论与技术^[22]。并行数据处理是光学系统固有的能力,如在光学系统中一幅二维图像中的每一个像素都可以同时地被传播和处理。当进行大量信息处理时,光学系统的并行处理能力很明显占有绝对的优势,并且,所处理的图像越复杂,信息量越大,这种优势就越明显。同时,光学加密装置比电子加密装置具有更多的自由度,信息可以被隐藏在多个自由度空间中。在完成数据加密或信息隐藏的过程中,可以通过计算光的干涉、衍射、滤波、成像、全息等过程,对涉及的波长、焦距、振幅、光强、相位、偏振态、空间频率及光学元件的参数等进行多维编码。与传统的基于数学的计算机密码学和信息安全技术相比,光学信息安全技术具有多维、大容量、高设计自由度、高鲁棒性、天然的并行性、难以破解等诸多优势^[23]。

1.2.1 光学安全认证技术

光学图像安全认证系统,通常采用 Vander Lug 相关器(VLC)或联合变换相关器(JTC)作相关检验来判别真伪,安全性很高^[24~31]。

VLC 实际上是一个频谱面相关器,它是通过利用傅里叶频谱面的掩膜来进行图像识别的匹配滤波的光学相关系统。通常,将待认证图案置于输入面,在频谱面上放置空间匹配滤波器做匹配滤波。如果滤波函数与输入信号相匹配,则在输出面上能产生高于阈值的相关峰值,通过 CCD 或 CMOS 等光强探测器件可以检测到

认证信号。

JTC 是由 Weaver 和 Goodman 提出的一种光学相关系统。较之 VLC, JTC 产生的相关峰值相对较低,但却克服了前者的诸如结构复杂、对两块傅里叶透镜焦点对准精度要求极其苛刻、空间带宽积不够大等缺点,并且相关峰值低的这一缺点可以通过功率谱相减技术^[28]得到改进。目前 JTC 已经广泛应用于光学信息处理、模式识别和光学神经网络等方面^[22]。验证时,将参考信号和输入信号同时分别置于输入端的两个半平面上,在相干光的照射下,在第一个透镜的后焦面上可以记录得到联合变换的傅里叶功率谱,然后联合变换的傅里叶功率谱再经过另一次傅里叶变换就可得到相关输出,利用 CCD 接收可以实现相关峰值的检测。

1991 年,Fielding 和 Homer 等提出了基于二元联合变换相关器(BJTC)的光学指纹识别系统^[30],该系统可实时处理并具有较好的识别性能,这是最早开始的光学生物特征识别的研究之一。20 世纪 90 年代中期,Javidi 和 Homer 首先提出了用随机相位编码对图像加密和防伪的理论^[24]。采用随机相位编码技术对图样编码,可以将用来作为防伪标识的图样在密钥的控制下编码为强度探测器难以感知的随机相位掩膜,具有安全性能高、鲁棒性好等特点,可广泛应用于信息的保密和防伪技术中,解决诸如信用卡、身份证、护照、大额票据、乃至高技术产品等的防伪问题。这些工作正式开启了光学信息安全研究的先河。

近年来,光学信息处理技术在生物测定的研究方面取得了引人注目的进展,1999 年,Weber 和 Trolinger 提出基于光学非线性联合变换相关器(NJTC)原理的生物测定方法^[29],该方法不仅在身份证、护照、信用卡的防伪检测以及访问控制的身份安全认证中显示出极大的潜力,而且有可能与数字网络集成。Stoianov 等提出了一种利用光学相关器的高速指纹识别系统^[31]。2004 年,美国国家标准技术研究所(NIST)的 Watson 等也报道了他们在光学生物特征识别方面的研究进展^[32]。

1.2.2 基于光学理论与方法的数据加密

在采用光学方法对数据进行加密和解密方面,美国 Connecticut 大学 Javidi 教授课题组的研究成果在该领域最具有代表性。自 1995 年 Refregier 和 Javidi 首次提出在标准 $4f$ 光信号处理器中通过双随机相位编码进行数据加密的光学方法^[33]以来(图 1-5),不断发表了与该技术相关的、采用光学方法实现图像加密和解密的研究报道^[22,34~38],并获得多项基于此技术的美国专利保护^[39~42]。2000 年 Javidi 和 Nomura 将双随机相位编码加密方法与数字全息技术结合起来,构建了一种可能用于视频存储和传输的安全系统^[43]。Wang 等深入研究了双随机相位加密系统中解密图像的信噪比,提出了一种改进系统容偏能力的方法^[44]。Tajahuerce 等将相移数字全息术与双随机相位编码加密方法相结合来加密信息^[45]。相移数字全息术可以更有效地利用 CCD 的带宽。测量相位信息比数字记录离轴全息图精确得多。

并且这种加密技术在解密时只需一步基于快速傅里叶变换的重建过程。Mogensen 等基于广义相衬技术,提出了一种纯相位光学加密技术^[46]。2001 年,Mogensen 等又利用铁电空间光调制器在实验室构建了一种高速、大容量的光学加密系统^[47]。

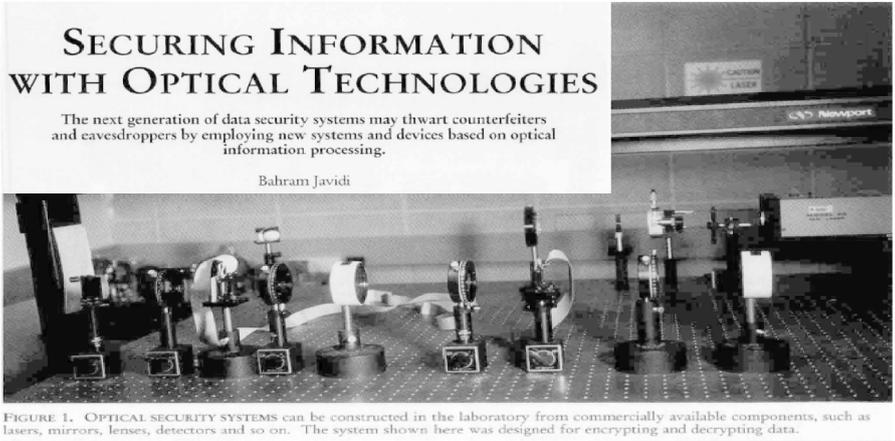


图 1-5 Javidi 首次提出的双随机相位编码光学加密系统(*Physics Today*, 1997)

分数傅里叶变换是一类称为规范变换或二次相位变换的广义积分变换族中的一员。分数傅里叶变换推广了传统傅里叶变换,传统傅里叶变换实际上是分数傅里叶变换的一阶形式。分数傅里叶变换在微分方程、量子力学、量子光学、光学衍射理论、光束传播(包括激光)、光学系统、光学信号处理、频扫滤波器、时变滤波与混频、模式识别、时-频分布的研究中具有极其广泛的应用潜力^[48-51]。在利用分数傅里叶变换技术完成光学图像加密方面,2000 年印度理工学院(IIT)的 Unnikrishnan 等提出用分数傅里叶变换域来代替双随机相位编码系统中的傅里叶变换域,即分数傅里叶变换域双随机相位编码思想^[52]。Unnikrishnan 等构建的光学加密系统与 Javidi 等的 $4f$ 加密系统类似,均是把两块统计无关的随机相位模板分别置于光学系统的输入平面和加密平面,分别对原始图像 $f(x, y)$ 的空间信息和分数傅里叶域信息做随机扰乱,在系统输出平面将得到平稳白噪声。除了随机相位模板密钥外,加密系统中涉及的分数傅里叶变换的阶数及输入、输出尺度因子等也可被设计成为密钥。这种加密方案不仅增加了系统的安全性,同时也具有较好的抗噪性能。随后,Zhu 等提出了一种多重分数傅里叶变换加密算法,算法的解密过程不仅对分数级次,而且对变换周期十分敏感,具有良好的安全性。由于该算法并非通过与其他随机代码进行相关或卷积运算获得加密效果,因而具有抵抗盲解卷积特性,也无需考虑相干谱噪声的影响^[53,54]。2001 年 Liu 等提出了一种基于级联分数傅里叶变换的光学图像加密系统^[55],进一步提高了系统的安全性。Unnikrishnan 和 Singh 研究了二次相位加密系统中分数傅里叶变换阶数及尺度因子等参数取值的优化问

题,并给出了设计二次相位加密系统的一般流程^[56]。

在采用光学方法设计流密码方面,1997年 Madjarova 等首次用光学方法实现了基于细胞自动机(cellular automata)的流密码算法^[57]。1999年 Zhang 和 Karim 利用混合细胞自动机代替单一细胞自动机作为密钥流生成器,提出了一种新的光学流密码系统^[58]。这种方法增加了攻破系统密钥流生成器的复杂度,提高了流密码系统的安全性。Han 等利用偏振编码原理实现光学“异或(XOR)”操作,构造了设计流密码的光学组件^[59]。该技术通过输入图像与密钥“位流”之间的光学“异或”操作来实现图像加密。密钥“位流”是由数字算法生成,因为它是二值的,所以需要将一幅灰度输入图像转换为8个位平面。密钥“位流”和位平面之间的光学“异或”操作可以利用偏振编码原理来实现。用 CCD 记录光学“异或”的结果,然后将它们转换成灰度图像的形式,就可以最终得到加密灰度图像。2000年 Sasaki 等利用光学仿射变换构造了一种新的流密码系统并分析了其实现性能^[60]。

自2005年以来,采用光学方法对数据进行加密的最新进展还包括:Situ 和 Zhang 将波长复用技术引入到了菲涅耳域的双随机相位加密系统中^[61],完成了多幅图像的加密,并分析了系统的最小波长间隔和复用容量等问题;Chen 等提出的基于分数小波变换(FWT)的光学图像加密方法^[62];Barrera 等给出了一种利用波带片完成的光学图像加密技术^[63];Hennelly 和 Sheridan 研究了基于傅里叶变换、分数傅里叶变换、菲涅耳变换、广义线性规范变换等光学信号处理技术的图像加密系统中的空间带宽积问题,分析了加密系统的性能及参数取值问题^[64]。Doh 等提出了一种能够保护个人身份识别信息的光学安全系统^[65];2006年 Kim 和 Lee 提出了一种新颖的体全息图光学加密系统^[66]。

近年来,获得的其他与光信息安全有关的国外专利还包括:Steenblick 和 Hurt 的“光学图像加密和解密过程”^[67];Tomko 和 Stoinaov 的“利用指纹加密和解密的全息方法”^[68];Jackson 的“光学加密接口”^[69];Moorhouse 等的“光学安全系统”^[70]以及 Gluckstad 的“光学加密和解密的方法及系统”^[71]等。

1.2.3 基于光学理论与方法的信息隐藏

信息光学理论除了在密码学研究方面显示出极大的潜力外,在发展新的信息隐藏理论与技术方面也表现出极大的活力。2002年 Takai 和 Mifune 提出利用全息技术可以进行数字水印的研究^[72]。该方法首先将水印信息用随机相位函数调制并用傅里叶变换全息术记录下来数字全息图,接着将宿主图像经过低通滤波器进行滤波以去除高频分量,最后将得到的数字全息图加载于低通滤波后的宿主信息上,从而完成水印的嵌入过程。水印提取的过程非常简单,只需对嵌入水印后的载体数据进行逆傅里叶变换即可提取出水印信息。该水印技术具有较强的鲁棒性和抗攻击性,尤其具有抗剪切的特点。但是,由于在水印的嵌入过程中对宿主信息进

行了低通滤波操作,因此会使嵌入水印后的图像信息产生较明显的降质。Kishk 和 Javidi 提出了一种基于双随机相位编码技术的信息隐藏方法^[73],该方法使欲隐藏的信息 $f(x, y)$ 在空间域受到随机相位函数密钥 $\exp[j2\pi p(x, y)]$ 的调制,在频率域被随机相位函数密钥 $\exp[j2\pi b(v, w)]$ 滤波,从而得到经过双随机相位编码加密后的结果,将该结果加载到宿主信息之上即可完成信息的隐藏过程。提取隐藏信息时,首先对含有隐藏信息的图像进行傅里叶变换并与解密密钥 $\exp[-j2\pi b(v, w)]$ 相乘,然后再对得到的结果进行逆傅里叶变换并与另一解密密钥 $\exp[-j2\pi p(x, y)]$ 相乘,即可提取出隐藏信息。由于采用了双随机相位编码技术,该信息隐藏方法具有较强的抗噪声能力,并能较好地抵抗剪切、数据压缩等常见的信号处理操作,具有较强的鲁棒性。2003 年 Kishk 和 Javidi 提出了利用相移数字全息技术与双随机相位编码加密技术相结合的方法在三维物体中嵌入水印^[74]。该方法首先通过相移数字全息技术获得三维宿主物体的全息图,水印信息经过双随机相位编码加密后被嵌入到该全息图中去。随后,他们又提出了用类似的方法在三维物体中嵌入三维水印的技术^[75]。该技术首先通过相移数字全息技术分别获得三维宿主物体和三维水印的全息图,然后将获得的三维水印的全息图进行双随机相位编码加密并嵌入到三维宿主物体的全息图中。最终,嵌入水印后的全息图再次经过双随机相位编码加密以增强其安全性。

最近,Chang 和 Tsan 改进了 Takai 和 Mifune 提出的基于数字全息的水印技术,提出了一种离散余弦变换(DCT)域的数字全息水印技术^[76],极大地改善了 Takai 和 Mifune 水印算法中所存在的宿主信息嵌入水印后的明显降质问题。Chang 和 Tsan 的水印方法首先将水印信息用随机相位函数调制并用傅里叶变换全息术记录下来数字全息图,接着将宿主图像作离散余弦变换并将数字全息图加载到中频系数上去,然后再进行逆离散余弦变换以得到嵌入水印后的图像。提取水印时,首先计算嵌入水印后图像的离散余弦变换并从中提取出嵌入的数字全息图,接着再进行一次逆傅里叶变换即可提取出水印信息。由于该水印方法避免了在水印嵌入过程中对宿主信息进行的低通滤波操作,因此显著提高了嵌入水印后的图像质量。实验结果表明,该方法能有效抵抗叠加噪声、剪切、低通滤波等常见的信号处理操作,具有较强的鲁棒性。Kim 和 Lee 研究了采用相移数字全息术和双随机相位编码加密在三维物体中嵌入水印时,控制水印添加强度的尺度因子 w 的最优取值问题^[77]。Situ 和 Zhang 提出了一种级联迭代傅里叶变换算法用于把图像加密成为若干个具有随机分布的相位函数,并将该算法用于光学图像隐藏^[78]。Cheng 等利用数字全息技术进行了水印技术的研究,水印的嵌入与提取过程均采用光学方法实现,充分发挥了光学信息处理的能力^[79]。

1.2.4 国际学术组织的活动

近年来,国际光学工程学会(SPIE)、国际电子电气工程师协会(IEEE)、美国光

学学会(OSA)、国际光学委员会(ICO)等国际学术组织召开了多次专题国际会议,并多次发行了光学信息安全方面的会议论文集,为国际学术界建立了广泛的学术交流平台。*Optical Engineering* 分别在1996年、1999年、2004年出版了3期基于光学信息处理技术的光学信息安全、加密、认证、隐藏等方面的期刊专辑^[80~82]。特别值得注意的是,“911事件”后美国政府开始了一项耗资巨大的所谓“国土安全计划”(homeland security),其中涉及庞大的有关光信息安全的研究与开发,与之有关的研究结果的报道最近已经成为 SPIE 最热门的议题之一。

1.2.5 国内的研究进展情况

在国内,一些研究人员也积极地投入到了光学信息安全理论与技术的研究中,并已经取得了一定的进展。例如,刘树田等研究了分数傅里叶变换在光学图像加密和模式识别等方面的应用,提出将广义分数卷积概念应用于光学图像加密,进而又发展了一种多重分数傅里叶变换加密算法^[53~55]。刘福民等提出了一种基于相息图迭代的随机相位加密方法。该方法通过在随机谱和相息图之间进行相位恢复迭代以确定相息图和密钥的相位分布,因而能够减小图像的解密误差^[83]。杨晓苹等采用基于记忆的模拟退火法对双随机相位加密中的相息图进行了优化设计^[84]。于斌和彭翔提出了一种基于级联相位恢复算法的光学图像加密方法^[85],该方法利用级联迭代角谱相位恢复算法把待加密图像分别编码到两块相位模板之中,从而实现图像的加密。司徒国海和张静娟提出了一种菲涅耳域的双随机相位编码加密技术^[86],并分析了该技术的性能,进而在该系统中引入波长复用技术实现了多图像加密^[61]。山东大学在利用相移干涉技术完成图像加密和水印方面进行了研究^[87,88]。华南师范大学、苏州大学、中国科学院西安光机所、深圳大学等研究单位的部分人员也在开展光学信息安全相关方面的研究^[89~91]。但是从总体上来说,国内在光学信息安全理论与技术领域的研究尚处于初步的探索性阶段,仍然缺乏全面系统和更加深入的研究。作者的课题组在虚拟光学密码学和信息隐藏,以及光学密码分析方面也进行了一系列的研究与探索^[92~105]。

参 考 文 献

- 1 孙圣和,陆哲明,牛夏牧,等. 数字水印技术及应用. 北京:科学出版社,2004:4~10
- 2 冯登国. 计算机通信网络安全. 北京:清华大学出版社,2001:2~4
- 3 Stallings W. *Cryptography and Network Security: Principles and Practice*. 2nd ed. NJ: Prentice Hall, 1999
- 4 Schneier B. *Applied Cryptography: Protocols, Algorithms, and Source Code in C*. NY: Wiley, 1996
- 5 王衍波,薛通. 应用密码学. 北京:机械工业出版社,2003:30~32

- 6 蔡乐才. 应用密码学. 北京:中国电力出版社,2005: 1~ 5
- 7 章照止. 现代密码学基础. 北京:北京邮电大学出版社,2004: 1~ 3
- 8 杨波. 现代密码学. 北京:清华大学出版社,2003: 1~ 8
- 9 孙淑玲. 应用密码学. 北京:清华大学出版社,2004: 9~ 30
- 10 胡子濮,张玉清,肖国镇. 对称密码学. 北京:机械工业出版社,2002: 2~ 15
- 11 Diffie W, Hellman M. New directions in cryptography. *IEEE Transactions on Information Theory*, 1976, 22(6): 644~ 654
- 12 王丽娜,张焕国. 信息隐藏技术与应用. 武汉:武汉大学出版社,2003: 1~ 12
- 13 钮心忻. 信息隐藏与数字水印. 北京:北京邮电大学出版社,2004: 117~ 130
- 14 冯登国. 国内外密码学研究现状及发展趋势. *通信学报*, 2002, 23(5): 18~ 26
- 15 杨义先,钮心忻. 多媒体信息伪装综论. *通信学报*, 2002, 23(5): 32~ 38
- 16 易开祥. 数字图像加密与数字水印技术研究[博士学位论文]. 浙江大学, 2001
- 17 Hartung F, Kutter M. Multimedia Watermarking Techniques. *Proc IEEE*, 1999, 87(7): 1079~ 1107
- 18 Hartung F, Ramme F. Digital rights management and watermarking of multimedia content for M-commerce applications. *IEEE Communication Magazine*, 2000, 38(11): 78~ 84
- 19 Langelaar G, Setyawan I, Lagendijk R. Watermarking digital image and video data, a state-of-the-art overview. *IEEE Signal Processing Magazine*, 2000, 17(5): 20~ 46
- 20 Petitcolas F, Anderson R J, Kuhn M G. Information hiding—a survey. *Proc IEEE*, 1999, 87(7): 1062~ 1078
- 21 陈明奇,钮心忻,杨义先. 多址隐像术. *通信学报*, 1999, 20(12): 59~ 64
- 22 Javidi B. Securing information with optical technologies. *Physics Today*, 1997, 50(3): 27~ 32
- 23 张鹏. 基于信息光学的多维数据加密及数字水印[博士学位论文]. 天津大学, 2006
- 24 Javidi B, Homer J. Optical pattern recognition for validation and security verification. *Optical Engineering*, 1994, 33(6): 1752~ 1756
- 25 Javidi B, Sergeant A. Fully phase encoded key and biometrics for security verification. *Optical Engineering*, 1997, 36(3): 935~ 942
- 26 Javidi B. Optical spatial filtering for image encryption and security system. *SPIE*, 1997, 3386: 14~ 23
- 27 Javidi B, Zhang G, Li J. Experimental demonstration of the random phase encoding technique for image encryption and security verification. *Optical Engineering*, 1996, 35(9): 2506~ 2512
- 28 Soon B, Kari M, Alam M. Using the joint transform correlator as the feature extractor for the nearest neighbor classifier. *Optical Engineering*, 1999, 38(1): 39~ 46
- 29 Weber D, Trolinger J. Novel implementation of nonlinear joint transform correlators in optical security and validation. *Optical Engineering*. 1999. 38(1): 62~ 68

- 30 Fielding K, Horner J, Makekau C. Optical fingerprint identification by binary joint transform correlation. *Optical Engineering*, 1991, 30(12): 1958~ 1961
- 31 Stoianov A, Soutar C, Graham A. High-speed fingerprint verification using an optical correlator. *Optical Engineering*, 1999, 38(1): 99~ 107
- 32 Watson C, Casasent D. Recognition of live-scan fingerprints with elastic distortions using correlation filters. *Optical Engineering*, 2004, 43(10): 2274~ 2282
- 33 Refregier P, Javidi B. Optical image encryption based on input and Fourier plane random encoding. *Optics Letters*, 1995, 20(7): 767~ 769
- 34 Javidi B, Sergent A, Zhang G, et al. Fault tolerance properties of a double phase encoding encryption technique. *Optical Engineering*, 1997, 36(4): 992~ 998
- 35 Javidi B, Zhang G, Li J. Encrypted optical memory using double-random phase encoding. *Applied Optics*, 1997, 36(5): 1054~ 1058
- 36 Goudail F, Bollaro F, Javidi B, et al. Influence of perturbation in a double phase-encoding system. *Journal of the Optical Society of America A*, 1998, 15(10): 2629~ 2638
- 37 Javidi B, Bernard L, Towghi N. Noise performance of double-phase encryption compared to XOR encryption. *Optical Engineering*, 1999, 38(1): 9~ 19
- 38 Matoba O, Javidi B. Encrypted optical memory system using three dimensional keys in the Fresnel domain. *Optics Letters*, 1999, 24(11): 762~ 764
- 39 Javidi B. Method and apparatus for encryption; U. S. , 5903648. 1999
- 40 Javidi B. Method and apparatus for encryption; U. S. , 6002773. 1999
- 41 Javidi B, Osamu M. Method and apparatus for secure ultrafast communication; U. S. , 20020150242. 2002
- 42 Javidi B. Method and apparatus for encryption using partial information; U. S. , 6519340. 2003
- 43 Javidi B, Nomura T. Securing information by use of digital holography. *Optics Letters*, 2000, 25(1): 28~ 30
- 44 Wang B, Sun C, Su W, et al. Shift-tolerance property of an optical double-random phase-encoding encryption system. *Applied Optics*, 2000, 39(26): 4788~ 4793
- 45 Tajahuerce E, Matoba O, Verrall S, et al. Optoelectronic information encryption with phase-shifting interferometry. *Applied Optics*, 2000, 39(14): 2313~ 2320
- 46 Mogensen P, Gluckstad J. Phase-only optical encryption. *Optics Letters*, 2000, 25(8): 566~ 568
- 47 Mogensen P, Eriksen R, Gluckstad J. High capacity optical encryption system using ferroelectric spatial light modulator. *Journal of Optics A: Pure and Applied Optics*, 2001, 3(1): 10~ 15
- 48 Almeida L. The fractional Fourier transform and time-frequency representations. *IEEE Transactions on Signal Processing*, 1994, 42(11): 3084~ 3091
- 49 Ozaktas H M. Mendlovic D. Fractional Fourier optics. *Journal of the Optical Society of*

- America A, 1995, 12(4): 743~ 751
- 50 Ozaktas H, Arıkan O, Kutay M, et al. Digital computation of the fractional Fourier transform. *IEEE Transactions on Signal Processing*, 1996, 44(9): 2141~ 2149
- 51 Zayed A. A class of Fractional integral transforms: a generalization of the fractional Fourier transform. *IEEE Transactions on Signal Processing*, 2002, 50(3): 619~ 627
- 52 Unnikrishnan G, Joseph J, Singh K. Optical encryption by double-random phase encoding in the fractional Fourier domain. *Optics Letters*, 2000, 25(12): 887~ 889
- 53 Zhu B, Liu S, Ran Q. Optical image encryption based on multifractional Fourier transforms. *Optics Letters*, 2000, 25(16): 1159~ 1161
- 54 朱邦和. 基于分数傅里叶变换的光学安全和模式识别[博士学位论文]. 哈尔滨工业大学, 2003
- 55 Liu S, Yu L, Zhu B. Optical image encryption by cascaded fractional Fourier transforms with random phase filtering. *Optics Communications*, 2001, 187(1~ 3): 57~ 63
- 56 Unnikrishnan G, Singh K. Optical encryption using quadratic phase system. *Optics Communications*, 2001, 193(1~ 6): 51~ 67
- 57 Madjarova M, Kakuta M, Yamaguchi M, et al. Optical implementation of the stream cipher based on the irreversible cellular automata algorithm. *Optics Letters*, 1997, 22(21): 1624~ 1626
- 58 Zhang S, Karim M. High-security optical integrated stream ciphers. *Optical Engineering*, 1999, 38(1): 20~ 24
- 59 Han J, Park C, Ryu D, et al. Optical image encryption based on XOR operations. *Optical Engineering*, 1999, 38(1): 47~ 54
- 60 Sasaki T, Togo H, Tanida J, et al. Stream cipher based on pseudorandom number generation with optical affine transformation. *Applied Optics*, 2000, 39(14): 2340~ 2346
- 61 Situ G, Zhang J. Multiple-image encryption by wavelength multiplexing. *Optics Letters*, 2005, 30(11): 1306~ 1308
- 62 Chen L, Zhao D. Optical image encryption based on fractional wavelet transform. *Optics Communications*, 2005, 254(4~ 6): 361~ 367
- 63 Barrera J, Henao R, Torroba R. Optical encryption method using toroidal zone plates. *Optics Communications*, 2005, 248(1~ 3): 35~ 40
- 64 Hennelly B, Sheridan J T. Optical encryption and the space bandwidth product. *Optics Communications*, 2005, 247(4~ 6): 291~ 305
- 65 Doh Y, Yoon J, Choi K, et al. Optical security system for the protection of personal identification information. *Applied Optics*, 2005, 44(5): 742~ 750
- 66 Kim H, Lee Y. Encryption of a volume hologram by complementary input image and binary amplitude mask. *Optics Communications*, 2006, 258(1): 9~ 17
- 67 Steenblich R, Hurt M. Optical image encryption and decryption process: U. S. , 5715316. 1998

- 68 Tomko G, Stoinaov A. Holographic method for encrypting and decrypting information using a fingerprint: U.S. , 5740276. 1998
- 69 Jackson D. Optical encryption interface: U.S. , 5793871. 1998
- 70 Moorhouse J, Bodin M, Larsen K. Optical security system: U.S. , 6499660. 2002
- 71 Gluckstad J. Optical encryption and decryption method and system: U.S. , 6907124. 2005
- 72 Takai N, Mifune Y. Digital watermarking by a holographic technique. *Applied Optics*, 2002, 41(5): 865~ 873
- 73 Kishk S, Javidi B. Information hiding technique with double phase encoding. *Applied Optics*, 2002, 41(26): 5462~ 5470
- 74 Kishk S, Javidi B. Watermarking of three-dimensional objects by digital holography. *Optics Letters*, 2003, 28(3): 167~ 169
- 75 Kishk S, Javidi B. 3D object watermarking by a 3D hidden object. *Optics Express*, 2003, 11(8): 874~ 888
- 76 Chang H, Tsan C. Image watermarking by use of digital holography embedded in the discrete-cosine-transform domain. *Applied Optics*, 2005, 44(29): 6211~ 6219
- 77 Kim H, Lee Y. Optimal watermarking of digital hologram of 3-D object. *Optics Express*, 2005, 13(8): 2881~ 2886
- 78 Situ G, Zhang J. Image hiding with computer-generated phase codes for optical authentication. *Optics Communications*, 2005, 245(1~ 6): 55~ 65
- 79 Cheng C, Lin L, Dai W. Construction and detection of digital holographic watermarks. *Optics Communications*, 2005, 248(1~ 3): 105~ 116
- 80 Horner J, Javidi B, et al. Special issue on optical security. *Optical Engineering*, 1996, 35(9): 2451~ 2547
- 81 Horner J, Javidi B, et al. Special issue on optical security. *Optical Engineering*, 1999, 38(1): 8~ 119
- 82 Javidi B, et al. Special issue on optics and photonics for homeland security. *Optical Engineering*, 2004, 43(10): 2222~ 2311
- 83 刘福民, 翟宏琛, 杨晓苹. 基于相息图迭代的随机相位加密. *物理学报*, 2003, 52(10): 2462~ 2465
- 84 杨晓苹, 翟宏琛. 双随机相位加密中相息图的优化设计. *物理学报*, 2005, 54(4): 1578~ 1582
- 85 于斌, 彭翔. 基于级联相位恢复算法的光学图像加密. *光学学报*, 2005, 25(7): 881~ 884
- 86 Situ G, Zhang J. Double random-phase encoding in the Fresnel domain. *Optics Letters*, 2004, 29(14): 1584~ 1586
- 87 Cai L, He M, Liu Q, et al. Digital image encryption and watermarking by phase-shifting interferometry. *Applied Optics*, 2004, 43(15): 3078~ 3084
- 88 He M, Cai L, Liu Q, et al. Phase-only encryption and watermarking based on phase-shifting interferometry. *Applied Optics*, 2005, 44(13): 2600~ 2606
- 89 陈林森, 周小红, 邵洁. 一种基于二元位相加密的大信息量数字全息水印. *光子学报*. 2005.

- 34(4):616~ 620
- 90 李榕,李萍. 基于随机相位实值编码的光学图像加密. 光子学报,2004,33(5):605~ 608
- 91 张培琨,李育林,刘家英,等. 光学图像相位加密中旋转不变性的实现及环形相位解密. 中国激光,2000,27(3):224~ 228
- 92 Peng X, Yu L, Cai L. Double-lock for image encryption with virtual optical wavelength. *Optics Express*, 2002, 10: 41~ 45
- 93 Peng X, Cui Z, Tan T. Information encryption with virtual-optics imaging system. *Optics Communications*, 2002, 212: 235~ 245
- 94 Yu L, Peng X, Cai L. Parameterized data encryption by digital optics. *Optics Communications*, 2002, 203: 67~ 77
- 95 Peng X, Cui Z, Cai L, et al. Digital audio signal encryption with a virtual optics scheme. *Optik*, 2003, 114(2): 69~ 75
- 96 Peng X, Yu L, Cai L. Digital watermarking in three-dimensional space with a virtual-optics imaging modality. *Optics Communications*, 2003, 226(1~ 6):155~ 165
- 97 彭翔,张鹏,牛憨笨. 基于虚拟光学的三维空间数字水印系统. 光学学报,2004, 24(11): 1507~ 1510
- 98 张鹏,彭翔,牛憨笨. 一种虚拟光学数据加密的系统实现. 电子学报,2004, 32(10): 1585~ 1588
- 99 彭翔,张鹏,牛憨笨. 虚拟光学信息隐藏理论及并行硬件实现. 光学学报,2004, 24(4): 623 ~ 627
- 100 Peng X, Zhang P, Cai L. Information security system based on virtual-optics imaging methodology and public key infrastructure. *Optik*,2004, 115(9): 420~ 426
- 101 Peng X, Zhang P, Niu H B. Architecture design of virtual-optics data security using parallel hardware and software. *Optik*, 2004, 115(1): 15~ 22
- 102 Peng X, Zhang P, Wei H, et al. Known-plaintext attack on optical encryption scheme based on double random phase keys. *Optics Letters*, 2006, 31(8): 1044~ 1046
- 103 Peng X, Wei H, Zhang P. Chosen-plaintext attack on lensless double-random phase encoding in the Fresnel domain. *Optics Letters*, 2006, 31(22): 3261~ 3263
- 104 Peng X, Wei H, Zhang P. Asymmetric cryptography based on wavefront sensing. *Optics Letters*, 2006, 31(24): 3579~ 3581
- 105 彭翔,汤红乔,田劲东. 双相位随机编码光学加密系统的唯密文攻击. 物理学报,2007, 56(5): 262,263

第 2 章 光学密码系统的理论基础

基于光学理论与方法的密码技术是近年来在国际上开始起步发展的新一代密码理论与技术。与传统基于数学的计算机密码学相比,光学密码技术具有多维、大信息量、多自由度、固有的并行数据处理能力等诸多优点。从本质上看,光学密码学属于信息光学的范畴。信息光学是光学与信息科学相结合的一门学科,采用傅里叶分析理论来解释和分析光波的传播、衍射和成像的物理现象及过程,利用光学的方法实现对输入信息的各种变换或处理^[1-7]。光学加密方法就是通过一定的光学变换扰乱原图像的波前或光强分布,实现图像数据的加密。由于光波在传播过程中,其波前分布主要是由其相位来决定,因此可以通过对物光波相位编码来达到改变其波前或光强分布的目的。光学加密方法通过相位、振幅、偏振、波长等参数来提供多种加密自由度,实现数据的多维加密。

本章介绍光学密码学中用到的一些基础知识,简要分析了透镜的傅里叶变换性质,讨论了光波的非涅耳衍射与夫琅禾费衍射、角谱传播理论、傅里叶数字全息术、相移数字全息术等基础理论方法在光学加密中的典型应用,介绍了典型的光学加密系统,着重介绍了基于微光学实现的纯相位加密系统、基于分割合成滤波函数的随机相位加密系统和基于光学异或的流密码系统。最后从密码编码学的角度,对目前光学密码系统的特点进行了研究和分析。

2.1 光学加密系统的相关理论基础

2.1.1 传播理论

衍射是光波在空间传播过程中的一种基本属性。实际上,在光波的传播过程中,只要光波波面受到了某种限制,如振幅或相位的突变等,就必然伴随着衍射现象的发生。任何光波在光学系统中的传播过程,实际上都是一种在相应光学元件调制下的衍射过程。在光学密码系统中,光波在自由空间的传播参数,如波长、衍射距离都可以作为系统的密钥,通过衍射变换达到数据加密的目的。下面首先简要介绍一下光波的非涅耳衍射理论和角谱传播理论。关于傅里叶光学的更详细内容,读者可以参考专门的著作。

1. 菲涅耳衍射与夫琅禾费衍射

光是电磁波,它的传播遵循电磁场传播规律。衍射规律是光传播的基本规律。

在满足衍射孔径必须比波长大得多及观察点必须离衍射孔足够远的情况下,可以把光波作为标量处理,即只考虑电场(或磁场)的一个横向分量的标量振幅,而不研究其方向,并假定任何别的有关分量可以用同样的方法独立处理,这就是标量衍射理论^[1]。

标量衍射理论所要解决的问题是:光场中任一点的复振幅能否用光场中其他各点的复振幅表示出来?这个问题直接用基尔霍夫衍射公式来计算通常比较困难,具有实用意义的是对其作某些近似,用所得的近似公式计算一定范围内的衍射场分布,按照近似程度不同,分为菲涅耳衍射与夫琅禾费衍射^[2]。

如图 2-1 所示,孔径 Σ 所在的平面坐标为 (x_1, y_1) , 与其距离 z 的观察平面的坐标为 (x_0, y_0) 。按照基尔霍夫衍射公式,观察点 $P_0(x_0, y_0)$ 的复振幅,在傍轴近似条件下

$$U_0(x_0, y_0) = \frac{1}{j\lambda z} \iint_{-\infty}^{\infty} U_1(x_1, y_1) \exp(jkr_{01}) dx_1 dy_1 \quad (2-1)$$

式(2-1)指数中的 r_{01} 不能简单用 z 代替,必须采用更高一级的近似。因为在指数中, r_{01} 只发生很小的误差就可能导致相位差远大于 2π 的变化。

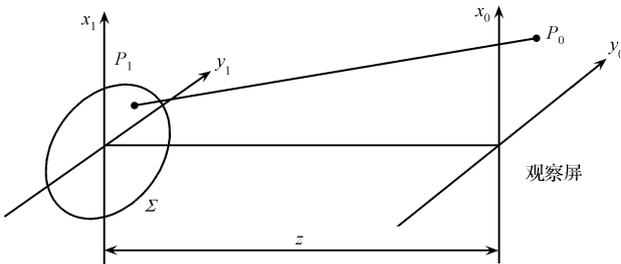


图 2-1 衍射理论几何示意图

由于

$$\begin{aligned} r_{01} &= \sqrt{(x_0 - x_1)^2 + (y_0 - y_1)^2 + z^2} \\ &= z \left[1 + \left(\frac{x_0 - x_1}{z} \right)^2 + \left(\frac{y_0 - y_1}{z} \right)^2 \right]^{\frac{1}{2}} \end{aligned} \quad (2-2)$$

对 r_{01} 作二项式展开时可略去高次项,只取前两项,即

$$r_{01} \approx z + \frac{(x_0 - x_1)^2 + (y_0 - y_1)^2}{2z} \quad (2-3)$$

式(2-3)称为菲涅耳近似,这个近似式成立的区域称为菲涅耳衍射区。

将式(2-3)代入式(2-1),可得

$$U_0(x_0, y_0) = \frac{\exp(jkz)}{j\lambda z} \iint_{-\infty}^{\infty} U_1(x_1, y_1) \exp \left[jk \frac{(x_0 - x_1)^2 + (y_0 - y_1)^2}{2z} \right] dx_1 dy_1 \quad (2-4)$$

若把指数中的二次项展开,还可表示为

$$U_0(x_0, y_0) = \frac{\exp(jkz)}{j\lambda z} \exp\left[j \frac{k}{2z}(x_0^2 + y_0^2)\right] \\ \times \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} U_1(x_1, y_1) \exp\left[j \frac{k}{2z}(x_1^2 + y_1^2)\right] \exp\left[-j2\pi\left[\frac{x_0}{\lambda z}x_1 + \frac{y_0}{\lambda z}y_1\right]\right] dx_1 dy_1 \quad (2-5)$$

这就是常用的菲涅耳衍射公式。

在导出菲涅耳衍射公式时,略去了 r_{01} 展开式中的高次项,为避免因此而导致明显的相位误差,则要求

$$\Delta = \frac{2\pi}{\lambda} \frac{[(x_0 - x_1)^2 + (y_0 - y_1)^2]^2}{8z^3} \ll 1 \quad (2-6)$$

若允许 (x_0, y_0) 取观察区域内任何值, (x_1, y_1) 取衍射孔径内任何值,则要求当 $[(x_0 - x_1)^2 + (y_0 - y_1)^2]^2$ 取最大值时, Δ 仍远小于 1rad, 即

$$z^3 \gg \frac{\pi}{4\lambda} [(x_0 - x_1)^2 + (y_0 - y_1)^2]_{\max}^2 \quad (2-7)$$

若采用比菲涅耳近似更严格的限制条件,当距离 z 满足

$$z \gg \frac{k}{2} (x_1^2 + y_1^2)_{\max} \quad (2-8)$$

式(2-7)中的相位因子 $\exp\left[j \frac{k}{2z}(x_1^2 + y_1^2)\right] \approx 1$, 于是得到夫琅禾费衍射方程, 即

$$U_0(x_0, y_0) = \frac{\exp(jkz)}{j\lambda z} \exp\left[j \frac{k}{2z}(x_0^2 + y_0^2)\right] \\ \times \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} U_1(x_1, y_1) \exp[-j2\pi(f_x x_1 + f_y y_1)] dx_1 dy_1 \quad (2-9)$$

式中: $f_x = \frac{x_0}{\lambda z}$;

$f_y = \frac{y_0}{\lambda z}$ 。

由式(2-9)易知,观察平面上的场分布可直接从孔径上的场分布的傅里叶变换求出。式(2-8)称为夫琅禾费近似,这个近似式成立的区域称为夫琅禾费衍射区。式(2-9)称为夫琅禾费衍射公式。

2. 角谱传播理论

由于各个不同空间频率的空间傅里叶分量可看作是沿不同方向传播的平面波,因此空间频谱为平面波谱即复振幅分布的角谱^[2,3]。本节从频域的观点讨论衍射规律。

设有一单色光波沿 z 方向投射到 $x-y$ 平面上,在 z 处光场分布为 $U(x, y, z)$ 。