光学信息安全导论

彭　翔　位恒政　张　鹏　著

科学出版社
www.sciencep.com

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

新蕾印刷厂印刷

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<明辉>）

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，介绍信息安全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领域的国际标准相结合，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

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，必须要有自主研制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。

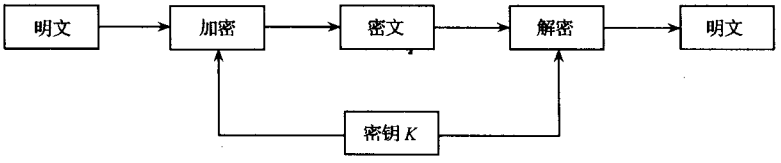

图 1-1　对称密码系统

序列密码属于对称密码体制的一种。设明文流为 $P=p_1p_2\cdots p_n$，密钥流为 $K=k_1k_2\cdots k_n$(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 $C=c_1c_2\cdots c_n$，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 $p_0, p_1, p_2, \cdots, p_i$ 划分成长为 L 位的组 $P=(p_1, p_2, p_3, \cdots, p_L)$，各个长为 L 的分组分别在密钥 $K=(k_1, k_2, k_3, \cdots, k_t)$ 的控制下变换成与明文组等长的一组密文输出 $C=(c_1, c_2, c_3, \cdots, c_L)$，$L$ 通常为 64 或 128，分组密码的模型如图 1-2 所示。

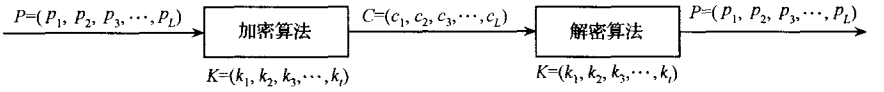

图 1-2 分组密码模型

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

Diffle 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。

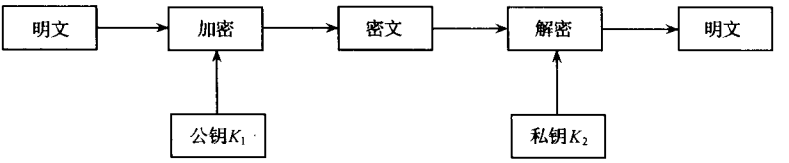

图 1-3　公钥密码系统

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]。

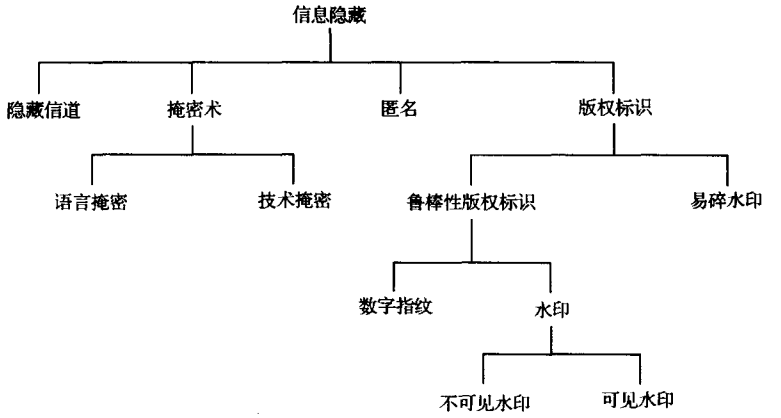

图 1-4 信息隐藏技术分类

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