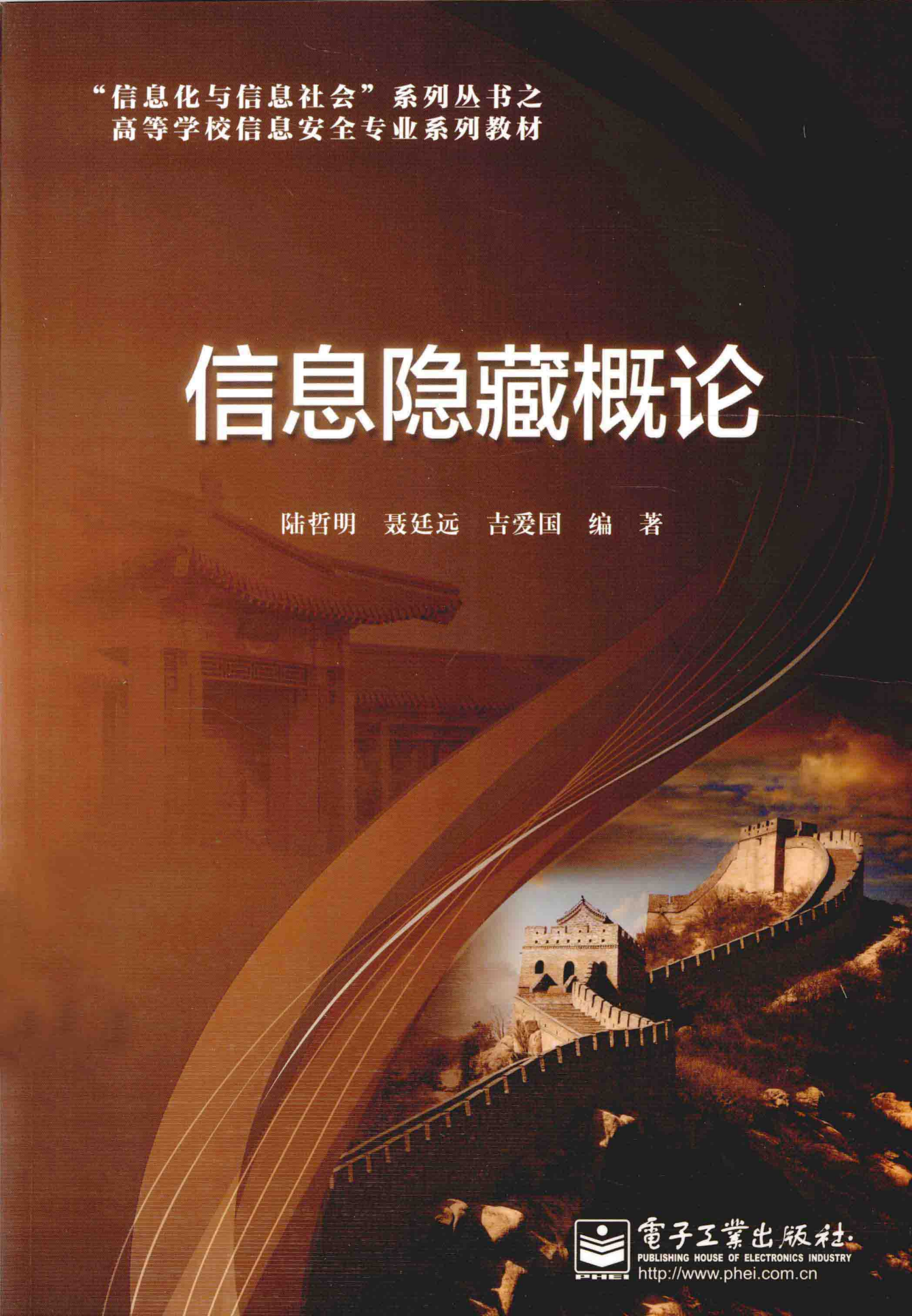
“信息化与信息社会”系列丛书之
高等学校信息安全专业系列教材

信息隐藏概论

陆哲明　聂廷远　吉爱国　编　著



電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

“信息化与信息社会”系列丛书之

高等学校信息安全专业系列教材

信息隐藏概论

陆哲明　聂廷远　吉爱国　编著

電子工業出版社

Publishing House of Electronics Industry

北京 • BEIJING

内 容 简 介

信息隐藏技术是一种重要的现代信息安全技术。本书全面介绍了信息隐藏的概念、发展现状、各个研究分支的基础理论和技术方法及其在信息安全领域的应用。本书首先介绍信息隐藏的基本概念、模型、研究分支、发展现状和相关理论与技术。其次，详细介绍三类主要的信息隐藏技术——隐写术、数字水印技术和数字指纹技术的概念、基础理论和主要方法。接着，介绍一种近年来比较热门的无损信息隐藏技术以及信息隐藏技术的其他研究分支。然后，分别介绍针对隐写技术和数字水印的攻击技术——隐写分析和数字水印攻击技术的基本概念、分类和典型方法。最后，介绍信息隐藏技术在知识产权保护、内容认证和保密通信等领域的典型应用。

本书可作为高等院校具有一定计算机基础的信息安全专业、电子信息工程专业、计算机专业、通信工程专业的研究生或高年级本科生的教材或参考书，也可作为科研院所相关专业的科技工作者的参考书。

图书在版编目（CIP）数据

信息隐藏概论 / 陆哲明，聂廷远，吉爱国编著. —北京：电子工业出版社，2014.11
（信息化与信息社会系列丛书）
高等学校信息安全专业系列教材
ISBN 978-7-121-24390-5

Ⅰ. ①信… Ⅱ. ①陆… ②聂… ③吉… Ⅲ. ①信息系统－安全技术－高等学校－教材 Ⅳ. ①TP309

中国版本图书馆 CIP 数据核字（2014）第 220491 号

策划编辑：刘宪兰
责任编辑：郝黎明
印　　刷：北京京师印务有限公司
装　　订：北京京师印务有限公司
出版发行：电子工业出版社
　　北京市海淀区万寿路 173 信箱　邮编　100036
开　　本：787×1092　1/16　印张：26.25　字数：672 千字
版　　次：2014 年 11 月第 1 版
印　　次：2014 年 11 月第 1 次印刷
印　　数：3000 册　　定价：53.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888。
质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。
服务热线：（010）88258888。

作 者 简 介

陆哲明，男，工学博士，浙江大学航空航天学院教授、博导、副所长。1974 年生。分别于 1995 年、1997 年和 2001 年获得哈尔滨工业大学学士、硕士和博士学位。1999 年留哈尔滨工业大学任讲师，2000 年破格为副教授，2003 年破格为教授，2004 年评为博士生导师。2004 年 10 月—2006 年 1 月作为洪堡学者赴德国弗赖堡大学作图像检索方向的访问研究。2006 年 1 月回国在哈尔滨工业大学深圳研究生院视觉信息分析与处理研究中心任主任、教授、博导；2007 年 2 月作为百人计划引进到中山大学信息科学与技术学院任教授、博导；2009 年 1 月引进到浙江大学航空航天学院航天电子工程研究所任教授、博导、副所长。陆博士为 2002 年哈尔滨市青年科技奖获得者、2003 年全国优秀博士学位论文奖获得者、2004 年教育部新世纪人才获得者、2005 年德国洪堡学者、2006 年深圳市特殊津贴专家、2011 年浙江省自然科学基金杰出青年基金获得者。陆博士长期从事多媒体信号处理、信息隐藏、复杂网络三个领域研究。这三个方面的研究工作并不是孤立的，都是在数字媒体和网络技术飞速发展的背景下展开的。截至 2014 年 1 月，陆博士在上述领域共主持省部级以上项目 12 个，共发表 SCI 检索论文 104 篇，EI 检索论文 146 篇，出版专著/教材 8 部，获省部级科技一等奖 1 项、二等奖 3 项、三等奖 1 项，厅级科技一等奖 2 项，发明专利授权 1 项。陆博士的主要学术兼职如下：国家国防科技工业局 CCSDS 工作专家组成员、IEEE 高级会员、教育部国家科学技术奖励评审专家、国家自然科学基金评审专家、SCI 国际期刊 KSII Transactions on Internet and Information Systems 编委、EI 国际期刊 Journal of Information Hiding and Multimedia Signal Processing 编委、EI 国际期刊 Information Technology Journal 编委、国际期刊 Research Journal of Information Technology 编委、国际期刊 Journal of Artificial Intelligence 编委、IEICE 会员、IIHMSP 和 IMCCC 国际会议程序委员会主席、IEEE Trans. Multimedia 和 Image Processing 等六个 IEEE 期刊审稿人、IET Image Processing 和 Electronics Letters 等四个 IET 期刊审稿人。

总　序

信息化是世界经济和社会发展的必然趋势。近年来，在党中央、国务院的高度重视和正确领导下，我国信息化建设取得了积极进展，信息技术对提升工业技术水平、创新产业形态、推动经济社会发展发挥了重要作用。信息技术已成为经济增长的“倍增器”、发展方式的“转换器”、产业升级的“助推器”。

作为国家信息化领导小组的决策咨询机构，国家信息化专家咨询委员会按照党中央、国务院领导同志的要求，就我国信息化发展中的前瞻性、全局性和战略性的问题进行调查研究，提出政策建议和咨询意见。信息化所具有的知识密集的特点，决定了人力资本将成为国家在信息时代的核心竞争力。大量培养符合中国信息化发展需要的人才是国家信息化发展的一个紧迫需求，也是我国推动经济发展方式转变，提高在信息时代参与国际竞争比较优势的关键。2006 年 5 月，我国公布《2006—2010 年国家信息化发展战略》，提出“提高国民信息技术应用能力，造就信息化人才队伍”是国家信息化推进的重点任务之一，并要求构建以学校教育为基础的信息化人才培养体系。

为了促进上述目标的实现，国家信息化专家咨询委员会致力于通过讲座、论坛、出版等各种方式推动信息化知识的宣传、教育和培训工作。2007 年，国家信息化专家咨询委员会联合教育部、原国务院信息化工作办公室成立了“信息化与信息社会”系列丛书编委会，共同推动“信息化与信息社会”系列丛书的组织编写工作。编写该系列丛书的目的是，力图结合我国信息化发展的实际和需求，针对国家信息化人才教育和培养工作，有效梳理信息化的基本概念和知识体系，通过高校教师、信息化专家、学者与政府官员之间的相互交流和借鉴，充实我国信息化实践中的成功案例，进一步完善我国信息化教学的框架体系，提高我国信息化图书的理论和实践水平。毫无疑问，从国家信息化长远发展的角度来看，这是一项带有全局性、前瞻性和基础性的工作，是贯彻落实国家信息化发展战略的一个重要举措，对于推动国家的信息化人才教育和培养工作，加强我国信息化人才队伍的建设具有重要意义。

考虑到当时国家信息化人才培养的需求，各个专业和不同教育层次（博士生、硕士生、本科生）的需要，以及教材开发的难度和编写进度时间等问题，“信息化与信息社会”系列丛书编委会采取了集中全国优秀学者和教师，分期分批出版高质量的信息化教育丛书的方式，结合高校专业课程设置情况，在“十一五”期间，先后组织出版了“信息管理与信息系统”、“电子商务”、“信息安全”三套本科专业高等学校系列教材，受到高校相关专业学科以及相关专业师生的热烈欢迎，并得到业内专家和教师的一致好评和高度评价。

但是，随着时间的推移和信息技术的快速发展，上述专业的教育面临着持续更新、不断完善的迫切要求，日新月异的技术发展及应用变迁也不断对新时期的建设和人才培养提出新要求。为此，“信息管理与信息系统”、“电子商务”、“信息安全”三个专业教育需以综合的视角和发展的眼光不断对自身进行调整和丰富，已出版的教材内容也需及时进行

更新和调整，以满足需求。

这次，高等学校“信息管理与信息系统”、“电子商务”、“信息安全”三套系列教材的修订是在涵盖第 1 版主题内容的基础上进行的更新和调整。我们希望在内容构成上，既保持原第 1 版教材基础的经典内容，又要介绍主流的知识、方法和工具，以及最新的发展趋势，同时增加部分案例或实例，以及新的分册，使每一本教材都有明确的定位，分别体现“信息管理与信息系统”、“电子商务”、“信息安全”三个专业领域的特征，并在结合我国信息化发展实际特点的同时，选择性地吸收国际上相关教材的成熟内容。

对于这次三套系列教材（以下简称系列教材）的修订，我们仍提出了基本要求，包括信息化的基本概念一定要准确、清晰，既要符合中国国情，又要与国际接轨；教材内容既要符合本科生课程设置的要求，又要紧跟技术发展的前沿，及时地把新技术、新趋势、新成果反映在教材中；教材还必须体现理论与实践的结合，要注意选取具有中国特色的成功案例和信息技术产品的应用实例，突出案例教学，力求生动活泼，达到帮助学生学以致用的目的，等等。

为力争修订教材达到我们一贯秉承的精品要求，“信息化与信息社会”系列丛书编委会采用了多种手段和措施保证系列教材的质量。首先，在确定每本教材的第一作者的过程中引入了竞争机制，通过广泛征集、自我推荐和网上公示等形式，吸收优秀教师、企业人才和知名专家参与写作；其次，将国家信息化专家咨询委员会有关专家纳入到各个专业编委会中，通过召开研讨会和广泛征求意见等多种方式，吸纳国家信息化一线专家、工作者的意见和建议；再次，要求各专业编委会对教材大纲、内容等进行严格的审核，并对每本教材配有一至两位审稿专家。

我们衷心期望，系列教材的修订能对我国信息化相应专业领域的教育发展和教学水平的提高有所裨益，对推动我国信息化的人才培养有所贡献。同时，我们也借系列教材修订出版的机会，向所有为系列教材的组织、构思、写作、审核、编辑、出版等做出贡献的专家学者、教师和工作人员表达我们最真诚的谢意！

应该看到，组织高校教师、专家学者、政府官员以及出版部门共同合作，编写尚处于发展动态之中的新兴学科的高等学校教材，有待继续尝试和不断总结经验，也难免会出现这样那样的缺点和问题。我们衷心希望使用该系列教材的教师和学生能够不吝赐教，帮助我们不断地提高系列教材的质量。

2013 年 11 月 1 日

序　言

“十一五”期间，由国家信息化专家咨询委员会牵头，教育部信息安全专业类教学指导委员会有关领导、学者组织，众多信息安全专业著名专家和教师参与开发，并由电子工业出版社出版的“高等学校信息安全专业系列教材”，由于在体系设计上较全面地覆盖了新时期信息安全专业教育的各个知识层面，包括宏观视角上对信息化大环境下信息安全相关知识的综合介绍，对信息安全应用发展前沿的深入剖析，以及对信息安全系统建设各项核心任务的系统讲解和对一些重要信息安全应用形式的讨论，在“高等学校信息安全专业系列教材”面市后，受到高校该专业学科及相关专业师生的热烈欢迎，得到业内专家和教师的好评和高度评价，被誉为该学科专业教材中的精品系列教材。

但是，随着信息技术的快速发展，信息安全专业教育面临着持续更新、不断完善的迫切要求，其日新月异的技术发展及应用变迁也不断对新时期信息安全建设和人才培养提出新的要求。为此，信息安全专业教育需以综合的视角和发展的眼光不断对教学内容进行调整和丰富，已出版的教材内容也需及时进行更新和修改，以满足需求。

这次修订，除对“高等学校信息安全专业系列教材”第 1 版各册教材的主题内容进行了相应更新和调整外，同时对系列教材的总体架构进行了调整并增加了 3 个分册，即《信息安全数学基础》、《信息安全实验教程》和《信息隐藏概论》。

调整后的教材在体系架构和内容构成上既保持了基础的经典内容，又介绍了主流的知识、方法和工具，以及最新发展趋势，同时增加了部分案例或实例。使得系列中的每一本教材都有明确的定位，充分体现了国家“信息安全”的领域特征，在结合我国信息安全实际特点的同时，还注重借鉴国际上相关教材中适于作为信息安全本科教育知识的成熟内容。

我们希望这套修订教材能够成为新形势下高等学校信息安全专业的精品教材，成为高等学校信息安全专业学生循序渐进了解和掌握专业知识不可或缺的教科书和知识读本，成为国家信息安全新环境下从业人员及管理者学习信息安全知识的有益参考书。

高等学校信息安全专业系列教材编委会

2013 年 10 月于北京

前　言

随着计算机网络技术和多媒体处理技术的迅速发展，信息技术已经广泛应用于社会生产的各个领域。数字多媒体信息（如声音、图像、视频等）可以通过互联网快捷而有效地进行传播，这不但满足了人们的生产生活需要，也为资源共享提供了条件。然而，信息在网络传输中也存在安全隐患，例如：数字多媒体作品的版权容易受到侵犯和伪造，内容容易受到非法盗用和篡改；各种机密信息，如信用卡账号、个人隐私等容易受到非法截获和查看等。如今，信息产业已经成为国民经济中的一个重要组成部分，是社会发展的重要战略资源，信息安全已经成为影响国家安全、社会稳定、经济发展、个人利益的重大关键问题。

广义上，凡是涉及信息的安全性、完整性、可用性、真实性和可控性的相关理论和技术都是信息安全所要研究的领域。狭义上，信息安全是指信息内容的安全性，即保护信息的机密性、真实性和完整性，避免攻击者利用系统的安全漏洞进行窃听、冒充、诈骗、盗用等有损合法用户利益的行为，保护合法用户的利益和隐私。当前，密码术（Cryptography）仍然是信息安全的核心技术，基本思想是利用单钥或双钥密码算法把明文变换成密文后通过公开信道传输到接收者手中。也就是说密码术的实质是通过打乱信息内容，使其看上去像随机乱码来达到保护信息内容的目的。然而，密码术有一个致命的缺点，就是它明确地提示攻击者哪些是重要信息，因而容易引起攻击者的好奇和注意，并有被破解的可能性，而且一旦加密文件被破解后其内容就完全透明了。而且，攻击者可以在破译失败的情况下将信息破坏，使得即使是合法的接收者也无法阅读信息内容。在硬件技术高速发展以及基于互联网的强大的并行计算逐步发展的今天，传统的密码术正经受着巨大的冲击。

那么，什么技术能够弥补密码术的缺陷呢？既然乱码能激起攻击者破译热情，能不能让攻击者看不到乱码呢？答案是肯定的。人们很快想到了“暗度陈仓”的方法：明着传输无关紧要的载体而实际上暗藏着重要的秘密信息，这就引出了信息安全领域的另一个重要分支——信息隐藏（Information Hiding），其标志性里程碑是 1996 年第一届国际信息隐藏学术研讨会在英国剑桥的胜利举行。这样，人们开始构建以信息隐藏为核心的全新信息安全概念：信息隐藏就是将秘密信息隐藏于另一非机密的载体中。载体形式可以为任何一种数字媒体，如图像、声音、视频或一般的文档等。比较而言，密码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。传统的以密码术为核心技术的信息安全和隐藏式信息安全技术不是互相矛盾、互相竞争的技术，而是互补的。

一般认为，现代信息隐藏技术是由古老的隐写术（Steganography）发展而来的。该词来源于希腊语，其对应的英文是“Covered Writing”。在早期，人们常用暗号来传递秘密信息。早在公元 1 世纪，就已经出现用隐形墨水来传递隐秘消息。公元前 400 年，历史学之父 Herodotus 在《历史》一书中记录了几个采用不同手段进行秘密信息传递的例子：把消息藏在野兔的肚子里，假扮成猎人把消息传出去，成功地躲过了敌方哨卡的检查；剃光一位奴隶的头发并把消息刺在其头皮上，等其头发长起来后把人送往另一营地，从而实

现秘密信息的传送；将秘密消息刻在木板上，然后铺上蜡，再在蜡上写些无关紧要的话送出去。中国古代也有利用藏头诗传递秘密信息的例子以及在米粒上刻字、使用隐写墨水、道士画符遇水显影或遇火显影等例子。这些古代信息隐藏的应用实例采用了各种不同的手段，目的都是为了不引起他人的注意和怀疑。这也就引出了信息隐藏的根本目的，即隐藏信息的存在。古代隐写术发展一直比较缓慢，没有成为一门独立的学科，使得人们对于信息保密更多的是采用密码术。直到信息技术和计算机技术高度发达的今天，数字化信息与隐写术相结合为古老的隐写术注入了新的活力，使得数字化信息隐藏技术成为一门全新的技术，为探索非密码的通信安全提供了新途径。现代信息隐藏技术是在 20 世纪 90 年代后才逐步发展起来的，大家普遍公认的时间起点是 1994 年，那一年 Schyndel 等人在 IEEE 国际图像处理会议上首次明确提出了“数字水印”概念。

1996 年 5 月在英国剑桥召开的第一次国际信息隐藏学术研讨会上，使得一些研究团体在信息隐藏的基本概念和术语上达成共识，从而使信息隐藏作为一门新学科开始得到快速发展。信息隐藏也称数据隐藏，它是集多学科理论与技术于一身的新兴技术，它利用人类感官对数字信号的感觉冗余，将秘密信息隐藏于另一非保密载体（如图像、视频、音频、信道甚至整个系统）中，以不引起检查者的注意。信息隐藏技术有多种含义：一是信息不可见，二是信息的存在性隐蔽，三是信息的接收方和发送方隐蔽，四是传输的信道隐蔽。信息隐藏技术包括隐蔽信道、匿名通信、隐写术、数字水印技术、数字指纹技术、阈下信道和低截获概率通信等多个学科分支。

基于信息隐藏这门新学科的发展现状，本书旨在介绍近二十年来信息隐藏领域的公认的广泛提及和深入研究的一些基础理论和典型方法，尽量以浅显易懂的方式为学习信息隐藏技术的来自信息安全专业的本科生和研究生提供入门教材。在学习本书之前，读者们需要具备微积分、概率论、信息论、正交变换和计算机科学的基础知识，了解图像处理、音频信号处理、视频信号处理、模式识别等相关概念，掌握必要的计算机编程语言和具备较好的仿真验证能力。本书一共 9 章，分别是绪论、隐写术、数字水印技术、数字指纹技术、无损信息隐藏技术、其他信息隐藏研究分支简介、隐写分析技术、数字水印攻击技术和信息隐藏技术的应用。为了让读者更好地理解信息隐藏技术，各章都配有习题。若要粗略学习信息隐藏的主要分支，建议学习第 1 章到第 4 章，建议教师各分配 2 学时、8 学时、8 学时、6 学时课堂授课，且为第 2 章和第 3 章各配 2 学时上机实验，这样一共 24 学时课堂 4 学时上机。若要对所有信息隐藏研究分支作了解，建议学习第 1 章到第 6 章，其中第 5 章分配 6 学时课堂讲授和 2 学时上机实验，第 6 章分配 2 学时课堂讲授，这样一共 32 学时课堂 6 学时上机。若要详细了解隐写术和数字水印技术的攻防两个方面及其应用，建议学习第 1、2、3、7、8、9 章这六章，其中 7、8、9 三章分别分配 6、6、2 学时课堂授课，这样一共是 32 学时课堂 4 学时上机。下面介绍各章的背景和主要内容。

信息隐藏技术是在传统密码术原理的基础上发展起来的一门涉及信息论、密码学、应用数学、计算机科学、网络技术、通信技术等多种学科的综合性学科。相对于密码术，信息隐藏技术的优点在于它隐藏了秘密信息的存在性，减小了受攻击的风险。正是这种特性使得信息隐藏技术在保护信息安全方面比密码技术具有更好的发展前景。本书的第 1 章从网络信息安全问题入手，对信息隐藏技术的概念、模型、分类、研究分支、历史发展和应用领域进行概述。

与其他信息隐藏研究分支相比，隐写术是一门古老的技术，主要用于保密通信。它将秘密信息嵌入到看上去普通的信息中进行传送，以防止第三方检测出秘密信息。隐写术

关注的重点是如何让秘密信息的存在不被发现。本书的第 2 章首先概述保密通信的有关背景，接着概述隐写术的有关概念、分类和性能评价问题，然后按照载体类型的不同分别介绍基于文本、图像、音频和视频等载体的隐写术。

信息技术和计算机网络的迅速发展，使得在网上传播的多媒体作品的版权保护和内容认证面临着日益严峻的挑战。为了保护数字媒体的知识产权，以前人们采用了将数据加密的方法，使得只有掌握密钥的授权用户才能解密数据，从而使用数字媒体产品。但这种方法只能控制用户是否能够存取数据，与数据本身并无直接关系，因此一旦被破解，这些数据就会很轻易地被修改、复制、传播。为消除这个隐患，人们又提出了新的知识产权保护手段——数字水印技术。数字水印技术是将一段标志版权所有者的信息嵌入到要保护的媒体中，但在这个过程中通常采用特定的技术手段使被嵌入的信息不会被人感知到，只有知识产权的所有者才能通过检测器确定数字水印是否存在。本书第 3 章从数字水印技术的提出背景入手，首先介绍数字水印技术的相关概念、分类、框架模型和性能评价，然后按照载体类型的不同分别介绍用于图像、音频和视频等载体的数字水印技术。

信息技术的迅猛发展及以其为基础的电子商务的广泛应用，使各类文字、图片、影视等作品通过网络的传播范围空前扩大，为创作者和发行商带来了新机遇。但同时，人们也很容易对以数字形式存在的产品进行非法复制和分发。数字指纹技术是近几年发展起来的一种新型数字版权保护技术，它的原理是版权者在其分发的数字作品复制中嵌入与用户身份相关的唯一信息，当发现非法复制时，版权者凭借嵌入信息可以识别非法分发复制的用户，进而通过法律诉讼和惩罚来达到保护版权权益、对非法行为进行威慑的目的，可以看出数字指纹技术实现了一种版权跟踪机制。本书第 4 章从数字指纹技术的提出背景入手，首先介绍数字指纹技术的相关概念、分类、框架模型和性能评价，然后概述最重要的指纹编码和指纹协议问题，接着详细介绍基于不同指纹协议的数字指纹技术，最后讨论抗共谋攻击的指纹编码问题。

传统信息隐藏技术通常给载体对象引入了一些细微的、不可逆的或一些永久的失真，尽管这些失真是非常轻微的，但是在一些对精度要求高的领域，比如法律、医学和军事系统等，当秘密信息被提取后，需要无失真地恢复原始载体，因此即使是非常轻微的失真也是不允许的。在这种情况下，出现了无失真恢复原始载体的嵌入技术，称为无损信息隐藏技术。本书的第 5 章从无损信息隐藏技术的提出背景入手，首先介绍无损信息隐藏技术的相关概念、分类、框架模型和性能评价，接着以图像为载体对象介绍基于不同嵌入域（空域、整数变换域和压缩域）的无损信息隐藏技术。

除了隐写术、数字水印技术和数字指纹技术外，信息隐藏领域还有一些其他研究分支，例如：普遍存在于安全操作系统、安全网络、安全数据库系统中的危害系统安全策略的隐蔽信道；针对公钥密码技术的数字签名、认证等应用密码体制的阈下信道等。为了让读者对信息隐藏的各个分支都有所了解，本书第 6 章分别简要介绍隐蔽信道、阈下信道、低截获概率通信和匿名通信等研究分支。

隐写术为大众在机密性和个人隐私性方面提供了保护，同时也使得恐怖组织或谍报机构进行非法信息传递变得更为便利。如果不当地使用隐写术，会损害企业和国家利益，给公共安全和社会稳定带来威胁。在检测隐藏信息、监控和阻截非法隐蔽通信方面，各国军方和安全部门表现出了十分迫切的需求，隐写分析术（Steganalysis）应运而生。隐写分析术是对数字媒体信号进行统计分析，判断其中是否藏有秘密信息的技术。更高层次的隐写分析术可以对秘密信息的长度、隐藏位置等进行判断。隐写分析的目的是检测、阻截和

破坏隐蔽通信。隐写分析术和隐写术是两种相互对抗且相互促进的技术。本书第 7 章首先介绍了隐写分析的基本概念、分类和评价指标，然后分别介绍针对图像、音频和视频载体的隐写分析技术，其中以图像载体为主。针对每种载体，主要分专用分析法和通用分析法分别进行介绍。

数字水印作为一种数据认证和版权保护的手段，必然会受到各种形式的攻击。研究数字水印攻击的目的是发现现有技术的漏洞和缺陷，以提出对策来提升未来水印设计的抗攻击能力。本书第 8 章首先给出攻击的定义、分类和相关概念，然后介绍针对安全性的三种攻击技术，最后介绍针对应用系统而与水印算法安全性及鲁棒性无关的系统攻击技术。

信息隐藏技术已经在许多领域得到了广泛应用，主要集中在如下几大方面：① 数据保密通信；② 身份认证；③ 数字作品的版权保护与盗版追踪；④ 完整性、真实性鉴定与内容恢复。本书第 9 章首先介绍信息隐藏技术的四个最重要的应用领域：知识产权保护、军事保密通信、交易跟踪和真伪鉴别。然后介绍复制控制、广播监控、设备控制及其他一些应用领域。

本书可作为高等院校具有一定计算机基础的信息安全专业、电子信息工程专业、计算机专业、通信工程专业的研究生或高年级本科生的教材或参考书，也可作为科研院所相关专业的科技工作者的参考书。本书的第 1、2、3、5、7、8 章由陆哲明教授执笔，第 4、6 章由聂廷远副教授执笔，第 9 章由吉爱国教授执笔，最后由陆哲明教授审定。本书广泛参考了国内外信息隐藏研究领域的学术论文、学位论文和学术著作，并包含了作者的部分研究成果，这些成果得到了多个国家自然科学基金项目（No. 61171150、No. 61003255 和 No. 60272074）和浙江省杰出青年基金项目（No. R1110006）的资助，在此致以深深的谢意。在本书的撰写过程中还得到了浙江大学航空航天学院航天电子工程研究所、青岛理工大学信息对抗研究所各位教师、博士生和硕士生的协助，在此表示衷心的感谢。

限于水平，书中难免有错误与不妥之处，恳请读者批评指正。

陆哲明
于杭州浙江大学航空航天学院航天电子工程研究所
聂廷远，吉爱国
于青岛理工大学信息对抗研究所
2014 年 2 月

目　录