HZ BOOKS
华章教育

高等院校信息安全专业规划教材

数字图像隐写分析

Digital Image Steganalysis

刘粉林 刘九芬 罗向阳 ◎ 等编著

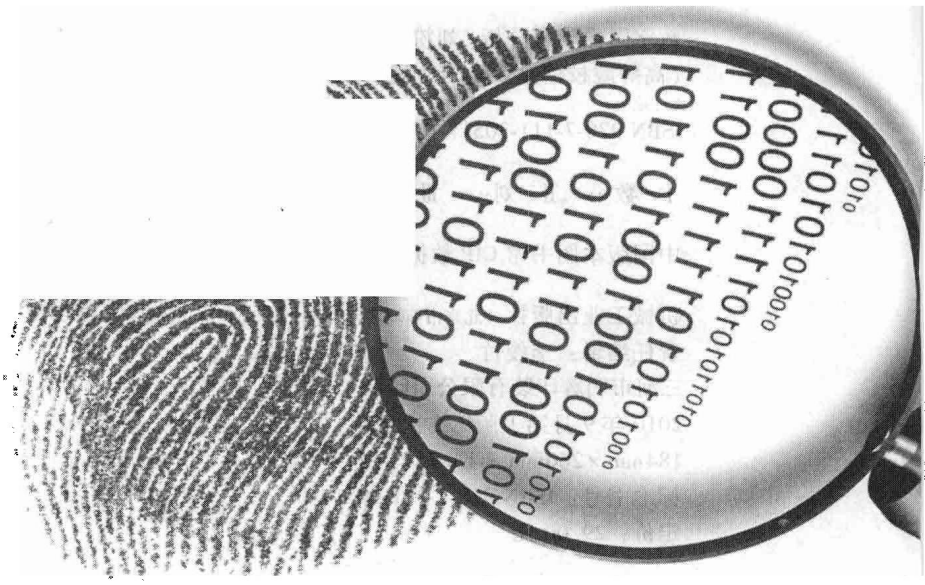
机械工业出版社
China Machine Press

高等院校信息安全专业规划教材

数字图像隐写分析

Digital Image Steganalysis

刘粉林 刘九芬 罗向阳 ◎ 等编著



机械工业出版社
China Machine Press

本书介绍了典型隐写和隐写分析方法的原理、技术基础和主要算法，着重反映国内外近年来的研究进展。全书共7章，主要内容包括信息隐藏简介、图像隐写的预备知识、数字图像典型隐写术、空域特定隐写检测方法、JPEG图像的特定隐写检测方法、通用盲检测方法和图像隐写信息提取技术。

本书可作为通信与多媒体安全相关专业的研究生和高年级本科生的教材，也可供相关工程技术人员参考。

图书在版编目（CIP）数据

数字图像隐写分析/刘粉林等编著. —北京：机械工业出版社，2010.6
（高等院校信息安全专业规划教材）

ISBN 978-7-111-30517-0

Ⅰ.数…　Ⅱ.刘…　Ⅲ.电子计算机－密码术－高等学校－教材　Ⅳ.TP309.7

中国版本图书馆CIP数据核字（2010）第076714号

机械工业出版社（北京市西城区百万庄大街22号　邮政编码　100037）
责任编辑：李俊竹
三河市明辉印装有限公司印刷
2010年9月第1版第1次印刷
184mm×260mm · 13.75印张
标准书号：ISBN 978-7-111-30517-0
定价：29.00元

凡购本书，如有缺页、倒页、脱页，由本社发行部调换
客服热线：（010）88378991；88361066
购书热线：（010）68326294；88379649；68995259
投稿热线：（010）88379604
读者信箱：hzjsj@hzbook.com

编委会

丛书序

经过数年的筹划与努力，信息安全系列丛书终于和广大读者见面了。

众所周知，进入21世纪以来，信息化对社会发展的影响日益深刻。全球信息化正在引发当今世界的深刻变革，重塑世界政治、经济、社会、文化和军事发展的新格局。

人们在享受信息化所带来的便利的同时，也不得不面对各种信息安全问题。信息安全是信息化的关键，各种天灾（如地震、洪水、飓风）和“人祸”（如网络故障、黑客入侵、病毒等）都会影响信息化进程。因此，在发展信息化的同时要重视信息安全，要在安全中发展，在发展中确保安全。

目前，世界各国都将信息安全视为国家安全的重要组成部分。党的十六届四中全会在《中共中央关于加强党的执政能力建设的决定》中明确提出：“坚决防范和打击各种敌对势力的渗透、颠覆和分裂活动，有效防范和应对来自国际经济领域的各种风险，确保国家的政治安全、经济安全、文化安全和信息安全”。党中央把信息安全和政治安全、经济安全、文化安全并列，作为我们国家四大安全内容之一，可见信息安全之重要，绝不能掉以轻心。近年来，我国在信息安全保障方面的工作逐步加强，制定并实施了国家信息安全战略，建立了信息安全管理体制和工作机制。基础信息网络和重要信息系统的安全防护水平明显提高，互联网信息安全管理进一步加强。

信息安全问题的解决，既要依靠技术的发展，更要重视人的作用。随着科技的进步，信息安全的概念和内涵不断发生变化，今天我们所说的信息安全是一个涉及计算机科学、网络技术、通信技术、密码技术、信息安全技术、应用数学、数论、信息论等领域的交叉学科，各种保障信息安全的技术也不断推陈出新。我们应大力培养信息安全的专业人才，对从业人员进行技术、职业道德、法律等全方位的教育。同时，要普及信息安全教育，增强国民的信息安全意识，提高全民的信息化知识水平和防范意识。

面对社会对信息安全人才的迫切需求，国内已有几十所高校设立了信息安全专业，还有众多高校开设了信息安全相关的必修与选修课。为了有力地支持信息安全相关课程的教学，促进信息安全的科学研究，在机械工业出版社华章分社的精心策划与组织下，国内高校从事信息安全领域研究、教学的专家和教师共同编写了这套“高等院校信息安全专业规划教材”。这套丛书是各位作者多年教学、科研成果的结晶，其特点是理论与实践紧密结合、深入浅出、实例丰富，既包括基础知识，也反映最新科研成果与发展趋势。我深信，丛书的出版必将对

信息安全知识的普及和推广、信息安全人才的培养、教学与科研产生积极影响并作出重要的贡献。

最后，作为本丛书的编委会主任，我对各位编委的努力工作、各位作者的辛勤劳动、机械工业出版社华章分社的大力支持表示衷心的感谢。

丛书编委会主任　卿斯汉

2009 年 6 月

前　言

自 Simmons 提出不可视通信的“经典”模型——“囚犯问题”以来，现代信息隐藏技术的发展已经走过了 27 年，其在多媒体内容安全、多媒体产品知识产权保护及隐蔽通信等方面诱人的应用前景，吸引了来自多个领域的专家学者。信息隐藏及其反向技术已成为信息安全的重要研究内容。

数字隐写（steganography）是信息隐藏的一个重要分支，其目的是以表面正常的数字载体（如图像、音频和视频信号等）作为掩护，将秘密信息嵌入（隐藏）其中，并将其与大量正常的多媒体数据混杂在一起，通过各种渠道尤其是因特网发送出去。信息的嵌入不会改变载体的感官质量。这种隐蔽通信方式不但掩盖了通信的内容，还掩盖了“正在进行通信”的事实。目前已公开的数字隐藏工具软件已达数百种之多。

与数字隐写相对应的就是所谓的隐写分析（steganalysis），隐写分析包括隐写检测与秘密信息提取两个过程。其首要任务是对多媒体信号进行统计分析，判断其中是否含有秘密信息，即进行隐写检测。通常认为，只要一个经隐写的载体被检测出可能存在秘密信息，那么所用的隐写算法就是不安全的。目前，隐写分析的研究主要集中在隐写检测方面。

与密码学相比，数字隐写能够掩盖“正在进行通信”这一事实，使其在隐蔽通信方面有着独特的优势。这一优势已成为隐写与隐写分析研究者们探索的强大动力。数字隐写的伪装性、与载体的不可分离性使得隐蔽通信具有更强的信息安全性，成为网络环境下安全、可靠地传递国家政治、军事、经济信息的基本通信方式之一。同时，由于因特网通信的开放性和应用的普遍性，隐蔽通信也会被敌特机构、恐怖组织和非法组织用于计划和协调犯罪活动，成为危害国家政治、经济安全和社会稳定的通信工具。因此，开展数字隐写分析方面的研究具有重要理论价值和现实意义。

本书将介绍典型隐写和隐写分析方法的原理、技术基础和主要算法，着重反映国内外近年来的研究进展。此外，书中还包含了编者所在课题组近几年的部分相关研究成果。全书共 7 章，第 1 章为概论，主要内容包括信息隐藏的定义、信息隐藏的历史、现代信息隐藏技术以及数字隐写分析的基本概念；第 2 章介绍图像隐写的预备知识，主要包括数字图像基础知识、图像的常见频域变换以及模式识别和分类器的基础知识；第 3 章主要介绍数字图像的典型隐写术，主要内容包括数字隐写的基本原理、空域图像隐写方法、DCT（离散余弦变换）域图像隐写方法等；第 4 章着重讨论空域的特定隐写检测方法，主要内容包括针对 LSB（最低有效位）替换的隐写检测、针对 MLSB（最低多位有效位）替换的隐写检测、针对 $\pm K$ 和随机调制的隐写检测，给出了多种典型的隐写检测算法；第 5 章主要介绍 JPEG 图像的特定隐写检测方

法，主要内容包括针对JSteg隐写的检测、针对F5隐写的检测、针对OutGuess隐写的检测以及针对MB隐写的检测；第6章着重讨论通用盲检测方法，主要内容包括图像隐写通用盲检测技术的研究内容和原理、典型的通用盲检测方法以及通用盲检测中的难点问题和值得研究的方向；第7章着重介绍图像隐写信息提取技术，主要内容包括提取攻击概述、隐写信息难提取性的信息论分析、对连续LSB替换隐写术的提取攻击、对随机LSB隐写术的提取攻击、对基于图像格式的隐写术的提取攻击等。

本书中的所有算法均给出了主要的实现步骤，以帮助感兴趣的读者实现相应的算法。此外，本书附有大量参考文献，希望能帮助读者快速进入相应的研究领域并了解国内外的研究进展。

本书可供计算机、通信、计算机网络、信息技术、信息安全、信号分析与处理等领域关注通信与多媒体安全的科研教学人员、研究生和高年级本科生使用，也可供相关工程技术人员参考。

本书由解放军信息工程大学信息工程学院网络工程系组织编写，具体分工如下：第1章由刘粉林和刘九芬编写，第2章由刘粉林和何雄飞编写，第3章由孙怡峰和杨春芳等编写，第4章和第5章由罗向阳和杨春芳编写，第6章由罗向阳编写，第7章由刘九芬和张卫明编写。全书由刘粉林统稿。此外，卢记仓、叶茂、宗睿、王杏艳等也参与了本书的编写工作。

感谢本书中所涉及的专家学者，本书的完成与他们辛勤的工作是分不开的。感谢机械工业出版社为本书出版所付出的辛勤劳动。此外，本书还得到了国家自然科学基金项目（批准号：60970141，60902102）的资助。

由于信息隐写和隐写分析技术的发展十分迅速，加之编者水平有限，疏漏和错误之处在所难免，恳请读者和有关专家不吝赐教。

编　者

教学和阅读建议

本课程假定读者具有一定的计算机知识，具有较强的数学思维能力。在一学期30学时的课程学习中，对各章的教学内容可作如下安排：

第1章　概论（3学时）：

教学内容：

- 信息隐藏基本概念；
- 隐写术的起源与发展；
- 信息隐藏的作用、意义与分类；
- 数字图像隐写分析技术发展概况。

考核要求：

- 了解信息隐藏相关概念、与密码技术的主要区别、信息隐藏技术的主要应用场景、隐写与数字水印的异同；
- 了解隐写分析技术的主要分类与概况；
- 掌握隐写的统计检测法的基本原理。

第2章　预备知识（4学时）

教学内容：

- 数字图像的基本知识、常见的图像变换；
- 模式识别的基本知识。

考核要求：

- 了解数字图像的生成和存储格式等相关知识；
- 理解常见的图像变换：离散傅里叶变换、离散余弦变换和离散小波变换；
- 掌握隐写检测中常用分类器的基本原理和使用方法。

第3章　数字图像典型隐写术（4学时）

教学内容：

- 数字隐写的基本原理；
- 典型的空域隐写方法；
- 典型的DCT域隐写方法。

考核要求：

- 了解不可视通信的基本模型、数字隐写系统模型、数字隐写系统的安全性相关知识与主要分类；

- 掌握 LSB 替换、MLSB 替换、$\pm K$ 与随机调制隐写等空域隐写方法的基本原理与主要过程，了解调色板与二值图像中的隐写方法的基本原理；
- 掌握 JSteg、F5、OutGuess 和 MB 等 DCT 域隐写的基本原理与主要过程。

第 4 章　空域特定隐写检测（6 学时）

教学内容：

- 针对 LSB 替换隐写的检测方法；
- 针对 MLSB 替换隐写的检测方法；
- ±K 与随机调制隐写的检测方法。

考核要求：

- 掌握卡方、RS、SPA、WS 等 LSB 替换隐写的检测方法的基本原理与主要过程；
- 了解 DIH、JPEG 兼容性分析以及 DRS 和 LSM 等改进的 LSB 替换隐写的检测方法的基本原理；
- 掌握针对 2LSB 替换隐写的 Couples 检测和针对 TMLSB 替换隐写的 WS 检测的基本原理与主要过程；
- 掌握 $\pm K$ 和随机调制隐写的检测的基本原理与主要过程。

第 5 章　JPEG 图像的特定隐写检测（4 学时）

教学内容：

- 针对 JSteg 隐写的检测方法；
- 针对 F5 隐写的检测方法；
- 针对 OutGuess 隐写的检测方法；
- 针对 MB 隐写的检测方法。

考核要求：

- 掌握针对 JSteg 隐写的快速卡方检验方法的基本原理和主要过程；
- 掌握基于直方图的 F5 隐写的信息比率估计方法的基本原理和主要过程；
- 掌握基于分块效应的 OutGuess 隐写的信息比率估计方法的基本原理和主要过程；
- 了解针对 Cauchy MB 隐写的检测方法。

第 6 章　图像隐写通用盲检测（4 学时）

教学内容：

- 通用盲检测技术的研究内容和基本原理；
- 典型通用盲检测方法。

考核要求：

- 了解隐写通用盲检测的研究内容和一般原理框架，能够区别纯盲检测和半盲检测；
- 了解基于图像质量度量的盲检测方法、基于直方图特征函数质心的盲检测方法、基于共生矩阵的盲检测方法的基本原理；
- 掌握基于小波域高阶概率密度函数矩的盲检测方法；
- 掌握小波系数直方图特征函数矩的盲检测方法；
- 掌握基于多域特征综合的盲检测方法。

第 7 章　数字图像隐写信息提取（5 学时）

教学内容：

- 提取攻击研究概述；
- 隐写信息难提取性的信息论分析；
- 对连续 LSB 替换隐写术的提取攻击；
- 对随机 LSB 隐写术的提取攻击；
- 对基于图像格式的隐写术的提取攻击。

考核要求：

- 了解密码算法在隐写术中的应用，熟悉其实现机制；
- 理解难提取性的信息论分析方法；
- 掌握分析格式隐写术冗余空间的方法；
- 掌握估计连续隐写术消息嵌入起止点的方法；
- 掌握区分随机隐写术真伪密钥的方法。

目　录

Chapter 1

第1章 概论

1.1 信息隐藏简介

1.1.1 什么是信息隐藏

信息隐藏是集多学科理论与技术于一身的新兴技术，它利用载体信息在时间或空间等方面的冗余特性，把一个有意义的秘密信息(如软件序列号、消息或版权信息)隐藏到载体信息中，从而得到隐密载体，其载体可以是文字、图像、声音和视频等多媒体信息。信息隐藏后，非授权者无法确认该载体中是否隐藏了信息，也难以提取或去除所隐藏的信息，从而达到隐蔽通信、版权保护等目的。信息隐藏技术主要包括隐写术、数字水印、隐蔽信道等分支。

隐写术是利用信息隐藏技术实现隐蔽通信的技术。隐写术和密码技术各有优势，密码技术是将所要传递的信息进行特殊的编码，形成不可识别的乱码形式，使得加密后的文件变得难以理解(看不懂)；隐写术则是将特定的秘密信息隐藏在某种公开信息之中，由于对外表现的是载体信号的内容和特征，有公开信息作掩护，因此第三方不会感觉到秘密信息的存在(看不见)。从信息拦截者的角度来说，如果面对的是一堆看似杂乱无章的密文，会更加激起他破解的激情，而如果面对的是一幅已嵌入秘密信息的精美的油画，则会因受到麻痹而减弱其敏锐的观察力。因此，从解密的角度上看，用信息隐藏技术隐藏的秘密数据被第三方侦察和恢复的难度更大，它不会引起攻击者的注意和重视，从而减少被非法拦截者攻击的概率，在此基础上再运用密码技术可以进一步增强信息隐藏的安全效果。由此可见，隐写术是一种安全有效的隐蔽通信方式。

日益发展的信息技术在为多媒体信息的存取提供

了极大便利的同时也使得作品侵权更加容易，篡改更加方便。因此，信息隐藏在秘密通信之外又有了新的用武之地——版权保护和数据完整性保护等。作为信息隐藏领域的一个重要分支，数字水印为知识产权保护和多媒体防伪提供了一种有效的手段，拥有潜在的应用市场和广阔的发展前景。

1.1.2 信息隐藏的历史

现代信息隐藏技术来源于古代的隐写术(steganography)，公元 1499 年 Johannes Trithemius 将“steganos”与“graphein”两个希腊字根合并组成单词“steganography”，意味着隐写(covered writing)，即隐藏消息的存在性(existence)。隐写术是一门古老而有趣的安全传递秘密信息的方法，从中国古代文人的藏头诗到德国间谍的隐写信，从古希腊的蜡板藏书到现在的网络隐蔽通信，无不蕴藏着人类的智慧。下面介绍一些文献上记载的重要历史事件，以帮助读者了解历史上人们是如何利用隐写术的。古代的隐写术从应用上可以分为几个方面：技术性的隐写术、语言学中的隐写术等。

1. 技术性的隐写术

最早的隐写术的例子可以追溯到远古时代。在公元前 480 年著名的温泉关战役中，斯巴达国王莱奥尼达斯就是在提前接到警报后才与波斯国王薛西斯率领的军队作战的，该警报刻在一块当时人们用于书写的小蜡板上。Herodotus（公元前 486—公元前 425）在他的《Histories》一书中曾经描述到：“在古希腊反抗波斯人的战争中，为了安全地传送军事情报，奴隶主剃光奴隶的头发，将情报刻在奴隶的头皮上，待头发长起后再派出去传送秘密信息。”还有，在信函中，通过改变其中某些字母笔画的高度，或者在某些字母上面或下面挖出非常小的孔，以标识某些特殊的字母，这些特殊的字母组成秘密信息。一些夸张的绘画作品，从正面看是一种景象，从侧面看又是另一种景象，这其中就可以隐含作者的一些政治主张或思想。

英国人 Wilkins(1614—1672)是资料记载最早使用隐写墨水进行秘密通信的人。在中国的魔术中，用笔蘸淀粉水在白纸上写字，然后喷上碘水，淀粉和碘起化学反应后会显出棕色字体，这其中也隐含了隐写术的思想。化学的进步促使人们开发更加先进的墨水和显影剂。这种方法在两次世界大战中又被德国间谍重新使用起来。但是，随着“万用显影剂”的发明，不可见墨水的隐写方法就无效了。“万用显影剂”的原理是，根据纸张纤维的变化情况来确定纸张的哪些部位被水打湿过，这样，所有采用墨水的隐写方法，在“万用显影剂”下都无效了。

1857 年，Brewster 就已经提出将秘密消息隐藏在“大小不超过一个句号或小墨水点的空间里”的设想。到 1860 年，制作微小图像的难题被法国摄影师 Dragon 解决了，很多消息可以放在微缩胶片中。在 1870 至 1871 年弗朗格－普鲁士战争期间，巴黎被围困时，通过信鸽传递印制在微缩胶片中的消息。Brewster 的设想在第一次世界大战期间付诸实现，其做法是：先将间谍之间要传送的消息经过若干照相缩影后缩小到微粒状，然后粘贴在无关紧要的杂志等文字材料中的句号或逗号上。

2. 语言学中的隐写术

语言学中的隐写术最广泛使用的方法是藏头诗。国外最著名的例子可能要算 Giovanni Boccaccio(1313—1375)的诗作《Amorosavisione》，据说是“世界上最宏伟的藏头诗”作品。他先创作了三首十四行诗，总共包含大约 1500 个字母，然后创作了另一首诗，使连续三行押韵诗句的第一个字母恰好对应十四行诗的各个字母。中国古代也有很多藏头诗(也称嵌字诗)，并且这种诗词格式也流传到现在。相传宋代时，蜀郡才女苏小妹曾三难新郎，开始她写了四句诗让秦少游猜，诗云：“钢铁投洪冶，蝼蚁上粉墙。阴阳无二义，天地我中央。”秦少游一看，这四句诗正是嘲笑他的，因为他曾假扮云游道人，在岳庙化缘，去相苏小妹。于是他便写了一首诗云：

化工何意把春催?
缘到名园花自开。
道是东风原有主，
人人不敢上花台。

苏小妹一看，原来是一首藏头诗，每句顶头一字，合之乃“化缘道人”四字，正合她的诗谜。

到了 16 世纪和 17 世纪，已经出现了大量关于伪装术的文献，其中许多方法都依赖于一些信息编码手段。Gaspar Schott(1608—1666)在他的 400 页著作《Schola Steganographica》中，扩展了由 Trithemius 在《Polygraphia》一书中提出的“福哉马利亚”(Ave Maria)编码方法(《Polygraphia》和《Steganographia》是密码学和隐藏学领域所知道的最早出现的两本专著)。扩展的编码使用 40 个表，其中每个表包含 24 个用四种语言(拉丁语、德语、意大利语和法语)表示的条目，每个条目对应于字母表中的一个字母。每个字母用出现在对应表的条目中的词或短语替代，得到的密文看起来像一段祷告、一封简单的信函或一段有魔力的咒语。

尽管信息隐藏技术已经有久远的研究和应用历史，但是在当时的技术条件下，信息隐写的手段和应用条件是十分有限的。在很长一段时间里，信息隐藏技术无论在研究领域还是在实际应用中都未受到关注。随着科学技术的发展，古老的隐写术在信息时代又成为新的研究热点。在数字化、计算机、网络等这些新时代的产物的孕育中，基于信息理论、数理统计理论、认知心理学和现代信息技术手段，崭新的隐写术——现代的信息隐藏技术应运而生。新的内涵，新的处延，新的方法，新的技术，使人们不得不重新审视和研究这一源远流长的信息安全技术。

1.1.3 现代信息隐藏技术

1. 现代信息隐藏技术的特点

经过十几年的研究和发展，信息隐藏技术不同的应用使它形成了不同的特点。但是，所有的信息隐藏系统共有一些基本的特点。作为利用数字通信技术来进行隐蔽信息通信的一种手段，信息隐藏技术具有的基本特点主要有以下几种。