信号与信息处理丛书

国家自然科学基金研究专著

数字密写和密写分析

—— 互联网时代的信息战技术

王朔中 张新鹏 张开文 著

清华大学出版社

信 号 与 信 息 处 理 丛 书

国家自然科学基金研究专著

数字密写和密写分析

——互联网时代的信息战技术

王朔中 张新鹏 张开文 著

清华大学出版社

北 京

内 容 简 介

数字密写和密写分析是互联网时代信息战中的一项重要技术。本书以密写、反密写之间的对抗为主线，讨论当前这一领域的主要技术和发展前沿，还反映了作者近年来的研究成果。第1、2章介绍信息隐藏和数字密写的基本概念、分类和一般技术要求。第3章到第8章分别讨论各种密写和密写分析技术，包括以各种图像和音频为载体的密写和密写分析技术，如基于LSB的密写及其分析方法、基于视听觉特性的方法、扩频技术的应用、无损密写技术、隐蔽嵌入信息的存在性检测等。第9、10、11章分别讨论对密写的积极攻击、密写编码、密写和计算机网络安全的关系等问题。

密写和反密写研究对信息安全具有重要意义，随着信息技术的迅速发展正在受到愈来愈多的关注。本书可供信息技术、通信工程、计算机科学和工程、电子技术等领域中关注信息安全和多媒体应用的工程技术人员和科研教学人员阅读，也可以作为研究生和大学高年级学生的教材和参考书。

图书在版编目(CIP)数据

数字密写和密写分析——互联网时代的信息战技术/王朔中，张新鹏，张开文著．—北京：清华大学出版社，2005.4

(信号与信息处理丛书)

ISBN 7-302-10285-6

Ⅰ．数…　Ⅱ．①王…　②张…　③张…　Ⅲ．电子计算机－密码术　Ⅳ．TP309.7

中国版本图书馆CIP数据核字(2004)第143574号

出 版 者：清华大学出版社
http://www.tup.com.cn
社 总 机：010-62770175
地　　址：北京清华大学学研大厦
邮　　编：100084
客户服务：010-62776969

组稿编辑：陈国新
文稿编辑：张占奎
印 刷 者：北京密云胶印厂
装 订 者：北京市密云县京文制本装订厂
发 行 者：新华书店总店北京发行所
开　　本：185×260　**印张**：12　**彩插**：1　**字数**：281千字
版　　次：2005年4月第1版　2005年4月第1次印刷
书　　号：ISBN 7-302-10285-6/TN·228
印　　数：1～3000
定　　价：24.00元

丛书出版说明

FOREWORD

信号与信息处理可以说是信息技术中的核心部分。随着信息科学与技术的飞速发展，随着信息技术深入到各个领域而得到广泛的应用，信号与信息处理也作为前沿技术而发生着重大的变化。编辑出版“信号与信息处理丛书”正是为了反映这种变化，为了加速培养这方面的人才，也为了进一步推动这一领域的发展。本丛书的内容力求能反映信号与信息处理技术的前沿内容，具有高的学术意义与应用价值。入选的书稿可以是创作的专著，也可以是高水平的译作。

这套丛书不仅适合于作研究生教学参考之用，可作为高校教师与有关领域研究人员学习与参考书。

从历史来看，真正影响着生活的是不断增长的知识与技术的积累和经反复探索所形成的观念。相信这套丛书的出版，会增加正在成长中的信号与信息处理技术的各积累，而它对生活的作用则是显而易见的。

李衍达

2004 年 8 月 24 日

序

PREFACE

20世纪90年代以来，随着计算机网络通信的蓬勃发展，借助个人计算机连接因特网，可将各种消息（文字、图像、声音、多媒体数据等）迅速地传播到世界各地。低廉的通信费用，便捷的上网方式，给人们提供了一个全新的通信环境。政府、企业、个人都在利用这一开放互连的公共信息网络平台，构建各自的专用网络，传递各自的私密信息。因特网的平民化和便捷性，既给人们带来了信息传递的快捷通道，同时也给人们带来了信息安全上的诸多问题。

信息安全的概念是随着信息技术的发展而不断拓宽和深化的。从早期的通信安全，发展到计算机安全、信息系统安全，现已拓展到对信息基础设施、信息应用服务和信息内容等实施全面保护的信息安全保障。信息安全的内涵也不断丰富，由单一的通信信息的保密，拓展到对信息的保密性、完整性、真实性、可控性、信息基础设施的可用性以及信息交互行为的不可否认性等的全面保护。信息安全已成为国家安全的重要组成部分，具有与国家政治安全、经济安全、领土安全同等重要的地位，为经济发展、社会稳定、国家安全和公众权益提供保障。

信息安全技术也随着信息化的发展而不断发展和丰富。信息隐藏技术作为信息安全中的一项重要技术，近十年来引起了国内外学术界和相关部门的重视。出于对保护多媒体产品知识产权不断增长的需求，出于使用密码技术受到限制而又必须进行隐秘通信的特殊需求，信息隐藏中的数字水印技术和隐藏通信技术（或称数字密写技术）得到了迅速发展。数字密写是将秘密信息嵌入到载体信号中，通过公众媒体传输而不被察觉，不引起任何怀疑。针对数字密写这一隐藏通信手段，反密写技术也相应地发展起来，其中密写分析就是利用各种统计分析方法，揭示载体信号中隐蔽信息的存在性，这是反密写技术的关键一步。只有发现载体信号中嵌有隐藏信息，才能开展隐藏信息的提取和破译工作。

数字密写和密写分析涉及计算机、通信、编码、信号处理、数理统计、视听觉特性等知识和技术，是一个跨学科的新领域。无论是在多媒体信号中嵌入不易察觉的隐蔽信息，还是从大量媒体信号中检测这种隐藏信息的存在性，都是富有挑战性的技术课题。研究人员不断提出新的密写方法，有些方法不久就被证实是可以检测出隐藏信息的，这个结果又推动研究人员提出新的密写方法。这种交替更新促进了信息隐藏技术的不断发展。如同密码学中破译学滞后编码学，破译一个密码比编制一个密码更难一样，密写分析滞后于数字密写，对密写的成功分析要比密写本身更加困难。总的来说，数字密写和密写分析的矛盾双方都

有不少问题未被认识，有不少难点尚未攻克，需要有志于研究信息隐藏的人员不断地进行深入的研究。

我欣喜地看到由王朔中教授、张新鹏博士、张开文博士合著的《数字密写和密写分析——互联网时代的信息战技术》一书的出版。该书将基础理论与技术方法紧密结合，反映了当前数字密写和密写分析的研究前沿，包含了该领域中许多重要方法，是一本很有参考价值的专著。书中较系统地介绍了国内外学术界近年来在信息隐藏方面取得的进展，也总结了作者近几年来在密写和密写分析方面的研究工作。作者站在信息对抗的高度对数字密写和密写分析中的重要问题展开广泛深入的讨论，展现了数字密写和密写分析这对矛盾相互促进、交替发展的特点。

数字密写和密写分析的研究正方兴未艾，本书既可作为数字密写和密写分析的入门书，也可以当作深入研究的起点。本书的出版必将有助于读者掌握数字密写和密写分析的基本概念和主要方法，了解这一领域的现状和发展趋势，并将对信息安全的研究和应用起到积极的推动作用。

中国工程院院士 周仲义

2004 年 11 月

前言

FOREWORD

自从20世纪90年代初以来，信息隐藏技术作为信息安全中的重要课题引起了国际学术界的普遍重视。首先是对保护多媒体产品知识产权的数字水印研究急剧升温。从1995年开始，公开发表的数字水印方面的论文逐年呈指数上升，到20世纪90年代后期已出现大批高水平的研究成果，不少开发数字水印产品的公司也应运而生，其产品在不同领域得到了广泛的应用。近年来，数字水印技术仍保持着强劲的发展势头。

隐蔽通信或数字密写(steganography)是信息隐藏的另一个重要分支，其发展相对滞后一些。虽然早就出现了一些简单的密写方法，但对这一领域的深入研究是从世纪之交真正开始的。到目前为止，有关研究成果的发表已表现出明显的上升趋势。密写的目的是以表面正常的数字载体(如静止图像、数字音频和视频信号等)作为掩护，在其中隐藏秘密信息。额外数据的嵌入既不改变载体信号的视觉、听觉效果，也不改变计算机文件的大小和格式(包括文件头)，从而使隐蔽信息能以不为人知的方式进行传输。含密载体通常与大量正常的多媒体资料混在一起，经过各种渠道特别是互联网传播出去。与传统的密码通信不同的是，这里“正在进行通信”这一事实本身也被隐藏起来。

针对密写这一隐蔽通信手段，反密写技术也迅速发展起来。反密写的首要目标是对多媒体信号进行统计分析，判断其中是否含有隐蔽信息，即进行密写分析(steganalysis)。一般认为，只要隐蔽信息的存在性受到怀疑，那么所用的密写技术就是不安全的，或者说密写失败了。对密写的成功分析要比密写本身更加困难，因为各类数字载体数量巨大，嵌入方法又千变万化，从中搜寻隐蔽信息犹如大海捞针。另外，对密写还可以实施积极攻击(active attack)，即删除或破坏嵌入信息以达到阻止隐蔽通信的目的。

密写和反密写是互联网时代信息战的一项重要内容，对于信息安全具有重要意义。一方面，密写使保密通信更加安全。另一方面，随着网上信息量急剧增加，人们也注意到对信息新技术的恶意使用可能对社会安全造成严重威胁。“九一一”事件以后，密写被国际恐怖组织用于传递敌对信息的可能性引起了研究人员和公众的强烈关注。此外，密写还能使恶意代码潜入对方信息系统并带来巨大的破坏作用。因此，密写和反密写受到各国政府、军方、情报部门、研究机构的高度重视，近两年来研究力度已经明显加大。将密写与反密写作为一项重要课题纳入信息安全研究的框架以应对日益尖锐复杂的信息战，已成为十分紧

迫的任务。

由于密写是在一个数据量较大的数字载体中嵌入不可感知的附带信息，因此也有广泛的民用和商业前景，例如可望在新一代的视音频产品、远程教学、医学信号处理、移动多媒体通信等许多领域得到应用。

本书内容包括密写和反密写的原理、技术基础和主要方法，着重反映近年来国际上在这一领域的研究水平和动态，书中还包含了作者所在课题组近几年的研究成果。全书共11章。第1章为绪论。第2章扼要介绍信息隐藏技术的两个主要分支，即数字水印和数字密写，对它们的技术要求和性能指标进行比较。第3章至第7章分别介绍重要的密写和密写分析方法，包括最早出现且目前应用最广的LSB密写，基于调色板图像和JPEG图像的密写，利用扩频等技术、基于视觉特性的多种密写和密写分析技术。其中大部分是以图像为载体，有一些方法也可应用于数字音频信息。第8章讨论以音频为载体的密写和密写分析技术。第9章讨论对密写的积极攻击。第10章讨论密写编码，研究如何对原始载体作尽量小的改动来达到隐藏更多的秘密数据的目的，以及如何在保证安全性的前提下提高嵌入效率。第11章从网络信息安全的角度讨论密写和反密写技术的作用和地位。

本书可供信息技术、通信工程、计算机、电子技术等领域中关注信息安全和多媒体应用的工程技术人员、科研教学人员、研究生和大学本科高年级学生使用。

承蒙周仲义院士在百忙之中审阅书稿并为本书作序，他的建设性意见对我们今后的研究工作有极大的启发，我们在此表示由衷的感谢。

本书凝聚了课题组全体成员历年来研究工作的心血。第1、8、11章，以及第3、7、9章的部分内容由王朔中执笔；第2章至第6章，第3、7、9章的部分内容以及第10章由张新鹏执笔；张开文撰写了第7、9两章中的部分内容。王朔中负责全书的组织、整理和统稿。贾骏、胡烨雯、马田、桑宏伟在图像密写分析、数字音频信息隐藏等方面进行了大量的研究，为本书的写作提供了重要的素材。胡礼才、梁光岚、夏明一、马小松、李卫华、朱繁源、刘伟、陆健峰参加了研究工作并提出了许多有价值的见解。

本书工作受国家自然科学基金项目(60072030，60372090)和上海市重点学科建设项目(2001-44)项目资助。感谢国家自然科学基金委员会成果专著出版科学基金的资助(60424001)。

由于作者水平所限，书中不足和疏漏之处在所难免，敬请同行专家和广大读者不吝指教。

作　者

2004年9月于上海

目录

CONTENTS

第1章 CHAPTER 1

绪论

1.1 信息隐藏和互联网时代的信息战

20世纪90年代以来，信息隐藏成为信息技术领域的一大研究热点。信息隐藏的目的是在图像、音频、视频等数字媒体信号中嵌入不可察觉的隐蔽数据。这种技术的一个突出应用领域就是保护数字媒体知识产权的数字水印。随着互联网的迅速发展，数字媒体易于复制、易于广泛传播的特点使得版权保护的重要性日益突出。作为版权保护的一种技术手段，数字水印也日益受到重视，到20世纪90年代中后期，其研究成果大量涌现出来。

与此同时，针对数字水印的各种攻击手段也层出不穷，其目的是使水印失效从而实施侵权，例如使含水印的图像产生微小的几何形变或通过抽去数字音频信号的个别样本等方法破坏水印检测中的同步，加入伪造的水印以混淆版权的归属，根据多个含有合法水印的不同版本进行合谋攻击达到删除水印的目的等。除了这些恶意攻击外，常规的信号处理如滤波、信号剪裁、图像增强、压缩编码等也对数字水印的有效性构成严重威胁。凡此种种都促使水印嵌入技术不断改进，同时新的攻击手段又不断出现，形成了攻守双方相互对抗、相互推动的局面。

除了用于版权保护的数字水印以外，信息隐藏的另一重要分支是隐蔽通信。以图像、音频等数字媒体作为掩护，把要发送的秘密消息嵌入到载体信号内部，以不引起外界注意的方式通过公共信道，特别是互联网进行传递，这就是密写(steganography)。基于密写的隐蔽通信不同于传统的密码通信。密码通信传递加密的数据，使对方无法破译密码，从而达到保密目的。传统的密码通信一般并不刻意掩盖“正在进行通信”这一事实。密写则不同，它利用易于迷惑对方的载体(宿主信号)掩护欲传递的秘密消息，通过将消息嵌入宿主信号而不引起视(听)觉和统计可察觉的畸变来保证其安全性。“秘密通信正在进行”这一事实必须不为他人知晓。当然，数据在嵌入前也可以进行加密以进一步提高隐蔽通信的安全性，但一般说来这是两种相互独立的技术，密码学的问题不属于本书讨论

的范围。

早在2001年初，震惊世界的“九一一”事件发生半年多以前，美国发行量很大的报纸《今日美国》就曾刊登文章，指出本·拉丹及其同伙可能利用某些网站上的大量数字图像秘密传递与恐怖活动有关的信息，如指令、地图、攻击目标的资料等[1]。当时还有报道指出，一些著名的网站如eBay和Amazon等已成为传播密写信息的隐蔽渠道。据信首先将欧美科学家在密写研究中取得的早期成果用于实践的就有基地和哈马斯等国际恐怖组织[2]。另外，一些国家的警方也曾在恐怖组织的计算机内查获大量可疑图像和视频文件，据分析可能藏有与恐怖活动有关的信息[3]。

虽然大众媒体上的这些报道在当时并没有引起社会各界的普遍关注，却激发了少数研究人员的极大兴趣。一些研究者开始对著名拍卖网站eBay上数以百万计的图像展开搜索和检测，试图寻找可能存在的敌对隐蔽信息[4]，并用所谓字典式攻击法分析了USENET上数以百万计的文档[5]。这些努力的结果虽然未能找到隐蔽恐怖信息的确凿证据，却推动了信息技术和计算机网络领域中关注信息安全的科技人员对密写术和密写分析进行深入研究。“九一一”事件以后，密写被用于恐怖袭击的可能性经媒体广泛宣传，引起了各国政府和公众的强烈关注[6,7]，更加有力地促进了近年来信息隐藏这一重要分支的迅速发展。

密写和密写分析在军事、情报、国家安全方面的重要意义不言而喻，它们在信息安全中所处的重要地位成为研究者深入探索的强大动力。设计高度安全的密写方法是一项富于挑战性的课题，而对密写的准确分析往往比密写本身更加困难。一方面是要以尽可能隐蔽的方式将信息深藏于浩如烟海的数字多媒体信号中，毫不引起对方的怀疑而达到秘密通信的目的；另一方面则要以各种手段检测可疑信息的存在，寻找敌对隐蔽通信的信源，阻断隐蔽通信的信道。密写和密写分析的对抗和交互发展正方兴未艾，其发展还有待人们的不懈努力。这就是本书所讨论的主题，它是互联网时代信息战技术的一个新课题。

1.2 密写与密写分析的概念和基本技术要求

1.2.1 密写

密写一词来源于希腊文 στεγανοζ+γραφειν。利用密写传递秘密信息的实践古已有之[8~10]。一个著名的例子是罗马人将机密消息刺在剃光了头发的信使头上，等头发长长后再将信使派往敌后，收信方为了读取密写的消息需要重新将信使的头发剃去。在上一世纪的两次世界大战中，交战双方普遍使用隐形墨水书写机密文件，以便将信息送达潜伏在敌后的特工人员。另外还可在表面上看似普通的文件中嵌入隐蔽文字以实现密写，例如在第二次世界大战中，德国间谍曾在下列两段文字中秘密传递军事情报[11]：

- President's embargo ruling should have immediate notice. Grave situation affecting international law. Statement foreshadows ruin of many neutrals. Yellow journals unifying national excitement immensely.
- Apparently neutral's protest is thoroughly discounted and ignored. Isman hard