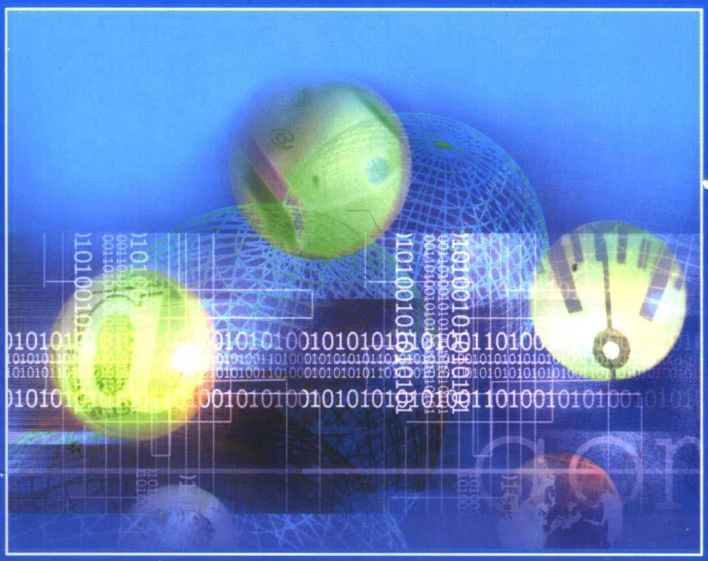
信息隐藏技术

Information Hiding Technique

王炳锡　彭天强　编著



国防工业出版社
National Defense Industry Press

信息隐藏技术

Information Hiding Technique

王炳锡　彭天强　编著

国防工业出版社

·北京·

图书在版编目(CIP)数据

信息隐藏技术/王炳锡，彭天强编著. —北京：国防工业出版社，2007.9

ISBN 978-7-118-05153-7

Ⅰ. 信… Ⅱ. ①王…②彭… Ⅲ. 信息系统—安全技术 Ⅳ. TP309

中国版本图书馆 CIP 数据核字(2007)第 060574 号

※

国防工业出版社出版发行

(北京市海淀区紫竹院南路 23 号　邮政编码 100044)

国防工业出版社印刷厂印刷

新华书店经售

*

开本 850×1168　1/32　印张 9　字数 225 千字

2007 年 9 月第 1 版第 1 次印刷　印数 1—3000 册　定价 32.00 元

(本书如有印装错误，我社负责调换)

国防书店：(010)68428422　　发行邮购：(010)68414474

发行传真：(010)68411535　　发行业务：(010)68472764

致 读 者

本书由国防科技图书出版基金资助出版。

国防科技图书出版工作是国防科技事业的一个重要方面。优秀的国防科技图书既是国防科技成果的一部分，又是国防科技水平的重要标志。为了促进国防科技和武器装备建设事业的发展，加强社会主义物质文明和精神文明建设，培养优秀科技人才，确保国防科技优秀图书的出版，原国防科工委于1988年初决定每年拨出专款，设立国防科技图书出版基金，成立评审委员会，扶持、审定出版国防科技优秀图书。

国防科技图书出版基金资助的对象是：

1. 在国防科学技术领域中，学术水平高，内容有创见，在学科上居领先地位的基础科学理论图书；在工程技术理论方面有突破的应用科学专著。

2. 学术思想新颖，内容具体、实用，对国防科技和武器装备发展具有较大推动作用的专著；密切结合国防现代化和武器装备现代化需要的高新技术内容的专著。

3. 有重要发展前景和有重大开拓使用价值，密切结合国防现代化和武器装备现代化需要的新工艺、新材料内容的专著。

4. 填补目前我国科技领域空白并具有军事应用前景的薄弱学科和边缘学科的科技图书。

国防科技图书出版基金评审委员会在总装备部的领导下开展工作，负责掌握出版基金的使用方向，评审受理的图书选题，决定资助的图书选题和资助金额，以及决定中断或取消资助等。经评审给予资助的图书，由总装备部国防工业出版社列选出版。

国防科技事业已经取得了举世瞩目的成就。国防科技图书承担着记载和弘扬这些成就，积累和传播科技知识的使命。在改革开放的新形势下，原国防科工委率先设立出版基金，扶持出版科技图书，这是一项具有深远意义的创举。此举势必促使国防科技图书的出版随着国防科技事业的发展更加兴旺。

设立出版基金是一件新生事物，是对出版工作的一项改革。因而，评审工作需要不断地摸索、认真地总结和及时地改进，这样，才能使有限的基金发挥出巨大的效能。评审工作更需要国防科技和武器装备建设战线广大科技工作者、专家、教授，以及社会各界朋友的热情支持。

让我们携起手来，为祖国昌盛、科技腾飞、出版繁荣而共同奋斗！

国防科技图书出版基金
评审委员会

国防科技图书出版基金
第五届评审委员会组成人员

主任委员	刘成海			
副主任委员	王　峰	张涵信	程洪彬	
秘书长	程洪彬			
副秘书长	彭华良	蔡　镭		
委　　员	于景元	王小谟	甘茂治	刘世参
（按姓氏笔画排序）	杨星豪	李德毅	吴有生	何新贵
	佟玉民	宋家树	张立同	张鸿元
	陈冀胜	周一宇	赵凤起	侯正明
	常显奇	崔尔杰	韩祖南	傅惠民
	舒长胜			

前　言

信息隐藏技术作为信息安全领域的最新研究热点，在近几年得到了很大的发展，已经在人类生活的许多方面得到了相当广泛的应用，其驱动力来自信息时代的两大需求——信息安全和版权保护。由此，信息隐藏技术在隐秘术和数字水印两个方面展开。隐秘术研究如何将秘密信息隐藏在不太容易引起注意的消息中，从而使得秘密通信不被觉察，而数字水印则源于数字媒体作品的版权保护。

当前，我国信息化正以一日千里的速度飞速发展，信息安全的需求十分迫切。信息安全隐患全方位地危及社会的经济、政治、文化等各个方面，利用计算机网络进行犯罪、窃取机密信息的案例屡见不鲜。然而，网络与信息安全问题必须依靠我国自己的力量来解决，引进国外产品或照搬国外先进技术无异于引狼入室。为此，国家明确规定："信息安全产品一定要立足国内，自主开发。"

信息隐藏是一个既古老又年轻的技术。说其古老，历史上最早的记载可以在古希腊历史学家希罗多德（Herodotus，公元前484—425）的著作中找到。说其年轻，是现代信息技术和计算机技术的发展，以数字媒体为载体的信息隐藏技术刚刚创建。在国际上，1996 年在英国剑桥大学举行的第一届信息隐藏研讨会是现代信息隐藏的里程碑，它是信息科学、密码学、数字信号处理、计算机科学、网络技术、通信技术等多学科交叉融合的产物。2002 年在韩国汉城举办了第一届国际数字水印会议，以后每年举办一次，为数字水印技术的交流提供了一个国际平台。由于其在军事斗争、国家安全、电子商务、电子政务、网络通信、个人隐私、版权保护等方面的广泛应用，许多大学、研究机构、IT 公司纷纷开展这方面的

研究，国际上有公开的网站，提供交流的论坛，有成熟的软件下载。国内在信息隐藏方面的研究起步稍晚，但已引起信息安全领域学者的高度重视。国家自然科学基金委员会、国家重点基础研究发展规划以及信息安全国家重点实验室都给予了重点支持。1999年12月召开了第一届信息隐藏技术研讨会。会议决定每年召开一次，以促进国内信息隐藏技术的研究工作。2000年1月召开了国内第一届数字水印技术研讨会，并建立了数字水印研究主页和邮件列表，对国内信息隐藏研究工作起到了很好的促进作用。特别是2005年4月1日正式施行了《中华人民共和国电子签名法》，它规范了电子签名的行为，确立了电子签名的法律效力，维护了各方面的合法权益，使电子印章走向政府机关、商务贸易、金融证券及社会公众，标志着我国信息隐藏技术研究在实用化方面已达到国际先进水平。

信息隐藏技术要走向实用化，必须要解决嵌入容量、安全性和稳健性3个不同的但是又相互关联的问题。随着现代科学技术的发展，隐秘术和数字水印技术有了长足的发展，结合实际应用，又有新的技术不断产生。如利用操作系统中的漏洞制造的隐通道、数字签名中的潜信道、密码协议缺陷中的阈下通道、利用流星轨迹的猝发通信和扩频通信的低截获概率通信等，以及数字作品跟踪标识的数字指纹、计算机软件产品的软件水印、网上匿名通信、电子选举、电子现金、电子印章等。

信息隐藏分析作为信息隐藏的攻击技术同样重要。它们是一对孪生姐妹，是矛盾的两个方面。尽管信息隐藏系统要使人类感觉系统不容易察觉到某种程度的变形和降质，但某种程度的变形和降质确实存在。这种变形或降质如果被察觉到了，引起了怀疑，那么隐藏就是不成功的。隐藏分析是发现并获得隐藏信息或使这些信息无效。隐藏信息的发现、检测、提取是难度很大的一个课题，这需要寻找信息隐藏过程中各个环节的缺陷和特征，研制一系列分析工具；反过来，也能对开发健壮性更强的技术给予指导。这一对矛盾在斗争中发展，在斗争中创新。对于版权保护的数字水

印技术还需要相应的法律法规予以支撑。

实践表明，没有理论指导的研究是无源之水，无本之木。

应该看到，Simmons 在 1983 年提出以“囚犯问题”作为隐秘系统的通用模型，利用随机和冗余技术使其具备信息的隐形性，同时要求具有信息的完整性和机密性。对于数字水印稳健性要求更高一些。信息隐藏应用的广泛性，要求我们建立一个其安全性能够被数学证明的信息隐藏理论体系来为信息隐藏技术的可行性和安全性作出保障。我们认为，仅有 Shannon 密码系统理论和 Simmons 认证系统理论是不够的。从信号处理角度看，信息隐藏是强背景下叠加了一个弱信号；从通信角度看，信息隐藏是在一个宽带信道上用扩频技术传输一个窄带信号。这种思路同样有局限性，构建一个信息隐藏理论体系势在必行，需要广大学术界同行共同努力。

本书以作者的研究工作为主，重点对数字水印和隐秘通信两个方面的最新进展进行总结，其中在印刷品数字水印防伪技术研究、信道信息隐藏技术研究和信息隐藏分析研究方面有所创新。对于我们来说，分析、整理本身就是一个理清思路，提高自身认识水平的过程；同时与学术界同行交流，共同探讨也是我们的愿望。为了增强本书的可读性，我们对原理的讲述和方法的介绍并重。书中根据实验结果提供了大量的实验参数和图表供读者参考。

本书共分 8 章。第 1 章介绍信息隐藏基础知识，包括信息隐藏的基本概念、理论、应用和发展现状；第 2 章介绍隐秘术的基本原理和方法，并分析了隐秘系统的安全性；第 3 章至第 5 章介绍目前信息隐藏的重点——数字水印技术，包括数字图像水印、数字音频水印、视频和文本水印技术，较详细地介绍了几个应用实例；第 6 章介绍基于数字水印的印刷品防伪技术；第 7 章介绍信道信息隐藏技术；第 8 章介绍隐写分析技术。各章节之间紧密配合，前后呼应，具有很强的系统性。同时，通过书中对研究过程和研究方法的讲述，相信读者能够在以后的研究工作中得到很大的启发。

本书的撰写得到了解放军信息工程大学各级领导的关心和支

持，并得到了国内广大学者的支持和帮助，尤其是课题组的同志和研究生的研究成果充实和完善了本书的内容，在此一并表示感谢。书中引用了大量的文献资料，在此向原作者表示深深的谢意。

因本人学术水平有限，不足之处在所难免，恳请读者不吝赐教。

王炳锡

2006 年 10 月 30 日

于解放军信息工程大学

目　录

Contents