通信信息隐匿技术

Steganography of Telecommunication Information

柏 森 胡中豫 吴乐华 周道华 编著

国防工业出版社
National Defense Industry Press

通信信息隐匿技术

Steganaography of Telecommunication Information

柏　森　胡中豫
吴乐华　周道华　编著

国防工业出版社
·北京·

图书在版编目(CIP)数据

通信信息隐匿技术/柏森等编著.—北京:国防工业出版社,2005.7

ISBN 7-118-03923-3

Ⅰ.通… Ⅱ.柏… Ⅲ.通信对抗 Ⅳ.TN975

中国版本图书馆 CIP 数据核字(2005)第 046204 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)

腾飞胶印厂印刷

新华书店经售

*

开本 850×1168 1/32 印张 11½ 296 千字

2005 年 7 月第 1 版 2005 年 7 月北京第 1 次印刷

印数:1—3000 册 定价:36.00 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
第四届评审委员会组成人员

名誉主任委员	陈达植				
顾　　问	黄　宁				
主 任 委 员	刘成海				
副主任委员	王　峰	张涵信	张又栋		
秘　书　长	张又栋				
副 秘 书 长	彭华良	蔡　镭			
委　　员	于景元	王小谟	甘茂治	冯允成	
（按姓名笔画排序）	刘世参	杨星豪	李德毅	吴有生	
	何新贵	佟玉民	宋家树	张立同	
	张鸿元	陈火旺	侯正明	常显奇	
	崔尔杰	韩祖南	舒长胜		

前　言

20世纪90年代中后期，诞生了一门新的学科——信息隐藏学，其主要内容包括信息隐匿技术和数字水印技术。受安全通信和版权保护需求的驱动，该学科近年来的发展异常迅猛。作为军队的科技工作者，我们更着眼于前者。通信安全，尤其是军事通信安全保障迫在眉睫。加密通信保护通信的内容，使其不被第三方理解，其基本技术是置乱。隐蔽通信、保护通信信号，使其不被第三方干扰、检测和截获，比加密通信安全更进了一步，其基本技术是扩频、跳频等。以通信信息隐匿技术为核心的“掩密通信”(Steg－communication)既可保护通信的内容(通过加密)，又可保护通信信号(通过隐匿)，使其不被第三方获得。因此，可以说它是安全通信技术的又一次飞跃。在军事手段强大到“发现即摧毁”的今天，掩密通信技术将有望成为军事通信领域的重要通信方式之一。

《通信信息隐匿技术》是作者根据多年来在该领域的科研工作实践及科研成果，结合阅读国内外专家、学者发表或出版的相关领域论文和著作，在此基础上，经过研讨、分析和综合后撰写的。本书试图以基于信息隐匿的掩密通信技术为主线，比较全面、系统地阐述有关通信信息隐匿的基本理论、基本方法，为从事通信安全理论教学、科研的教师和工程技术人员提供一本较全面的参考书，为有志于从事该领域学习和研究的本科生和研究生提供一本研习用书。

全书共分为8章：第1章绪论，主要介绍掩密通信及通信信息隐匿技术的特性、发展历史及研究现状，阐述现代安全通信系统的发展趋势；第2章基本概念，主要介绍信息隐匿技术的基本概念，

论述信息隐藏学科的概貌及其与密码学的区别，介绍信息隐匿及掩密通信系统的基本模型和安全性问题；第 3 章预备知识，主要介绍信息隐匿技术中用到的图像声音质量的评价方法、人类视觉听觉掩蔽特性、置乱变换、小波变换等基础知识；第 4 章通信信息的预处理技术，论述置乱技术在信息隐匿技术中的功能和作用，着重研究各种置乱算法及其性能；第 5 章通信信息隐匿的基本技术，主要介绍和研究各类典型的信息隐匿技术的基本原理及性能；第 6 章信息隐匿于声音的技术，介绍声音中隐匿通信信息的基本原理、算法和仿真性能分析；第 7 章掩密通信的信道容量，讨论掩密信道的模型和容量定义，主要介绍以图像为掩密信道的信息隐匿容量的计算方法；第 8 章通信信息隐匿检测与攻击技术，主要介绍掩密分析的概念、分类和各种掩密分析方法，着重介绍以图像为载体的各种掩密分析方法的基本原理、关键技术及性能。

第 1 章～第 4 章由柏森教授撰写，第 5 章由胡中豫教授撰写，第 6 章由吴乐华教授撰写，第 7 章由周道华副教授撰写，第 8 章由柏森、胡中豫教授撰写。本书撰写过程中，得到了总参通信部李德毅院士的关怀和指导，在此表示深切的感谢。重庆大学朱桂斌博士提供了很多有价值的研究成果，重庆通信学院图像通信实验室研究生赵波、曹玉强、尤春艳、王潇、王修运为本书面世也付出了辛勤的劳动，在此一并表示感谢。

信息隐藏是一门新的学科，信息隐匿技术是新兴技术，其发展日新月异，最近几年的进展可以与密码学在 1945 年—1990 年的进展相比。其对抗技术，即掩密分析技术也在迅速发展，加之作者水平有限，难免有遗漏、错误和不妥之处，敬请读者不吝指正，作者不胜感激。

编者

目　录

Contents

第1章 绪 论

在人类历史的长河中，人们在不断地寻求更快捷、更有效和更安全的交流与通信技术。从最早的洞穴图画、烽烟信号、鸣鼓警报，到后来文字产生、电报发明、广播传送、电视普及，直至今天的Internet与E-mail。这还仅仅是我们所能描述的一个小小的片段，未来的通信将是难以想象的。不过，随着时代的前进，社会的进步，科技的发展，新的需要、新的发展机会将不断产生，通信中新的问题、新的技术将不断涌现。以通信信息隐匿技术为核心的掩密通信正是最新涌现出的一朵绚丽奇葩。

在通信安全方面，从古代的“隐写术”为代表的秘密通信，到近代以加密技术为代表的安全通信，再到现代以扩频、跳频等技术为代表的隐蔽通信，安全通信方式随着新技术发展正发生着巨大的变化。同时，随着计算机等技术的普及与发展，通信安全越来越面临着前所未有的挑战。20世纪末期，随着信息技术数字化、多媒体化及计算机通信技术的发展，诞生了一门新型学科——信息隐藏学(或称信息掩密学)，从而产生了以此为核心的掩密通信技术。尽管该门学科理论尚未成熟、技术有待发展，但我们相信，随着理论研究的深入、技术应用的广泛，该学科将迅猛发展。并且可以预料，在不久的将来，安全通信，特别是军事及保密通信将朝着掩密通信的方向发展，将从被动的“隐匿、置乱、躲避”到主动的“显现、明示、暴露”，使敌方找不到干扰、截获、攻击的目标。找不到敌人的战斗将是最困难的战斗。

1.1 掩密通信的特点和作用

1.1.1 加密通信的局限性及面临的挑战

在保密通信和军事通信中,仅希望信息接受者能收到通信的内容,即保证通信消息是秘密的。以前的做法是用加密技术将通信的内容进行加密,没有密钥的其他接受者不能理解通信的内容。今天,为防止欺诈,银行卡号通过加密后才能在网上电子商务中进行安全的交易。战时,军队的作战计划或重要的军事目标位置在传输前都要通过加密。公司新产品的设计和研发,也要通过加密来防止工业间谍。然而随着计算技术,特别是计算机网络化的迅速普及和发展,加密通信的安全问题越发显得突出,电子商务等应用系统的安全面临严峻的挑战。

传统密码学理论开发的加密系统——经典的密钥系统(如Data Encryption Standard,DES)受到威胁。从DES算法投入使用以来,人们一直在试图分析寻找它的弱点,其中差分分析法和线性分析法最具威胁。在DES使用20年后,最先对DES密码分析获得成功的却是一直不太被人们看好的穷举密钥攻击法。1997年初,美国著名的RSA数据安全公司为迫使美国政府放松对密码产品的出口限制,发起了"向密码挑战"的活动。其中挑战DES计划(DESCHALL),在Internet上数万名志愿者协助下,采用穷举密钥攻击法仅用了96天,在一台非常普通的奔腾PC上成功地找到密钥并破译出明文"强大的密码技术使世界变得更安全"。在随后的几年中,密码分析能力又有了重大进展,如美国EFF(Electronic Frontier Foundation)宣布他们以一台并不昂贵的专业解密机仅用56h就破译了DES;在公钥体制方面也破译了密钥为512b的RSA。

这一系列密码分析的成功,表明DES时代已经结束[1],同时也促使人们重新思考加密通信的安全性。