电子信息前沿技术丛书

Network Covert Communication and its Detection Technology

网络隐蔽通信及其检测技术

黄永峰 李松斌 编著
Huang Yongfeng Li Songbin

清華大學出版社

电子信息前沿
技术丛书

Network Covert Communication and its Detection Technology

网络隐蔽通信及其检测技术

黄永峰 李松斌 编著
Huang Yongfeng Li Songbin

清華大學出版社
北京

内 容 简 介

信息隐藏是一门新兴的信息安全技术，网络隐蔽通信技术是信息隐藏最近几年的研究新的分支方向。本书在总结多年科研成果基础上，从网络隐蔽通信及其检测两个方面系统地介绍了以网络流媒体为载体的信息隐藏理论模型、隐藏方法和检测技术等。全书分为上下两篇，上篇主要介绍网络隐蔽通信方法，分为4章；下篇主要介绍网络隐蔽通信的检测方法，分为6章。

本书是国际上第一本系统讲述以网络协议和流媒体为载体实现信息隐藏及其检测的著作。可供从事信息安全，特别是信息隐藏技术研究和开发的科技人员作为技术参考资料，也可供信息安全专业的本科生和研究生作为教学参考书。

图书在版编目(CIP)数据

网络隐蔽通信及其检测技术/黄永峰，李松斌编著. --北京：清华大学出版社，2016
电子信息前沿技术丛书
ISBN 978-7-302-42641-7

Ⅰ. ①网…　Ⅱ. ①黄…　②李…　Ⅲ. ①网络通信－通信技术－研究　Ⅳ. ①TN915

中国版本图书馆 CIP 数据核字(2016)第 017379 号

责任编辑：文　怡
封面设计：李召霞
责任校对：焦丽丽
责任印制：杨　艳

出版发行：清华大学出版社
网　　址：http://www.tup.com.cn，http://www.wqbook.com
地　　址：北京清华大学学研大厦 A 座　　邮　　编：100084
社 总 机：010-62770175　　邮　　购：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质量反馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
课件下载：http://www.tup.com.cn，010-62795954

印 刷 者：北京富博印刷有限公司
装 订 者：北京市密云县京文制本装订厂
经　　销：全国新华书店
开　　本：185mm×260mm　　**印　　张**：11　　**字　　数**：270 千字
版　　次：2016 年 3 月第 1 版　　**印　　次**：2016 年 3 月第 1 次印刷
印　　数：1～2000
定　　价：39.00 元

产品编号：066448-01

前言

FOREWORD

信息隐藏是21世纪初开始被关注的一门新兴的信息安全技术，是传统加密技术的有力补充。经过十多年的研究，信息隐藏技术得到飞速发展，并在相关领域得到应用。最初信息隐藏主要是以图像为隐藏载体，但近年来，随着互联网带宽的增长以及流媒体技术的发展，互联网流媒体应用已经深入影响社会生活的方方面面，并且已经成为互联网中最主要的网络流量。因此，信息隐藏也开始采用网络流媒体作为隐藏载体，因而出现了网络信息隐藏这一新的研究方向。

以网络流媒体为载体实现信息隐藏，具有其独特的优点。首先，网络流媒体数据的“海量”特点为信息隐藏提供了“天然隐蔽屏障”，也为流媒体隐蔽通信技术的实际应用奠定了基础。以互联网海量的流媒体为隐藏载体，发送者将秘密信息实时地隐藏其中进行传输；接收者实时提取秘密信息，且不保存流媒体载体信息。这样使得秘密信息的“存在性”得到了掩盖，极大地增强了网络隐蔽通信的隐蔽性，减少了被攻击的概率。因此，基于网络流媒体的隐蔽通信技术将具有巨大的应用前景和发展潜力。另外，流媒体载体特别适合于进行秘密信息的“动态、实时”隐藏，实现网络隐蔽通信应用。采用网络流媒体为载体实现隐蔽通信时，流媒体载体的产生和秘密信息的嵌入、提取都是“实时”完成的。攻击者在进行隐藏检测时，很难找到原始的流媒体载体。因此，攻击方只能进行信息隐藏的盲检测，检测难度非常大，这就在很大程度上提高了隐蔽通信过程的安全性。

正是基于上述理解与分析，从2005年开始，清华大学新一代网络技术与应用实验室率先开启了网络隐蔽通信的研究，并联合了中科院声学所、华中科技大学、华侨大学、中国地质大学、广州大学等单位相关研究人员，多年来一直致力于网络信息隐藏及其检测技术的研究。上述单位分别在网络协议隐藏与检测技术、网络语音流隐藏与检测技术、网络流媒体多维隐藏理论与隐藏方法等学术点上进行了深入研究和探索，取得了一些研究成果，但感觉很不够，进展还不够快。为了促进网络信息隐藏及其检测技术更广泛和更深入的应用，推动信息隐藏技术学科更快和更好发展，我们总结了研究团队在前期的研究成果和体会，撰写本书。参加本书编写的只有团队部分人员，但著作体现的成果应用来自团队所有人的共同贡献，具体包括清华大学袁键博士、肖博博士、陶怀舟博士等，广州大学李福芳副教授、中国地质大学杨婉霞博士、华侨大学周晖等，在此一同表示感谢。

全书的组织如下：第1章～第4章为本书的第一篇，即网络隐蔽通信技术部分。第1章首先对信息隐藏及网络隐蔽通信技术做了简要概述，第2章则系统阐述了网络隐蔽通信的分层模型，在后续的第3和第4章中给出了基于该分层模型，但分别以网络协议及语音流

媒体为载体时的隐蔽通信技术。第5章～第10章为本书的第二篇，即网络隐蔽通信检测技术部分。与静态媒体载体不同，流媒体可在网络协议以及语音载荷这两个不同的维度进行信息隐藏，其中在语音载荷维度的信息隐藏由于可与语音编码过程紧密结合，具有较高的隐蔽性，如何对其进行有效检测也是本部分的重点。具体而言，在第5章对隐蔽通信检测的相关背景知识进行简要概述后，在第6章讨论了压缩语音码流中量化索引调制隐蔽通信的检测方法，并在第7章中讨论了量化索引调制隐蔽通信的一种增强版本，即联合嵌入点的量化索引调制隐蔽通信的检测方法，第8章则介绍了另一种重要的压缩语音流媒体隐蔽通信方法：基音调制隐蔽通信的检测方法，随后在第9章阐述了低嵌入率条件下基于语音最低有效位替换的网络隐蔽通信的检测方法。最后，在第10章阐述了网络协议隐蔽通信的检测方法。

该著作应该是国际上第一部系统阐述网络隐蔽通信及其检测技术的专著，由于缺乏可供参考的相关专著的写作和组织经验，加之作者的水平有限，本书难免存在不足之处，欢迎指正！最后，作者要感谢国家自然科学基金委员会对本书相关研究的支持，本书先后得到了国家自然科学基金项目“基于机器学习的AbS-LPC压缩语音隐写分析研究”(No. 61303249)、“流媒体信息隐藏的时空概念模型及其应用方法的研究”(No. 61271392)、“基于网络文本语义的隐藏方法研究”、(No. 61472092)、“云数据安全审计模型与新方法”(No. 61405254)、“VoIP流媒体隐写的在线检测模型和方法研究”(No. 61402115)等资助。同时还要感谢清华大学出版社为本书的出版所提供的各项帮助！

作　者

2015年8月

目录

CONTENTS

第一篇　网络隐蔽通信技术

第一篇　网络隐蔽通信技术

第1章

信息隐藏技术概述

1.1 信息隐藏技术的发展

1.1.1 信息隐藏技术的起源

最早的信息隐藏技术案例可以追溯到大约公元前 440 年。据古希腊历史学家希罗多德记载，有位希腊贵族希斯泰乌斯为了安全地把秘密信息传送给米利都的阿里斯塔格鲁斯，他想出一个奇妙的方法，剃光送信奴隶的头发，将密信写在头顶上，等送信奴隶的头发长出来以后，写在头皮的消息被头发隐藏起来，当奴隶到达米利都后，又将头发剃去，从而将消息安全地传递给接收方[1]。另外，在波斯朝廷的一个希腊人 Demeratus，他要警告斯巴达，波斯准备对斯巴达(Sparta)发动一次突袭，便利用一层蜡把木板上的字遮盖住，并送给斯巴达波斯的同谋，从而逃过了海关士兵的检查，把消息成功地送到了斯巴达克[2]。类似地，在古代，出于当时的技术条件和战争需要，将信函隐藏在信使的鞋底，衣服的褶皱，妇女的头饰和首饰中等[3]，这些都是早期信息隐藏技术的雏形[4]。

在两次世界大战中，德国间谍在一篇信函中使用一些特殊字母记载秘密信息。方法是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。中国古代设计的信息隐藏方法中，发送者和接收者各持一张完全相同的、带有随机选定许多小孔的纸。发送者将带有孔的纸覆盖在一张纸上，将秘密消息写在小孔的位置，然后移去上面的纸，根据下面纸上留下的字和空余位置，编写一段普通的文章。接收者只要把带孔的纸覆盖在这张普通的文字上，就可以读出留在小孔中的秘密信息。在 16 世纪早期，意大利数学家 Cardan(1501—1576 年)也发明了这种方法，现在称其为卡登格子法[4]。

在 1860 年，法国摄影师 Dragon 发明了制作微小图像技术，能将很多消息存放在微缩胶片中，实现了 Brewster 将秘密消息隐藏在“大小不超过一个句号或小墨点的空间里”的构想。例如，在 1870—1871 年弗朗格-普鲁士战争期间，巴黎被围困，消息隐藏在微缩胶片中

通过鸽子传递出去。

信息隐藏技术很早就在我国的魔术中也得到应用。例如，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就显出棕色字体。与之对抗的技术就是人们后来研究出的“万用显影剂”[4]，该技术使得不可见墨水的隐写方法无效。“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”的作用下都无效了。

另外，人们还可以通过一些绘画作品或者音乐作品来实现信息隐藏。如图 1-1 所示，隐藏着一封密信的圣安东尼奥河面，沿河岸的短草叶代表莫尔斯电码的点，长草叶代表划，拼出的文字是“Compliments of CPSA MA to our chief Col Harold R. Shaw visit to San Antonio May 11th 1945”。在“二战”期间，一位女钢琴家，也是德国忠实的女间谍，把从联军那里获得的情报，按照事先规定的密码巧妙地将其编成乐谱，如图 1-2 所示，在电台演奏时一次次公开将情报通过悠扬的琴声传播出去[4]。

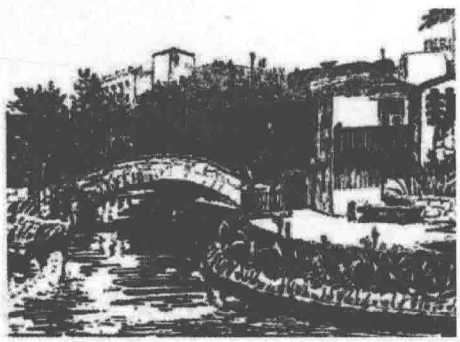

图 1-1 圣安东尼奥河面

图 1-2 乐谱图

中国古代还采用藏头诗来实现信息隐藏[6]。例如，中国古典名著《水浒传》第六十一回——“吴用智赚玉麒麟，张顺夜闹金沙渡”中有一首诗：

芦花丛中一扁舟，
俊杰俄从此地游。
义士若能知此理，
反躬逃难可无忧。

其中前面四个字连起来读，正是“芦俊义反”。

再比如有一年中秋节，绍兴才子徐文长在西湖赏月时，做了一首七言绝句：

平湖一色万顷秋，
湖水渺渺水长流。
秋月圆圆世间少，
月好四时最宜秋。

其中前面四个字连起来读，正是“平湖秋月”。

到 16 世纪和 17 世纪，已经出现了大量关于信息隐藏（也称为隐写术）的文献，如 Trithemius 的专著 *Polygraphia* 和 Gaspari Schotti 的专著 *Steganographica*，堪称密码学

和信息隐藏技术最早出现的两本专著，书中使用新颖的信息编码手段实现了很多算法，例如用特定的词或短语来替代字母，用乐谱中的音符来对应字母，或是用点、线或者三角来将一个秘密消息隐藏到一个几何图形中。

1.1.2 现代信息隐藏技术的发展

计算机技术、互联网及数字多媒体的发展为信息隐藏技术提供了新的发展空间和技术手段。国际上正式提出现代信息隐藏技术的研究是在 1992 年，1996 年 5 月 30 日～6 月 1 日，在英国剑桥大学召开了第一届国际信息隐藏学术研讨会(The First International Workshop on Information Hiding，IHW1996)，这标志着“信息隐藏学”的正式诞生。在国内，何德全、周仲义和蔡吉人三位院士于 1999 年在北京联合号召发起了第一届全国信息隐藏学术会议，这标志着我国信息隐藏技术研究正式开始。至 2015 年 3 月，全国信息隐藏学术会议已经召开十二届，期间还召开了许多次专门学术交流会。信息隐藏技术发展至今，已涉及多个学科，如密码学、信息处理技术、计算机技术、网络技术、生理和心理学等，信息与网络的安全需求不断提升。经过十多年的发展以及数字技术的发展，信息隐藏被赋予了新的含义，人们开始研究如何在数字数据中隐藏信息。同时，各种现代化的理论和数学工具也被用于信息隐藏中，慢慢形成和丰富了信息隐藏自身的理论基础信息和理论资源，多媒体数据压缩编码与扩频通信技术的发展为信息隐藏提供了必要的技术基础。信息隐藏技术已经成为信息安全领域中的一个研究热点，它在保护网络信息安全领域起到重要作用。它在工业界、商业界和军事界都具有广阔的应用前景。

1.2 信息隐藏技术的概念

信息隐藏最早的描述模型是 Simmons 提出的囚徒问题(The Prisoners' Problem)[7]。囚徒问题模型可以简单表述为：Alice 和 Bob 是狱友，他们想谋划一个越狱计划，但是他们的计划和行为又不能被监视他们的典狱官 Wendy 发现，以此为背景可以描述信息隐藏的一般框架，如图 1-3 所示。发送方 Alice 试图发送一个秘密信息 M 给接收方 Bob，为此，她将采用某种嵌入算法将秘密信息隐藏于一个载体信息(Cover-object)中得到载密对象(Stego-object)，并将其通过公共信道传递给 Bob；Bob 根据事先约定的密钥(Stego-key)可以完整地提取载密对象中秘密信息；攻击者 Wendy 即使有条件获取载密对象，也不能判断其中是否携带有秘密信息，从而基于信息隐藏的隐蔽通信得以进行。该模型表明了信息隐藏的目的不仅是保护秘密信息内容的安全，更为重要的是掩盖隐蔽通信的存在性。

对于上述的囚犯问题模型可以抽象为如下过程：甲打算秘密传递一些信息给乙，甲需随机选取一个看似平常的消息 R，当 R 消息公开在网络中传递时，不会引起任何怀疑，称消息 R 为载体对象。然后把需要秘密传递的信息 m 隐藏到载体 R 中，隐藏过程有时需使用嵌入密钥控制，此时，载体对象 R 形成带有消息的隐秘对象 S。当秘密信息 m 嵌入到载体对象 R 中后，要求隐秘对象 S 尽可能地保持原有载体 R 的特征不变，使得任何攻击者在仅知道表面无关紧要的消息 R 时，无法检测到秘密消息 m 的存在。这样，就实现了信息的隐蔽传输，即掩盖了秘密信息传输的事实，实现了信息的安全传递。在接收方接收到隐藏载体 S

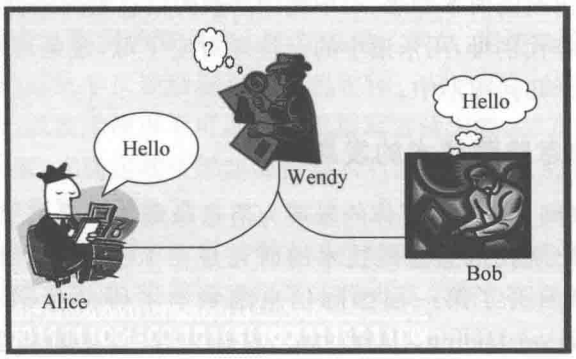

图 1-3 信息隐藏的囚犯问题模型

之前，隐藏载体 S 可能受到各种有意或者无意的攻击，由于接收方已知发送方的嵌入算法，接收方利用相应的提取算法从受到攻击后的载体中提取消息 m，或者判断接收到的载体中是否含有隐藏消息。秘密信息的嵌入过程，可能需要密钥，为了区别于加密的密钥，信息隐藏的密钥称为伪装密钥。因此，信息隐藏的原理如图 1-4 所示。

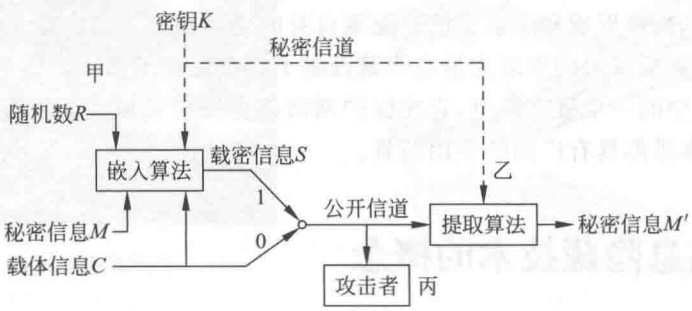

图 1-4 信息隐藏原理图

结合囚犯问题和上述模型的分析，信息隐藏(information hiding)的概念可以定义为将秘密信息隐藏于另一公开的隐藏载体之中。隐藏载体可为任何一种数字媒体，如图像、音频、视频、文本、网络协议或流媒体，也可以是信道，甚至是某种编码或整个通信过程。

之所以能够将信息隐藏在多媒体数据中，主要原因有两个：第一，从信息论的角度看，将这些秘密信息嵌入到冗余的多媒体信息编码过程中传送是完全可行的，且不会影响到多媒体信息本身的传送和使用。第二，可以充分利用人类的听觉和视觉系统的掩蔽性将信息隐藏而不被察觉。

信息隐藏和传统的信息加密的主要区别体现为：加密码技术主要是研究如何把要传递信息进行特殊编码，形成不可识别的秘文进行传输；而信息隐藏主要是研究如何利用载体的冗余将秘密信息隐藏于另一公开的载体中，成为载体不可分离的一部分，然后通过公开载体的传输来传递秘密信息。对于加密通信，攻击者可截取密文，并破译密文，或将密文进行破坏后再发送，从而影响秘密信息的安全；但对信息隐藏，监测者要从公开载体中判断是否存在秘密信息是较困难的，截获秘密信息则更困难，从而保证了秘密信息的安全。在实际应用中，一般会把加密技术和信息隐藏技术结合，即先加密嵌入对象得到密文，再把密文隐藏到载体对象中以增加破译的难度。因此，密文加密技术仅仅隐藏了信息的内容，而信息隐藏

技术既隐藏了信息的内容又隐藏了秘密信息的存在。而且传统的以密码学为核心技术的信息安全和信息隐藏技术不是互相矛盾和竞争的技术，而是一种互补技术。

1.3　信息隐藏技术的特点

经过十几年的研究和发展，信息隐藏技术在许多领域得到了应用，而且不同的应用领域具有不同的特点。下面重点分析信息隐藏技术在隐蔽信息通信应用领域所具有的特点。

(1) 鲁棒性(robustness)。指隐藏秘密信息必须能在隐藏载体进行变换操作情况下不会发生破坏。在载体产生失真的情况下，隐藏信息仍然能保持一定的完整性，并能以一定的正确概率被检测到。也就是说，常用的信号处理操作不应该引起隐藏信息的丢失，保持原有隐藏信息的完整性和可靠性。对隐藏载体的变换操作一般包括数/模、模/数转换；再取样、再量化和低通滤波；剪切、位移；对图像进行有损压缩编码，如变换编码、矢量量化；对音频信号的低频放大，等等。

(2) 安全性(security)。指隐藏算法必须能够承受一定程度的人为攻击，而使隐藏的信息在人为攻击下不被破坏。理想情况是对手不能检测到载体中是否包含隐藏信息。信息隐藏技术与信息加密一样，要把对信息的保护转化为对密钥的保护。因此，在设计一个信息隐藏系统时，密钥的产生、发放、管理等也必须安全，这是需要综合考虑的因素。

(3) 不可检测性(undetectability)。指隐藏载体与载体信息在统计特征上的一致性，使得非法护截者要检测到隐藏信息的存在并提取是相当困难的。例如，如果隐藏载体和隐藏信息具有一致的噪声统计分布，这就使得隐写分析者无法判断隐藏对象中是否隐藏信息。

(4) 透明性(invisibility)。也称为不可感知性(imperceptibility)，指载体在隐藏信息后不应使得载体发生可感知的改变，也不能使得载体在质量上发生可以感觉到的失真，更不能破坏载体的使用价值。因此，如果不使用特殊检查手段，就无法感知隐藏信息的存在。

(5) 隐藏容量。载体中能够容纳的隐藏信息位的最大值，它是指在隐藏秘密信息后仍满足不可感知性的前提下，数字载体中可以隐藏秘密信息的最大比特数。

在一般情况下，我们将面向隐蔽通信应用中的信息隐藏的主要特性归纳为三个方面，分别是鲁棒性、隐藏容量和隐蔽性。其中隐蔽性就包含前面所说的安全性、透明性和不可检测性。而且，隐蔽通信的这三方面特性之间体现“三角关系”。例如，隐藏容量与系统要达到的隐蔽性、鲁棒性等因素有关，在满足隐蔽性的条件下，隐藏的信息越多，鲁棒性就越差。同样，在满足鲁棒性的条件下，隐藏的信息越多，隐蔽性就越差。因此，在具体的隐藏系统中通常都会涉及隐蔽性、鲁棒性和隐藏容量三者之间的平衡。

1.4　信息隐藏技术的主要分支

按信息隐藏技术的应用目的和载体对象不同，信息隐藏可分为许多分支，如图 1-5 所示。下面对几个主要分支做简单介绍[4]。