信息隐藏技术及其应用

刘振华　尹　萍　编著

科学出版社

国家自然科学基金项目资助
国家重点基础研究规划项目资助

信息隐藏技术及其应用

刘振华　尹　萍　编著

科学出版社
2002

内 容 简 介

信息隐藏是一门新兴的学科，是与密码术、多媒体、计算机网络紧密相关的交叉学科，它通过将秘密消息隐藏在其他消息之中达到隐匿消息存在的目的，其在版权保护、保密通信等领域都具有广泛的应用价值。本书系统地阐述了信息隐藏的基本概念、主要技术、攻击方法和信息隐藏的应用，同时介绍了近年来国内外研究人员在这一领域的主要成果。

全书共分七章。第一章简要介绍了信息隐藏技术的发展、术语、主要原理及存在的局限性，其余各章分别对信息隐藏技术在隐写术、数字水印、数字指纹、计算机系统中的隐通道、密码术中的阈下通道、低截获概率通信、广播加密、匿名服务等方面应用的主要技术和攻击方法做了详尽的说明。

本书可作为信息安全、密码学等相关专业的大学高年级学生或研究生的教学用书，也可供以上领域的研究工作者参考。

图书在版编目(CIP)数据

信息隐藏技术及其应用/刘振华，尹萍编著. —北京：科学出版社，2002
ISBN 7-03-010084-0

Ⅰ.信… Ⅱ.刘… Ⅲ.信息处理-安全技术 Ⅳ.G202

中国版本图书馆 CIP 数据核字(2002)第 002646 号

科学出版社 出版
北京东黄城根北街16号
邮政编码:100717
http://www.sciencep.com
双青印刷厂 印刷
科学出版社发行 各地新华书店经销
*
2002 年 2 月第 一 版 开本:850×1168 1/32
2002 年 2 月第一次印刷 印张: 8
印数:1—4 000 字数:190 000
定价:15.00 元
(如有印装质量问题，我社负责调换〈路通〉)

序

今天，人们特别关注消息(Message)的信息(Information)属性。

看到一条消息，读不懂，人们就会认为它经过了有意变形，从而进一步推断这条消息的重要性，并对之采用各种信息分析手段来揭示该消息所携带的信息。密码术是利用随机性而使消息具备信息机密性(Confidentiality)的有效方法，密码术在与密码分析的对抗中不断进步，密码术的正确使用可以较好地保证消息的信息内涵不被非法获取。

在信息安全研究中还定义了信息的完整性(Integrity)。具备信息完整性的消息在传递、存储过程中，既不容易出错，又不容易被篡改。信息安全技术中利用加密和冗余来赋予消息的信息完整性属性。

具备信息机密性或信息完整性的消息，往往带有随机的数据特征，从而明显地暴露了消息的重要性，从信息安全观点看来这是个严重的缺憾。在网络空间中，在消息的汪洋大海中，别具一格、招摇过市、公然宣称自己的重要性总不是信息安全的初衷。

一条消息，利用随机和冗余技术还可使其具备信息的隐形性(Invisibility)。具备信息隐形性的消息一般都具备显含的、明确的甚至是自然的可接受信息(例如，中国北京申办2008年奥运会成功的图片)，发一条杂乱无章的消息可看成是不可接受的消息，或者是值得推敲的消息。具备信息隐形性的消息总是携带着隐含信息，这与一般的加密变形不同，它在传递和存储过程中，在消息的汪洋大海中不显山不露水、自然合理，往往不被人注意。

人的隐藏手段一向十分高明，由于计算机、网络和多媒体技术的发展，信息隐藏(Information Hiding)技术近10年来有了长足的

进步，古老的隐写术（Steganography）也发展到现代隐写术（Modern Steganography）。

刘振华教授近年来从事信息隐形性方面的研究，承担了国家自然科学基金项目和国家重点基础研究规划项目（973）的相关课题，带领研究生们在数字水印和隐蔽加密通信方面作了不少有益的工作。读刘振华教授等编著的《信息隐藏技术及其应用》一书可以了解信息隐藏技术各个侧面的进步和发展。本书为信息隐形性研究打下了一个坚实的基础。

吕述望

中国科学院研究生院信息安全国家重点实验室

2001 年 7 月 13 日

前　言

信息主要有两种基本保护方法：一种是利用密码术对明文实施各种变化，使它不为局外人所理解。这种利用随机性来对抗密码攻击的技术，在防止他人从中得到信息具体内容的同时，也暴露了消息的重要性，因此，成为攻击者注意的焦点，在实际应用中，这一点常常是需要极力避免的。另一种方法就是信息隐藏技术，利用载体信息中具有随机特性的冗余部分，将重要信息嵌入载体信息之中，使其不被其他人发现。在实际应用中，存在冗余信息的载体非常丰富，这一点也在客观上增强了信息隐藏技术的隐蔽性和可行性。这种通过把信息存在本身隐藏起来的技术使得攻击者无从获取秘密信息的位置，从而增强了安全性。

近年来，出于对数字作品版权保护和个人隐私保护等方面的需求，掀起了信息隐藏技术研究的热潮。许多大学、研究机构和公司已经纷纷开展了这方面的研究，并召开了专门的国际学术研讨会进行定期交流。在有关密码学和信息安全的国际会议和刊物上经常可以见到相关领域的论文和报告，许多公司也推出了相关的产品和技术服务。

我国在信息隐藏方面的研究起步稍晚，但已引起了信息安全领域研究人员的普遍关注，作者所在的信息安全国家重点实验室就是较早进行信息隐藏研究的单位之一。在广泛吸取国内外信息隐藏研究成果的基础上，我们编写了本书，希望能够促进信息隐藏技术研究的进一步开展。

信息隐藏技术的应用非常广泛。隐写术、数字水印、计算机系统中的隐通道、密码协议中的阈下通道、低截获概率通信等技术在保护数字作品版权和个人隐私方面都发挥着重要作用。另外，广播加密、匿名选举、数字现金等应用中也使用了信息隐藏技术。本

书力求对有关重要应用做出详尽的介绍。

作者的研究工作得到国家自然科学基金(项目编号:69873041)和国家重点基础研究发展规划项目(973,项目编号:G1999035805)以及信息安全国家重点实验室创新基金的资助,在此向提供支持的国家自然科学基金委员会和国家科技部表示感谢;作者所在的信息安全国家重点实验室良好的研究氛围为本书的写作创造了有利的条件;特别感谢吕述望教授对本书给予的关注和建议,与他的讨论使作者受益匪浅;还要感谢实验室的老师和同学们以及科学出版社的帮助和协作,使得本书得以顺利出版。

信息隐藏作为一门交叉性的学科,所涉及的应用非常广泛,相关研究的发展也非常迅速,由于作者学识有限,出版时间紧张,书中的错误与不足在所难免,如蒙指正不胜感激。

刘振华

目　录

第一章　信息隐藏概论

在现实生活中，人们对于信息的保密往往是求助于密码术，而计算机软硬件技术的发展使得密码破译能力越来越强，这迫使人们对加密算法的强度提出越来越高的要求。在许多领域，密码术的应用已经越来越显现出它的局限性。由于密码术是利用随机性来对抗密码攻击的，而密文的随机性同时也暴露了消息的重要性，即使密码的强度足以使得攻击者无法破解出明文，但攻击者有足够的手段来对其进行破坏，从而使得消息无法被接收。密文容易引起攻击者注意是密码术的一个显著弱点。因此，对于某些应用来说，仅仅对信息的内容加以保密是不够的，本书将介绍信息的另一种保密方式，即对信息存在本身或信息存在位置的保密——信息隐藏。

1.1　研究内容

在许多应用领域中，人们常常希望将秘密信息隐藏在某些对象中，或者防止别人通过这种方式秘密传递信息。其中比较有代表性的例子有出于某种利益的隐蔽通信，保护作者合法权益的版权标记，以及军事上所需的低截获概率通信等。对隐写术、数字水印、操作系统中隐通道、密码协议中阈下通道以及低截获概率通信等技术手段的研究能够在一定程度上从理论上和工程上满足人们的需求，这些都是信息隐藏所研究的内容。

隐写术（Steganography）是信息隐藏技术的一个重要分支，它的历史非常悠久，并且可以在很多领域得到应用。情报人员利用隐写墨水在报纸上写信或在磁带的特定位置加入次声波回声等方法来传递秘密信息，这就是隐写术应用的一个典型实例。在计

算机领域应用隐写术的基本原理是利用信息中普遍存在的冗余性向其中嵌入秘密信息，从而达到隐蔽重要信息存在的目的。举例来说，由于人眼的分辨率是有限的，对于一幅 8 比特/象素(Bit/Pixel) 的灰度图像，最低两位的随机变化并不会在视觉上造成差异，这样，就可以利用隐写术将秘密消息隐藏在图像之中。同样，视频、音频等媒体中也都含有大量信息冗余，可以为隐写术的使用提供条件。利用隐写技术将加密后的信息隐藏在无关紧要的信息中保存起来或发送出去，可以避免引起其他人的注意，是一种更为安全有效的信息保密方式。

近年来，由于计算机网络和多媒体技术的迅速发展，越来越多的文学和艺术工作者使用计算机进行创作，同时，大批网络创作者也应运而生，他们的共同特点是将作品以数字形式进行存储和传输。然而，数字作品的便利性与不安全性是并存的，它可以低成本、高速度地被复制和传播，为创作者和使用者都提供了有利条件，但这些特性也容易被盗版者所利用，因而，采取多种手段对数字作品进行保护、对侵权者进行惩罚已经成为迫在眉睫的工作。除了与传统作品版权保护相类似的法律和管理手段外，还应该针对数字作品的特点为其提供技术上的保护。向数字作品中加入不易察觉但可以鉴别的版权标记是进行数字作品版权保护的一种有效技术手段，这种技术被称为版权标记技术。

版权标记技术中的标记可以是一个商标、一个序列号、或是一种防止未授权用户直接拷贝的方法等。根据标记内容和所采用技术的不同可以将版权标记技术分为数字水印技术和数字指纹技术。数字水印技术是向数字作品中嵌入版权信息，从而达到确定所有者身份，识别侵权者的目的；数字指纹则是向为不同用户分发的数字拷贝中分别嵌入不同的序列号，使得版权所有者在发现非法再分发时能够确定是哪些用户违背了许可协议。版权标记能够保护几乎所有的数字产品，包括音频、视频、图像、图形、文本、软件等。因此，版权标记技术引起了音乐、电影、书籍出版者的广泛关注，成为目前信息隐藏研究的热点问题之一。

在长期的使用过程中人们发现，计算机系统中存在的安全漏洞也可以被用来秘密传输信息，这一技术被称为计算机系统中的隐通道技术，也是信息隐藏研究人员所关注的问题之一。计算机系统的进程通信中有大量的数据流存在，在对可信计算机平台的评估中，无论是存储隐通道还是时域隐通道，人们发现隐通道是不可能完全阻断的。现代计算机系统带宽越来越大，遗憾的是，要保证安全，就不可避免地要降低系统的带宽，人们必须折中考虑降低带宽对系统性能的影响。现在，人们通过使用特定的分析工具检测出系统中存在的隐通道，从而可以减少系统的安全漏洞。

在信息安全领域内，数学家创造性地利用各种数学结构来进行各种编码体制、密码协议的设计，但是这些数学结构也会被高手用来攻击密码算法和发现密码协议的缺陷，其中阈下通道就是攻击者研究的重点所在。自 1978 年人们发现苏美 SALT II 条约监督协议中存在着阈下通道以来，阈下通道就成为密码协议研究的一个重要选题，人们发现，数字签名协议在使用随机数来增强抗攻击能力的同时，也恰恰造出了可以被用来传输秘密消息的阈下通道。这样，阈下通道也可以成为进行信息隐藏的工具之一。

现代战争中，截获与反截获是机要通信战线上的重要斗争之一，低截获概率通信的研究已经越来越引起各国政府和军队的重视，成为现代通信的重大课题。20 世纪 50 年代中期开始研究的扩频通信技术就是一种无线低截获概率通信。它将待传送的信息数据进行伪随机编码调制，实现频谱扩展后再传输，接收端则采用同样的编码进行解调获取信息。扩频通信把原本集中于较窄频段的待传送信息展宽到较宽频带，并可以在很低的信噪比下传送信息。因此，在不知道伪随机编码的情况下，截获低功率谱密度的扩频通信信息将是一件很困难的事情。流星猝发通信则是利用微流星体电离轨迹进入地球的大气层会反射无线电波这一现象来建立远程通信连接。由于流星轨迹会迅速散射，因而信号强度也会快速衰减，流星猝发通信的这一间歇特性以及每一条轨迹相对

较小的覆盖区域，使得它们本质上难于被监视，可以用于低截获概率通信。

另外，在广播加密和匿名服务等领域也有信息隐藏技术的重要应用，本书的第二章到第七章将分别对信息隐藏各个应用分支的研究做更加详细的介绍。

1.2 基本概念

20 世纪 90 年代前期，信息隐藏的各种应用引起不同研究团体的关注和重视。最初，这些研究团体各自进行着他们的研究工作，也各自使用不同的术语。1996 年 5 月信息隐藏第一次国际学术研讨会的召开使这些独立的研究团体走到了一起，在这次会议上，人们对信息隐藏应用中的一些共同术语达成共识，本书借鉴了其中的大部分模型和术语。

1.2.1 术语

顾名思义，信息隐藏就是将保密信息隐藏于另一非保密载体中，以不引起检查者的注意。我们通常将希望被秘密保存的信息称为**嵌入对象**，将用于隐蔽嵌入对象的非保密载体称为**掩体对象**。嵌入对象通过嵌入过程被隐藏在称为掩体对象的非保密信息中，从而生成**隐藏对象**。掩体对象可以是掩体文本、掩体图像或掩体音频等，对应的隐藏对象也可以是隐藏文本、隐藏图像或隐藏音频等。将嵌入对象添加到掩体对象中得到隐藏对象的过程被称为**信息的嵌入**，嵌入过程中所使用的算法称为**嵌入算法**。信息嵌入的逆过程，即从隐藏对象中重新获得嵌入对象的过程称为**信息的提取**，也可称为信息的恢复。在提取过程中所使用的算法称为**提取算法**。执行嵌入过程和提取过程的组织或个人分别被称为**嵌入者**和**提取者**。

在嵌入和提取过程中通常会使用一个秘密信息来对其进行控制，使得只有它的持有者才能对其进行操作，这个秘密信息被称

为**隐藏密钥**，隐藏密钥在嵌入过程中被称为**嵌入密钥**，在提取过程中被称为**提取密钥**。通常情况下，嵌入密钥和提取密钥是相同的，这样的信息隐藏技术被称为**对称信息隐藏技术**；反之，若嵌入密钥与提取密钥不相同，则被称为非对称信息隐藏技术。

与密码术类似，我们可以将信息隐藏的研究分为**隐藏技术**和**隐藏分析技术**两部分。隐藏技术研究的主要内容是寻求向掩体对象中秘密添加嵌入信息的方法，而隐藏分析技术研究的主要内容则是考虑如何从隐藏对象中破解出嵌入信息，或通过对隐藏对象的处理达到破坏嵌入信息和阻止信息检测的目的。我们将隐藏技术的研究者称为**隐藏者**，将隐藏分析技术的研究者称为**隐藏分析者**。

1.2.1.1 隐写术

“隐写术”一词源于希腊词语“$\sigma\tau\varepsilon\gamma\alpha\nu\omega$”，其字面意思是**“掩饰性地写”**，通常被解释为将秘密信息隐藏在其他信息中。信息隐藏的基本概念可以直接引入隐写系统中，即将嵌入对象隐藏在掩体对象中，生成隐写对象，相应的密钥称为隐写密钥。不难看出，隐写术的主要目的在于将重要的信息隐蔽起来，以便不引人注意地传输或存储。因此，在一个隐写系统中，嵌入对象是主体，而掩体对象则可以是任何能够达到隐蔽传输目的的载体数据。通常情况下，选择掩体对象时需要考虑隐写容量的大小和隐写结果的不引人注意性这两方面因素。在实际应用中，通常可以精心设计一个掩体对象来隐藏嵌入对象，甚至还可以根据嵌入对象直接构造隐写对象，这样可以提高隐写容量，达到高效隐写的目的，但同时还应该考虑所生成的隐写对象应不引人注意这一原则。

在隐写信道中存在的隐藏分析者常常被称为**“看守者”**，这是因为人们一般将 Simmons 提出的“囚犯问题”作为隐写系统的通用模型。根据看守者能否对流经他的信息流进行改动和处理，还可以将隐写系统中的看守者分为**“被动看守者”**和**“主动**