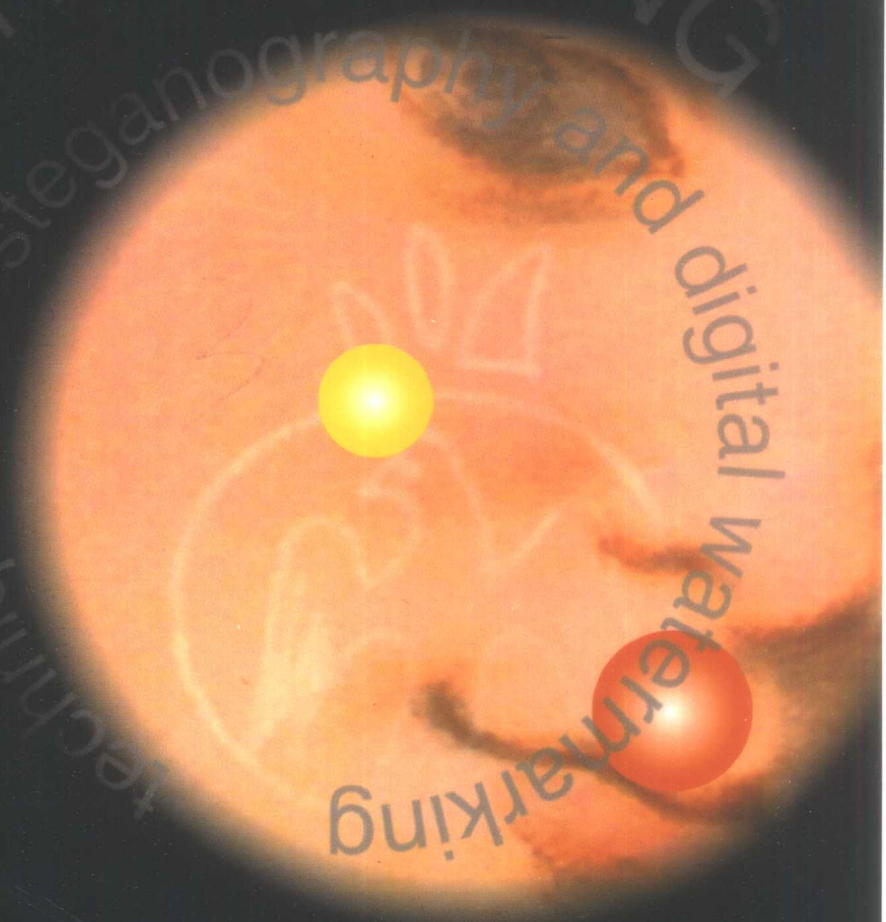
国瑞数码安全系列丛书

# 信息隐藏技术
## —隐写术与数字水印

Stefan Katzenbeisser
Fabien A.P. Petitcolas 编
吴秋新 钮心忻
杨义先 罗守山 杨晓兵 译

INFORMATION HIDING
techniques for steganography and digital watermarking



人民邮电出版社
www.pptph.com.cn

国瑞数码安全系列丛书

# 信息隐藏技术
# ——隐写术与数字水印

Stefan Katzenbeisser Fabien A.P. Petitcolas 编
吴秋新 钮心忻 杨义先 罗守山 杨晓兵 译

人民邮电出版社

**图书在版编目(CIP)数据**

信息隐藏技术——隐写术与数字水印/(英)卡曾贝塞(Katzenbeisser,S.),(英)佩蒂科勒斯(Petitcolas,F.A.P.)编;吴秋新等译.—北京:人民邮电出版社,2001.9

(国瑞数码安全系列丛书)

ISBN 7-115-09550-7

Ⅰ.信... Ⅱ.①卡...②佩...③吴... Ⅲ.数据通信-安全技术 Ⅳ.TN919

中国版本图书馆 CIP 数据核字(2001)第 049895 号

## 内 容 提 要

本书详细介绍了涉及数据通信安全的信息隐藏技术,以及用于数字产品知识产权保护的水印技术。除技术本身外,该书还涉及它们的历史、相互的差异、隐蔽通信的破译、水印的删除,以及数字水印和版权问题的法律意义。

本书适合关心网络通信安全和知识产权的读者,他们包括从事网络通信安全和水印制作的工程技术人员、管理人员、法律工作者、学者,也包括从事隐密通信和反盗版的情报人员、技术人员。

国瑞数码安全系列丛书

**信息隐藏技术——隐写术与数字水印**

◆ 编 Stefan Katzenbeisser Fabien A.P.Petitcolas

译 吴秋新 钮心忻 杨义先 罗守山 杨晓兵

责任编辑 陈万寿

◆ 人民邮电出版社出版发行 北京市崇文区夕照寺街 14 号

邮编 100061 电子函件 315@ pptph.com.cn

网址 http://www.pptph.com.cn

读者热线 010-67129212 010-67129211(传真)

北京汉魂图文设计有限公司制作

北京顺义振华印刷厂印刷

新华书店总店北京发行所经销

◆ 开本:787×1092 1/16

印张:11

字数:254 2001 年 9 月第 1 版

印数:1-4 000 册 2001 年 9 月北京第 1 次印刷

著作权合同登记 图字:01-2001-1103 号

ISBN 7-115-09550-7/TN·1755

定价:20.00 元

# 版 权 声 明



本书原版书名 Information Hiding Techniques for Steganography and Digital Watermarking

作者 Stefan Katzenbeisser, Fabien A. P. Petitcolas, editors

# 作 者 简 介

Stefan Katzenbeisser 是维也纳技术大学计算机科学系的一名学生。

Fabien A.P. Petitcolas 从英国剑桥大学获得博士学位，现受聘于微软剑桥研究院。

# 译者的话

网络信息安全保障迫在眉睫。现在世界上每年因利用计算机网络进行犯罪所造成的直接经济损失令人吃惊。利用计算机通过互联网络窃取机密信息的事例也是屡见不鲜。网络信息安全隐患,将全方位地危及社会的经济、政治、文化等各个方面。

当前,我国社会信息化正以一日千里的速度前进,对网络与信息安全的需求日益增大。与其他领域不同,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来解决信息安全问题无异于引狼入室。为此,国家已经明确规定:"信息安全产品一定要立足国内,自主开发"。

当前国内在网络与信息安全方面的基础(人员和技术)还相当薄弱,急需加强。"在游泳中学游泳",将国际上最新出版的一些著作以翻译的形式介绍给广大读者,是使国内同行更好更快地了解国际上在信息网络安全方面的最新进展的最佳途径之一。为了取得更好的效果,人民邮电出版社与北京邮电大学信息安全中心和天津市国瑞数码安全系统有限公司共同合作翻译出版了这套"国瑞数码安全系列丛书"。希望本系列丛书能够为促进我国的网络信息安全做出一定的贡献。

天津市国瑞数码安全系统有限公司(http://www.ncs-cyber.com.cn)是一家以网络安全和信息安全为主的高科技企业,公司致力于为我国社会信息化提供全方位的网络安全和信息安全保障。公司拥有一大批国内一流的密码学和信息网络安全专家,硕士、博士学位获得者超过公司员工总数的一半,公司真诚地欢迎更多的有志于我国数码安全的专家加盟(联系电话:010-62383780、022-27237081)。公司已经开发出具有完全自主知识产权的众多信息与网络安全产品。比如:B2B 电子商务安全平台、电子商务加速卡、网站卫士、安全替音电话、WAP 安全解决方案、宽频系统安全结构和多种加密卡和加密算法等。

北京邮电大学信息安全中心(http:\\www.bupt.edu.cn)是一个历史悠久的部级重点实验室,是国务院学位委员会正式批准的全国仅有的三个"密码学"博士点之一,长期致力于网络信息安全的理论和关键技术研究。欢迎有志青年来此攻读硕士、博士和博士后。

本丛书还得到了国家高等学校骨干教师资助计划项目(国家教育部)、国家重点基础研究发展规划项目(编号:G1999035805)、国家杰出青年基金项目(批准号:69425001)和国家自然科学基金项目(批准号:69882002,60073049)的资助。特此致谢。

北京邮电大学信息安全中心的研究生陈亚娟、王自亮、张振涛、张小芬等也参加了本书的部分翻译工作,特此致谢。

# 序

## (Ross J. Anderson)

每隔几年,计算机安全领域必定会有新的发展和突破,新的技术和新的应用也会给网络安全带来新的威胁,从而迫使我们发明新的安全保护机制。当商业领域开始建立网络化的计算机系统时,密码学就立即变得重要起来;当大量 PC 用户要相互交换信息时,计算机病毒就开始流行起来;当因特网发展起来以后,防火墙技术则迅速发展起来。

信息安全研究领域最新热点之一是信息隐藏研究,其驱动力在于信息时代的两大政策问题——版权保护和状态监视。

数字音乐和视频作品极容易被完美复制这一特性使娱乐界非常不安,因为盗版这种数字作品要比模拟家用录音带的盗版频繁得多,而且容易得多。MP3 编码的音乐不断流行起来更加剧了这种恐惧。这些问题的部分解决方案可以是改变音乐和视频作品的销售方式,然而,软件工业很大程度上放弃了版权控制机制,而选择这样一种商业模式,即频繁升级、在线注册以获得技术支持、对大规模盗版进行起诉以及对从商业应用到游戏的每一种软件产品都网络化。但对数字音乐和视频产品,人们希望技术保护机制也将能提供部分解决方案。其中的一种保护机制就是版权标记——将版权标识和序列号隐藏在音频或视频中,并使得盗版者难以消去它们。

因特网的迅猛发展也对国家情报和公安机关产生了巨大影响。他们宣称,随处可得的加密软件可能使搭线监听越来越困难,他们通常的反应是尽力限制加密算法的强度,或者要求拷贝备用的密钥以使他们需要时能即时获得。这激起了人权自由崇尚者的义愤,并谴责这是对个人隐私不可忍受的侵犯。这两种观点从某种程度来讲都过于单纯了一点。绝大多数维护安全的通信侦察并不是与搭线监听有关,而主要是与追踪双方联络的网络有关,并且最典型的犯罪通信工具是预付款的移动电话。在这两种情形中,问题不在于通信的保密性,而是他们的可追踪性。通过使用为版权标识开发的技术,通信也能被隐藏起来,并且它们能帮助犯罪分子逃脱使用"非法"密码系统的法律制裁。

正如对于版权保护和赞同加密者对法律执行辩论的长期解决方案是十分重要的一样,信息隐藏对于隐私也是重要的。从人口普查到医疗记录,大量的个人信息在处理过程中是不应该被别有用心的人识别出来的。有时候,这方面做得很好,但有时候不需要付出太多的努力就可能重新确定数据的主体内容。

随着这些力量的驱动,信息隐藏的研究呈指数级增长,它在最近五年所取得的成就完全可与 1945—1990 年间密码学所取得的成就相提并论,大量的信息隐藏系统被设计出来,其中许多系统已被攻破。关于什么系统能用,什么系统不能用,所感兴趣的研究方向等等,我们现在已有一个公正的见解。

所以我非常高兴在这里看到了第一本在信息隐藏方面很全面的技术书籍,我希望在未来许多年里它将成为该学科的标准参考书。

# 前　言

本书对隐写术和数字水印作了全面的介绍，这两个研究领域一般都统称为“信息隐藏”。隐写术主要研究如何将秘密信息隐藏在不太容易引起注意的消息之中，从而使得秘密通信不被察觉，而数字水印则源于数字媒体版权保护的需求。

就在几年之前，信息隐藏技术还没有像密码学一样引起研究团体和工业界更多的关注。然而，最近形势迅速发生变化。1996 年，召开了这方面的第一次国际学术会议，其主要驱动力在于对版权保护的关注。由于音频、视频和其它作品都能以数字形式获得，制作完美拷贝变得非常容易，这将会导致大规模非授权的拷贝，而这恰好是音乐、电影、书籍和软件出版业最为担忧的问题。

信息隐藏研究使各种不同背景的研究人员走到一起来，比如：电子工程、信号与图像处理、计算机科学以及密码学等等，这里就不一一列举了。到目前为止，对这个相对较新的研究领域还没有形成一个全面而统一的看法。可以从不计其数的论文和会议文集中获得这方面的相关信息资料。根据一个大型文献目录信息系统统计，1998 年发表了 103 篇专门研究数字水印的论文，而 1992 年只发表了 2 篇，这也表明信息伪装和数字水印越来越重要。本书的目标就是为该研究领域提供一本既可作教科书又可作全面参考手册的书籍。

本书第一章介绍了信息隐藏领域的状况，并对信息隐藏可能的应用作了一个全面的描述。本书第一部分专门讨论隐写术，其中第二章讨论了信息伪装的基本原理。第三章列出了隐写术的各种应用。第四章重点讨论如何攻破伪装通信。

本书的第二部分专门描述了数字水印系统，其中第五章讨论了水印系统的目标和要求。第六章概览了数字水印研究领域中使用的各种方法。第七章的主题是讨论数字水印的关键问题——健壮性。第八章讨论了数字指纹问题。最后一章讨论了因特网上结合水印技术的版权的法律含义。

# 致　谢

我们非常感谢那些为本书付出艰辛劳动的作者们。尽管他们本身也很忙，但他们还是圆满完成了涉及他们研究课题的有关章节的写作，这需要他们付出相当多的努力，同时也要感谢他们的合作与协助。对我们来讲，能编辑这样一本书以及与他们一起工作是一件十分愉快和荣幸的事情。

我们也要感谢阿尔泰克出版公司（Artech House）的 Viki Williams、Susanna Taggart、Michael Webb 和 Hilary Sardella，是他们帮助我们克服了在本书出版过程中的各种困难。同时，我们也要感谢 Philipp Tomsich，是他帮助我们建立了一个共享的计算机帐户。感谢 Raimund Kirner，是他制作了本书的各种插图。最后，我们还要提及那些不知姓名的校阅者，是他们提供了各种有用的反馈信息，这些反馈信息对我们编写本书有极大的帮助。

Stefan C. Katzenbeisser

Fabien A. P. Petitcolas

1999 年 6 月于维也纳和剑桥

# 目　录



## 第一部分　密写与隐写术

## 第二部分　数字水印与版权保护

# 第一章　信息隐藏入门

(Fabien A.P. Petitcolas)

由于音频、视频和其它作品都能以数字形式获得，制作其完美拷贝变得非常容易，从而可能会导致大规模非授权拷贝，而这极有可能会损害音乐、电影、书籍和软件等出版业的发展。对版权保护的这类关注引发了一个很有意义的研究方向：寻找将版权信息和序列号隐藏到数字媒体中的方法，其目标是：通过序列号来帮助识别版权侵犯者，而版权信息能用来检举和起诉盗版者。

同时，各级政府对普通百姓获取加密服务的限制，也驱使人们研究将私有信息嵌入到表面上看来无关紧要的掩饰信息之中的各种方法。

还有许多其它的应用前景引发人们对信息隐藏这一学科的兴趣。在这一章中，我们将描述它们中的一部分来说明这个研究主题的广阔性。但在此之前，我们将介绍与计算机系统有关的信息隐藏的各主要分支情况，并简要回顾这个引人注目的研究领域。

## 1.1　信息隐藏学的主要分支

隐蔽信道由 Lampson 在文献[1]中定义为：在多级安全水平的系统环境中(比如，军事计算机系统)，那些既不是专门设计的也不打算用来传输消息的通信路径称为隐蔽信道。这些信道在为某一程序提供服务时，可以被一个不可信赖的程序用来向它们的操纵者泄露信息。为了找到限制这种动机的方法，人们已经详细研究过这些通信信道[2]。在这个主题上我们将不会展开太多，只是介绍以太网上一个隐蔽通信的例子(见 2.7.2 节)，以及关于图像降质的背景和原由(见 3.2.3)。

匿名通信就是寻找各种途径来隐藏通信消息的主体，即消息的发送者和接收者。匿名通信早期的例子包括由 Chaum 在文献[3]所描述的信件匿名重发器和由 Goldschlag、Reed 和 Syverson 在文献[4]中所提出的洋葱路由，其想法是：只要中间参与者不相互串通勾结，通过使用一组邮件重发器或路由器，人们就可以将消息的踪迹隐蔽起来，因此信任是这些工具的基础。根据谁被“匿名”(发送者、接收者，或两者)，匿名通信又分为几种不同的类型。Web 应用强调接收者的匿名性，而电子邮件用户们更关心发送者的匿名性。

隐写术是信息隐藏学的一个重要分支。密码学研究如何保护消息内容，而隐写术专门研究如何隐藏实际存在的信息。隐写术的英文名词 Steganographia 是由 Trithemius(1462—1516)首先构造出来的，一般认为来源于希腊文 στεγανο-ζ、γραφ-ειν，其含义为“被掩盖的笔迹”[5]，该词的现代含义通常理解为将一个信息隐藏在另一个信息之中(图 1.2 显示了 Trithemius 著作的封面)。这方面的例子有：使用不可见墨水给报纸上的某些字母作上标记来向一个间谍发送消息，在一个录音带的某些位置加一些不易察觉的回声等。第二章将介绍一些把数据隐藏到另一些数据中的一般模型，而一些主要的伪装技术将在第三章进行阐述和评论。

与隐写术相反，水印技术需要增加健壮性要求，以对抗各种可能的攻击。在该领域中，术

语“健壮性”的含义一直不是很清楚，它取决于应用的场合，但一个成功的攻击只需使水印标记检测不出来即可。我们将在第七章展示这些攻击方法。健壮性在整个水印系统设计中具有非常重要的份量，这也是我们在本书中将隐写术和数字水印区别对待的原因之一。

水印并不总是需要隐藏起来，正如一些系统需要可见的数字水印[6]，但在文献中绝大多数情况下还是强调不可察觉的（或称不可见的、透明的或听不见的，依上下文而定）数字水印，因为它们的应用范围更广泛些。可见的数字水印完全可追溯到13世纪末期出现的标明纸张来源的纸张水印（见5.2.1节）。现代的可见水印可以是放置在数字图像上的各种可见图案（比如，一个公司的标识或版权标记），它们被那些对不可见水印技术不信任的摄影师们广泛使用（见[7]）。

从上述简要的介绍，读者也许已经注意到隐写术与水印的另一个根本的不同点，即水印系统所隐藏的信息总是与被保护的数字对象或它的所有者有关，而信息隐写系统可以隐藏任何信息。同时，“健壮性”评判标准也不同，因为隐写术主要关注被隐藏信息的检测，而水印技术则关注被盗版者擦除的可能性。最后，伪装通信通常是点对点的（在发送者与接收者之间），而数字水印技术通常是一点对多点的。

信息隐藏这两个分支的准确术语将在第二章和第五章给出。

## 1.2 对信息隐藏历史的简要回顾

在这一节里，我们并不想讲述信息隐藏的整个历史全貌，而只介绍一些重要的里程碑式的事件。希望了解更多历史细节的读者请参考文献Kahn[8]和[9,10]。

### 1.2.1 技术性的隐写术

隐写术最有名的例子可追溯到远古时代。Herodotus（C.486—425 B.C.）在他的著作 *Histories*[11]中讲述到：大约在公元前440年，Histiaus给他最信任的奴隶剃头并将一个消息刺在头上，直到他的头发重新长出后，这条信息才消失，这样做的目的是为了鼓动奴隶们起来反抗波斯人。令人惊讶的是，一些德国间谍在20世纪初期仍然使用这种方法。Herodotus还讲到，在波斯朝廷的一个希腊人Demeratus是如何警告斯巴达将发生一场由波斯国王薛西斯一世发动的入侵的。他先去掉书记板上的蜡，然后将他的消息写在蜡下面的木板上，最后再用蜡覆盖住那个消息。这个书记板看起来完全像一个空白的书记板（它几乎既欺骗了接收方也蒙骗了海关士兵）。有许多隐写技术是由战术家Aeneas发明或记载下来的[13]，包括将信函隐藏在信使的鞋底里或妇女的耳饰中，将正文消息写在木板上然后用石灰水把它刷白，以及由信鸽携带便条传送等等。Aeneas也提出了通过改变字母笔画的高度或在掩蔽文体的字母上面或下面挖出非常小的小孔来隐藏正文，后一种方法直到17世纪还在使用，但后来Wilkins（1614—1672）对它进行了改进，他不是挖制小孔而是用无形的墨水制作非常小的斑点[14]，并且该方法又被德国间谍在两次世界大战中重新使用起来[8,p.83]。这项技术的现代版本目前仍然在文本安全中使用，并且通过在纸页上打印各种小像素点组成的块来对诸如日期、打印机标识符、用户标识符等信息进行编码。

在1857年，Brewster就已经提出将秘密消息隐藏“在大小不超过一个句号或小墨水点的空间里”的设想[16]。到1860年，制作微小图像的基本难题已经被一个叫Dragon的法国摄影师