数字水印技术及应用

SHUZI SHUIYIN JISHU JI YINGYONG

孙圣和　陆哲明　牛夏牧　等著

科学出版社
www.sciencep.com

内 容 简 介

本书为关于数字水印技术及其应用的专著。全书共分11章。从信息隐藏的概念入手，首先介绍数字水印的概念、分类、框架及特性，数字水印的应用领域及相关的法律问题和评价问题；然后着重讨论数字水印系统水印生成、水印嵌入、水印检测和水印攻击四大关键技术的各种有效算法；接着介绍针对各种载体对象的音频、图像、文档、视频和三维模型的数字水印应用技术；最后介绍可见水印技术。

本书取材广泛，内容新颖，系统性与理论性强，充分反映了近几年来数字水印技术的最新研究动态，并包含了作者近五年来的研究成果。

本书可供从事信息隐藏、信息安全、版权保护、真伪鉴别与保密通信，计算机网络安全和防拷贝，数字图像、音频和视频信号处理，三维模型处理、信号检测与模式识别等领域的科技人员与教学人员阅读和参考，并可以作为相关专业研究生的教材。

图书在版编目(CIP)数据

数字水印技术及应用/孙圣和，陆哲明，牛夏牧等著. —北京：科学出版社，2004
ISBN 7-03-014206-3

Ⅰ.数… Ⅱ.孙… Ⅲ.电子计算机-密码术 Ⅳ.TP309.7

中国版本图书馆CIP数据核字(2004)第097424号

责任编辑：马长芳 / 文案编辑：董 斌 / 责任校对：张 琪
责任印制：钱玉芬 / 封面设计：耕者设计部

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
源海印刷有限责任公司印刷

科学出版社发行 各地新华书店经销

*

2004年11月第 一 版 开本：787×1092 1/16
2004年11月第一次印刷 印张：45 3/4
印数：1 —2 500 字数：1 058 000

定价：88.00元

(如有印装质量问题，我社负责调换〈环伟〉)

前　言

随着信息技术和计算机网络的飞速发展，数字多媒体信息（图像、文本、音频、视频、三维模型）的存储、复制与传播变得非常方便。我们的视觉和听觉尽情地享受着多媒体及数字传输技术带来的愉悦，不但可以通过互联网和 CD-ROM 方便快捷地获得多媒体信息，还可得到与原始数据完全相同的复制品。我们毫无限制地任意编辑、修改、拷贝和散布那些数字音乐和图像，但是这些数字媒体原创者的版权和经济利益如何得到保护，数字媒体是否安全、可信，由此引发的信息安全问题、盗版问题和版权纷争问题已成为日益严重的社会问题。因此，对多媒体内容的版权保护与内容鉴别已成为亟待解决的问题。

目前的版权保护系统广泛采用对网络资源的访问控制机制，它通过本地网或广域网控制某些 IP 地址或终端的连接，限制某些用户的访问权限，从而有效地防止非法用户对计算机系统的访问。但是，如果用户以合法账号得到多媒体信息，再对数据进行非法复制和传播，则安全访问控制机制就无能为力了。密码技术是信息安全技术领域的主要传统技术之一，是基于山农信息论及其密码学理论的技术，一般采用将明文加密成密文的秘密密钥系统或公开密钥系统，其保护方式都是控制文件的存取，即将文件加密成密文，使非法用户不能解读。但是，加密的密文容易引起许多好事者的兴趣，激发他们积极破译的热情。传统的加密方法对多媒体内容的保护和完整性认证具有一定的局限性。首先，随着计算机处理能力的快速提高，这种通过不断增加密钥长度来提高系统密级的方法变得越来越不安全；其次，加密方法只用在通信的信道中，一旦被解密，则信息就完全变成明文；另外，密码学中的完整性认证是通过数字签名方式实现的，它并不是直接嵌到多媒体信息之中，因此无法察觉信息在经过加密系统之后的再次传播与内容的改变。另一方面，多媒体技术已被广泛应用，需要进行加密、认证和版权保护的音像数据也越来越多。数字化的音像数据从本质上说就是数字信号，若对这类数据也采用密码加密方式，则其本身的信号属性就被忽略了。最近几年，许多研究人员尝试用各种信号处理方法对音像数据进行隐藏加密，并将该技术用于制作多媒体的“数字水印”。这样，数字水印技术作为加密技术的补充，在多媒体信息的版权保护与完整性认证方面得到迅猛发展。

数字水印技术是近几年来国际学术界兴起的一个前沿研究领域。它与信息安全、信息隐藏、数据加密等均有密切的关系。它通过在被保护的数字对象（如静止图像、视频、音频等）中嵌入某些秘密信息——水印（watermark）来证明版权归属或跟踪侵权行为。它通过一定的算法将一些标志性信息直接嵌到多媒体内容当中，但不影响原内容的价值和使用，并且不能被人的感知系统察觉，数字水印必须很难被清除。水印信息可以是作者的序列号、公司标志、有特殊意义的文本等，可用来识别文件、图像或音乐制品的来源、版本、原作者、拥有者、发行人、合法使用人对数字产品的拥有权。而且这种水印通常是不可见或不可察觉的，它与原始数据（如图像、音频、视频数据）紧密结合并隐藏其中，它可经历一些不破坏源数据使用价值或商用价值的操作而被保存下来。当然，从理论上讲，只要具有足够的知识，任何水印都可以去掉。但是，如果只能得到部分信息，而水印在图像中的精确位置未

知，那么破坏水印将导致原始图像质量严重下降。

与加密技术不同，数字水印技术并不能阻止盗版活动的发生，但它可以判别对象是否受到保护，监视被保护数据的传播、真伪鉴别和非法拷贝，解决版权纠纷并为法庭提供证据。为了给攻击者增加去除水印的难度，目前大多数水印制作方案都采用密码学中的加密（包括公开密钥、私有密钥）体系来加强，在水印的嵌入、提取时采用一种密钥，甚至几种密钥联合使用。

由于数字水印是实现版权保护的有效办法，因此如今已成为多媒体信息安全研究领域的一个热点，也是信息隐藏技术研究领域的重要分支。数字水印技术除了应具备信息隐藏技术的一般特点外，还有着其固有的特点和研究方法。在数字水印系统中，隐藏信息的丢失，即意味着版权信息的丢失，从而也就失去了版权保护的功能，也就是说，这一系统是失败的。由此可见，对版权保护应用领域来说，数字水印技术必须具有较强的透明性、安全性和鲁棒性。①透明性：在数字作品中嵌入数字水印不会引起作品明显的降质，并且不易被察觉。②隐藏位置的安全性：水印信息隐藏于数据而非文件头中，文件格式的变换不应导致水印数据的丢失。③鲁棒性：所谓鲁棒性是指在经历多种无意或有意的信号处理过程后，数字水印仍能保持完整性或仍能被准确鉴别。可能的信号处理过程包括信道噪声、滤波、数/模与模/数转换、重采样、剪切、位移、尺度变化以及有损压缩编码等。在数字水印技术中，水印的数据量和鲁棒性构成了一对基本矛盾。从主观上讲，理想的水印算法应该既能隐藏大量数据，又可以抵抗各种信道噪声和信号变形。然而在实际中，这两个指标往往不能同时实现，不过这并不会影响数字水印技术的应用，因为实际应用一般只偏重其中的一个方面。如果是为了隐蔽通信，数据量显然是最重要的，由于通信方式极为隐蔽，遭遇敌方篡改攻击的可能性很小，因而对鲁棒性要求不高。但对保证数据安全来说，情况恰恰相反，各种保密的数据随时面临着被盗取和篡改的危险，所以鲁棒性是十分重要的，此时，隐藏数据量的要求居于次要地位。

数字水印技术的基本思想源于古代的隐写术。古希腊的斯巴达人曾将军事情报刻在普通的木板上，用石蜡填平，收信的一方只要用火烤热木板，融化石蜡后，就可以看到密信。使用最广泛的隐写方法恐怕要算化学隐写了，牛奶、白矾、果汁等都曾充当过隐写药水的角色。可以说，人类早期使用的保密通信手段大多数属于隐写而不是密码。然而，与密码技术相比，隐写术始终没有发展成为一门独立的学科，究其原因，主要是因为隐写术缺乏必要的理论基础。如今，数字化技术的发展为古老的隐写术注入了新的活力，也带来了新的机会。在研究数字水印的过程中，研究者大量借鉴了隐写术的思想。尤其是近年来信息隐藏技术理论框架研究的兴起，更给隐写术成为一门严谨的科学带来了希望。毫无疑问，隐写技术将在数字时代得以复兴。目前，数字水印的研究涉及多学科领域的理论和技术，如信息论、编码理论、通信原理、保密技术、信号处理、优化理论、模糊集合论、矩阵分析、神经网络、小波变换、视觉模型、拓扑学、随机概率理论、预测技术、模式识别、法律问题等等。

本书为从事信息隐藏的研究人员介绍数字水印的各项关键技术以及数字水印的各种应用，目的是推出一本较新较全的数字水印著作，使研究人员能够对数字水印技术有全面了解，并推动国内对数字水印技术的深入研究。本书重点介绍了数字水印的四大关键技术，即水印生成、水印嵌入、水印检测以及水印攻击，并重点讨论数字水印技术在图像、文

本、音频、视频和三维模型等载体的版权保护和内容验证中的应用。本书共包括11章。第一章从信息隐藏技术的介绍入手，引出数字水印的概念、原理、关键技术和特性要求，介绍目前数字水印的应用领域和与此相关的法律问题和评价问题。第二章介绍各种数字水印生成技术。第三章介绍各种数字水印嵌入技术，包括时空域、变换域和压缩域数字水印嵌入技术等等。第四章介绍各种数字水印检测技术。第五章阐述数字水印攻击技术。第六章到第十章分别介绍数字水印技术在音频、图像、文本、视频和三维模型的版权保护和内容认证中的应用。最后一章介绍可见水印技术。本书与其他已有的数字水印专著相比，具有如下特点：①内容全面。涉及数字水印系统的各项关键技术理论和各种载体对象。②结构合理，系统性强。本书的前几章主要介绍数字水印系统的四大基础技术，后面几章重点介绍各种载体对象的数字水印应用技术。③内容新颖。本书详细介绍了可见水印技术和乐谱水印技术，系统介绍了几种特殊的图像水印技术，如可逆水印技术、抗几何攻击的水印技术和基于矢量量化的数字水印技术等，并系统介绍了数字图像水印系统的评测问题。④理论性强。本书介绍了许多与数字水印相关的基础理论，如密码技术、数字签名技术、伪随机序列、扩频、混沌、纠错编码、多分辨率分解、哈西函数、奇异值分解、离散正交变换、分形、相关、统计决策、神经网络、优化技术、半色调化技术、颜色量化、可视密码术、矢量量化技术、三维建模等。

本书的第一章由孙圣和教授执笔，第二章到第八章以及第十章和第十一章主要由陆哲明教授执笔，第九章由牛夏牧教授执笔，颜斌博士负责第四章和第六章的部分内容，杨边博士参与撰写第七章的部分内容，乔玉龙博士参与撰写第十一章的部分内容，刘旺博士参与撰写第十章的部分内容，俞龙江博士参与撰写第五章的部分内容。全书由孙圣和教授最终定稿。在本书的撰写过程中还得到了哈尔滨工业大学自动化测试与控制研究所的其他各位教师、博士生和硕士生的帮助，在此表示衷心的感谢。作者在本书中述及的研究工作得到国家自然科学基金、航天技术创新基金、全国优秀博士学位论文作者专项基金和哈尔滨工业大学交叉学科基金和科学研究基金资助。本书的出版得到中国科学院科学出版基金和哈尔滨工业大学出版著作基金资助。

限于水平，书中难免有错误与不妥之处，恳请读者批评指正。

作　者

2004年7月

于哈尔滨工业大学自动化测试与控制研究所

目　录

第一章 绪 论

多媒体数据的数字化为多媒体信息的存取提供了极大便利，同时也极大地提高了信息表达的效率和准确性。随着 Internet(因特网)的日益普及，多媒体信息的交流已达到了前所未有的深度和广度，其发布形式也愈加丰富。人们如今可以通过 Internet 发布自己的作品、重要信息和进行网络贸易等，但是随之出现的问题也十分严重，如作品侵权更加容易，篡改也更加方便。因此，如何既充分利用 Internet 的便利，又能有效地保护知识产权，已受到人们的高度重视。在这种背景下，一门新兴的交叉学科——信息隐藏学正式诞生。如今，信息隐藏学作为隐蔽通信和知识产权保护等的主要手段，正得到广泛研究与应用。

本章从网络信息安全问题出发，首先介绍传统的密码技术和数字签名技术，然后根据密码技术所存在的缺点引出信息隐藏技术，重点介绍信息隐藏学两大分支——隐写术和数字水印的基本概念和基本思想，最后重点介绍数字水印系统的框架与模型、应用与特性以及相关的一些法律问题和评价问题。

1.1 网络信息安全

1.1.1 网络时代和信息安全问题

真正的人类文明从网络开始。实际上，我们早已生活在各种各样的网络中，从电力网、电话网、广播电视网、商业网到交通网。但是，所有这些网络都没有像 Internet 那样，在如此短的时间内影响如此多的政府、企业和个人。目前，网络已经成为 Internet 的代名词。在过去的几年中，随着计算机和网络技术的快速发展，Internet 的规模急剧膨胀。以中国为例，Internet 的用户 1997 年底为 62 万户，1998 年底为 210 万户，到 2002 年初已达 1591 多万户。Internet 技术打破了传统的边界概念，使世界变得越来越小，而市场却越变越大，广阔的世界宛如地球村，全球经济一体化和信息网络化相互促进、相互依存的趋势越来越明显。在网络信息时代，任何产品、技术都要考虑到 Internet。电子商务作为网络时代经济活动全新的技术手段和方法，已成为 Internet 最广阔的应用领域。**电子商务**是指在网络环境特别是 Internet 上进行的商务活动。从交易的参与者来看，电子商务有企业对企业(B to B)、企业对消费者(B to C)和消费者对消费者(C to C)等几种类型。在网络经济时代，各国政府也都面临着角色转换以适应时代要求的新课题，许多国家都先后提出了构建**电子政府**的纲领，我国也于 1999 年启动了“政府上网工程”。网络信息系统将在政治、军事、金融、商业、交通、电信、文教等方面发挥越来越大的作用。

现有的计算机网络大多数在建设之初都忽略了安全问题，即使考虑了安全，也只是把安全机制建立在物理安全机制上，因此，随着网络的互联程度的扩大，这种安全机制对于

网络环境来讲形同虚设。另外，目前网络上使用的协议，比如 TCP/IP 协议，在制订之初也没有把安全考虑在内。开放性和资源共享是计算机网络安全问题的主要根源，它的安全性主要依赖于加密、网络用户身份鉴别、存取控制策略等技术手段。面对如此严重危害网络信息系统的种种威胁和网络安全与保密的重要性，必须采取有力的措施来保证网络信息的安全与保密。网络的安全措施一般分为三类：逻辑上的、物理上的和政策上的。面对越来越严重危害计算机网络安全的种种威胁，仅仅利用物理上和政策（法律）上的手段来防范计算机犯罪显得十分有限和困难，因此也应采用逻辑上的措施，即研究开发有效的网络信息安全技术。即使有了非常完备的安全与保密政策法规，有了非常先进的安全与保密技术，以及天衣无缝的物理安全机制，但是如果这些知识得不到普及，那么所有努力都是白费。

人们对信息安全概念的认识在不断地更新。在主机时代，人们把信息安全理解为对信息的机密性、完整性和可获性的保护，其概念是面向数据的。在 20 世纪 80 年代的微机和局域网时代，由于用户和网络结构比较简单，故信息安全是面向网管、面向规约的。20 世纪 90 年代进入了互联网时代，每个用户都可以连接、使用乃至控制分布在世界各个角落的上网计算机，故 Internet 的信息安全强调面向连接、面向用户。由此可见，面向数据的安全概念是信息的保密性、完整性和可获性，而面向使用者的安全概念则是鉴别、授权、访问控制、抗否认性和可服务性以及基于内容的个人隐私、知识产权等的保护。这两者结合就是**广义信息安全**概念，它是指所有涉及信息的安全性、完整性、可用性、真实性和可控性的相关理论和技术，它是物理安全、网络安全、数据安全、信息内容安全、信息基础设施安全与公共信息安全的总和。而**狭义信息安全**是指信息内容的安全性，即保护信息的秘密性、真实性和完整性，避免攻击者利用系统的安全漏洞进行窃听、冒充、诈骗、盗用等有损合法用户利益的行为，保护合法用户的利益和隐私。信息安全体系结构中的安全服务问题要依靠密码、数字签名、身份验证技术、防火墙、安全审计、灾难恢复、防病毒、防黑客入侵等安全机制（措施）加以解决。其中密码技术和管理是信息安全的核心，安全标准和系统评估是信息安全的基础。从技术角度看，信息安全是一个涉及计算机科学、网络技术、通信技术、密码技术、应用数学、数论、信息论等多种学科的边缘性综合学科。

下面我们简单介绍网络信息安全的几种主要威胁[1]：

（1）黑客攻击和高技术犯罪

现在人们几乎天天都能看到黑客的报道。**“黑客”**(hacker)原来是一个褒义词，指的是那些尽力挖掘计算机程序最大潜力的电脑精英。目前，黑客的普遍含义是指计算机网络系统的非法入侵者，他们大都是计算机天才，通过找出计算机网络系统的漏洞，使跨国公司和政府机构的网站崩溃。例如，2000 年 2 月，在短短的三天时间内，黑客使美国数家顶级互联网站，如 Yahoo!、Amazon、eBAY、CNN 等陷入瘫痪。他们采用的手法却非常简单，即用大量的无用信息或数据垃圾阻塞网站服务器或挤占路由器，使其为这些无法识别其真实目的的数据忙个不停而不能正常工作。2000 年 3 月 6 日晚 6 时 50 分，美国白宫网站主页被黑：在白宫上空飘扬的美国国旗竟变成了骷髅头的海盗旗；在克林顿与戈尔的合影中，戈尔成了独眼龙。据报道，我国有 90%的电子商务网站存在安全隐患，95%上网的网管中心都遭到过境内外黑客的攻击或侵入，其中银行、金融和证券机构是黑客攻击的重