ELECTRONIC ENGINEER

XIDIAN UNIVERSITY PRESS

Technology of Digital Watermarking

数字水印技术

王炳锡　陈琦　邓峰森　编著

Specially Designed for Engineers and Technicians of Electronics

西安电子科技大学出版社

http://www.xduph.com

数字水印技术

王炳锡　陈琦　邓峰森　编著

西安电子科技大学出版社

2003

内 容 简 介

信息隐藏是一门新兴的学科，而数字水印是信息隐藏研究的一个重要方向，它在数字图像、音频、视频、文本等多媒体版权保护领域都具有广泛的应用价值。本书从信息隐藏技术的基本概念出发，以用于图像、音频、视频、文本等数字产品的知识产权保护的水印技术为主，详细介绍了水印的设计、产生、嵌入、检测、攻击技术以及相应的评价指标。由于数字水印技术本质上是信源编码在信息安全领域的应用，所以对现代信源编码也做了相应的阐述，并结合作者的研究成果给出了大量的实例，因此本书在理论上较为系统，在实践上提供了实用的图表和参数，可操作性强。

全书共分八章，前三章介绍信息隐藏、数字水印、水印信号的设计与产生的基础知识；后五章介绍以图像、音频、视频、文本为载体的数字水印的产生、嵌入、提取、攻击及相应的评价指标和方法。每章后附有参考文献，供读者深入研究考证。书末附有英汉名词对照，供阅读外文资料时参考。

本书可作为高等学校理工科通信和信息处理及相关专业的高年级本科生和(硕士、博士)研究生的教材或参考书，也可供从事网络通信安全和水印制作的工程技术人员、管理人员、法律工作者及从事隐密通信和反盗版的情报人员及技术人员参考。

图书在版编目(CIP)数据

数字水印技术/王炳锡等编著. —西安：西安电子科技大学出版社，2003.11

ISBN 7-5606-1295-4

Ⅰ.数… Ⅱ.王… Ⅲ.数字技术—应用—水印 Ⅳ.TS805.4

中国版本图书馆 CIP 数据核字(2003)第 085786 号

责任编辑 臧延新

出版发行 西安电子科技大学出版社(西安市太白南路 2 号)

电 话 (029)8242885 8201467 邮 编 710071

http://www.xduph.com E-mail：xdupfxb@pub.xaonline.com

经 销 新华书店

印 刷 西安兰翔印刷厂

版 次 2003 年 11 月第 1 版 2003 年 11 月第 1 次印刷

开 本 787 毫米×1092 毫米 1/16 印张 13.25

字 数 310 千字

印 数 1～4000 册

定 价 20.00 元

ISBN 7-5606-1295-4/TN·0238

XDUP 1566001-1

前　言

信息隐藏技术是一个多学科交叉的现代高科技产物。由于多媒体技术的发展，信息隐藏技术一出现立即就得到商业应用。目前信息隐藏技术在图像、音频、视频、文本、网络通信中的隐蔽通信、复合传输、版权保护等方面已有较多的使用。但作为一门技术，它仍有大量的实际问题需要研究，仍有大量的理论问题需要探讨。在我们的学习和研究过程中，认为以下几个课题是急需解决的：① 信息载体的信息容量问题；② 秘密信息的安全嵌入问题；③ 对隐藏信息的检测、提取、攻击问题；④ 信息安全的认证问题。当然，信息隐藏技术是多学科交叉应用的产物，那么信息隐藏技术的理论研究也应当是以多学科的知识作支撑，我们认为至少应从信息论、密码学、数字信号处理、通信原理、计算机网络等几个学科入手。

应当说信息隐藏技术从有隐密通信就已开始研究，但由于其特殊的用途，一直被限制在军事和安全部门一个很小的范围内。随着多媒体技术的发展，网络通信逐步成为人们交流信息的方式之一，使得电子政务、电子商务、远程教育、数字图书馆、电子音像作品发行等的认证、防伪、抗攻击的社会需求越来越迫切。对信息隐藏技术大范围深入研究应该是在 1996 年英国剑桥举行的“第一届信息隐藏学术研讨会”之后。目前的研究思路基本上是把载体当作信道，把隐藏的信息用密钥扰乱，用各种算法嵌入载体。要求载体的变化不被感知，隐藏的信息经过传输仍然安全，由此衍生出来隐藏信息的发现、检测、攻击等技术。正像盾与矛一样，隐藏与攻击在斗争中发展，在斗争中创新。由于市场需求的牵引，信息隐藏吸纳了各种现代技术，因而发展十分迅猛，但其基础理论的研究仍然是一个薄弱环节。

数字水印是信息隐藏技术之一，是信息隐藏技术形象生动的应用。数字水印在声像艺术品的版权保护中已有应用，而在商标、票据、证书、标牌、专利等的电子制作中，水印技术的应用仍是一个技术难题，如电子水印是否能印刷在纸上，印刷后的水印是否能被检测出来，是否具有抗扭曲、剪切、扫描等几何形变的鲁棒性，也就是抗攻击能力。这些问题的提出只是一家之见，定有偏颇狭隘之处，希望能与学术界同行探讨，集大家之智慧，把信息隐藏技术推向更高的层次。这也是我们编著本书的目的之一。好在国际上已有公开的网站，如向水印研究者提供交流的论坛：http：//www. watermarkingworld. org/，以及一些由水印研究单位和学者维护的主页，如 http：//www-nt. e-technik. uni-erlangen. de/～hartung/watermarkinglinks. html、http：//cosimo. die. unifi. it/～piva/Watermarking/watermark. html 等。这些网站和主页为研究者提供了各种方便，大家可以相互学习和讨论，各抒己见，相信不用太多的时间，信息隐藏技术会产生一个质的飞跃。

适时地理清学习、研究工作的头绪，总结阶段性的进展和教训，吸纳众家之成果，为更深入地研究在方向上和方法上定位，则是我们编著本书的目的之二。

鉴于数字水印技术是一门新技术，涉及到多门学科和多种技术，各种文献资料使用符号繁杂，不便于交流，本书用 W 表示水印，用掩体对象符号上加波纹表示嵌入了水印，如

图像 I 嵌入水印后用 $\tilde{I}$ 表示。我们认为这样表示清晰、形象，便于对数字水印技术的学习和研究。欢迎学术界同仁对这种表示方法进行指正。

本书共分 8 章，第 1 章简要介绍了信息隐藏技术的概念、术语、主要原理；第 2 章介绍了数字水印技术；第 3 章给出了水印信息的产生方法；其后各章对不同类型的数字水印技术以及攻击方法进行了详细说明。前 4 章和第 6 章由王炳锡和陈琦编写，第 5 章由陈琦和邓峰森编写，第 7、8 章由邓峰森编写。全书由王炳锡统稿。本书的特点是注意基本概念和基础理论的阐述，侧重于水印技术的研究和总结，而且紧密结合自己的研究成果，吸纳最新的有创见的思想方法，此外本书较为系统，条理清楚，逻辑性强，语言流畅，易读实用。书后附有“英汉名词对照”、“名词概述”、“Matlab 语言典型算法程序”和“信息隐藏的软件与产品”。本书可作为大学高年级本科生及硕士生的选修教材或参考书，也可作为科研人员的参考资料。

本书的编著得到了解放军信息工程大学各级领导的关心和支持，并得到了国内广大学者的支持和帮助，尤其是课题组同志和研究生们的研究成果充实、完善了本书的内容，增强了本书的可读性和可操作性。书中引用了大量的文献资料，在此向原作者表示深深的谢意。因本人的研究水平和阅历有限，书中错漏之处在所难免，恳切希望读者不吝赐教，在此表示衷心感谢。请与作者联系，共同研讨问题，联系地址为河南省郑州市 1001 信箱 837 号(邮编 450002)。

王炳锡

2003 年 8 月

于解放军信息工程大学

目　录

第 1 章　信息隐藏技术概述

20 世纪 90 年代以来，计算机网络技术和多媒体处理技术在全世界范围内得到了迅猛发展。计算机网络技术的发展使得处在世界各地的人们进行信息交流更加方便、直接和经济，多媒体技术的发展为多媒体信息的存储和传播提供了极大的便利，同时也极大地提高了信息表达的效率和准确性。特别是最近几年，多媒体信息的交流已达到了前所未有的深度和广度，其传播形式也愈加丰富多彩。人们如今可以方便地通过因特网发布自己的作品、重要信息和进行网络贸易等。但是，网络在给人们带来便利的同时也暴露出越来越重要的安全问题：如媒体作品的版权侵犯，软件或文档的非法拷贝，电子商务中的非法盗用和篡改等。因此，如何既充分利用因特网的便利，又能有效地保护知识产权，已经成为了一个十分紧迫的课题。信息隐藏(Information Hiding)技术的研究在近年来成为了国际信息技术研究领域的一个新兴的研究方向，它作为隐蔽通信和知识产权保护等的主要手段，正得到广泛的研究与应用。

信息隐藏技术是研究如何将某一信息隐藏于另一公开的信息中，然后通过公开信息的传输来传递隐藏的信息。由于含有隐藏信息的媒体发布是公开的，而可能的检测者难以从公开信息中判断隐藏信息是否存在，更加难以截获隐藏信息，从而达到保证信息的安全的目的。

信息隐藏技术不同于传统的密码学技术。密码技术主要是研究如何将机密信息进行特殊的编码，以形成不可识别的密码形式(密文)进行传递；而信息隐藏技术则主要研究如何将某一机密信息秘密隐藏于另一公开的信息中，然后通过公开信息的传输来传递机密信息。对加密通信而言，可能的监测者或非法拦截者可通过截取密文，并对其进行破译，或将密文进行破坏后再发送，从而影响机密信息的安全；但对信息隐藏而言，可能的监测者或非法拦截者则难以从公开信息中判断机密信息是否存在，难以截获机密信息，从而能保证机密信息的安全。

1.1　信息隐藏技术的术语和模型

图 1－1 是一个信息隐藏的通用模型。我们称待隐藏的信息为秘密信息(Secret Message)，它可以是版权信息或是秘密数据，也可以是一个序列号；而公开信息则称为载体信息(Cover Message)，如图像、视频、文本或音频信号。这种信息的隐藏一般由密钥(Key)来控制，即通过嵌入算法(Embedding Algorithm)将秘密信息隐藏于公开信息中，而隐藏载体(隐藏有秘密信息的公开信息)则通过信道(Communication Channel)传递，然后检测器(Detector)利用密钥从掩蔽载体中恢复或检测秘密信息。

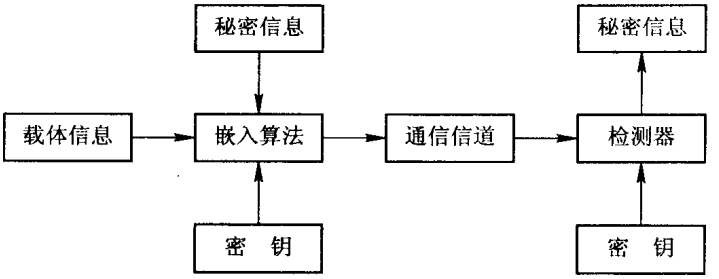

图 1－1 信息隐藏模型

1.2 信息隐藏技术的分类

信息隐藏的应用领域主要有隐蔽信道、隐写术、匿名技术和版权标记技术，故我们对信息隐藏技术进行了如图 1－2 所示的分类[1]。

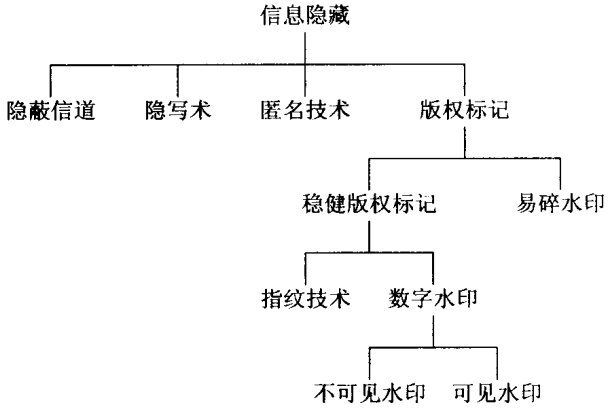

图 1－2 信息隐藏技术的分类

1. 隐蔽信道(Covert Channel)

隐蔽信道是一种通信信道，它存在于计算机系统之中，其特点是信息的传送方式违背了系统的安全原则，从而成为一个隐蔽的信息传输通道。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漏消息。

2. 隐写术(Steganography)

信息隐藏中一个重要的子学科是隐写术。不同于密码学中对信息内容的保护，隐写术着眼于隐藏信息本身的存在。它来自于希腊词根，字面的意义是“密写”，它通常被解释为把信息隐藏于其他信息当中。例如，通过在一份报纸上用隐形墨水标志特定的字母，达到给间谍发送消息的目的。现代的隐写术主要指在数字信息处理和计算机领域，利用信息中普遍存在的冗余性向其中嵌入秘密数据。

3. 匿名技术(Anonymity)

匿名技术是指不暴露身份和个人特征的一种技术，该技术主要应用于网络环境下。网

络匿名可分为发送方匿名和接收方匿名，分别保护通信双方的身份，所使用的主要技术有匿名重发和网络代理等技术。

4. 版权标记(Copyright Marking)

版权标记是向数字作品中嵌入可以鉴别的版权标记信息，该技术是进行数字作品版权保护的一种有效技术。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。与钞票水印相类似，数字水印技术是将特制的标记，利用数字内嵌的方法嵌入到数字图像、声音、文档、图书、视频等数字产品中，用以证明创作者对其作品的所有权，并作为鉴定、起诉非法侵权的证据，同时通过对水印的探测和分析保证数字信息的完整可靠性，从而成为知识产权保护和数字多媒体防伪的有效手段。数字指纹技术是为避免未经授权的拷贝和发行，出品人可以将不同用户的 ID 或序列号作为不同的指纹嵌入作品的合法拷贝。一旦发现未经授权的拷贝，可以从此拷贝中恢复指纹来确定它的来源。

1.3　信息隐藏技术的应用

信息隐藏技术的一个重要应用是数字水印技术，关于该方面的应用我们将在下一节详细介绍，除此之外，它还有以下应用[1-4]：

(1) 军事和安全部门需要不被入侵和破坏的掩蔽通信信道。在现代战争中，即使秘密内容被加密编码，对信号的检测及定位也会很快导致对信号发送装置的攻击。基于这种原因，军事通信可利用信息隐藏技术使得通信不被敌方检测和干扰。

(2) 互联网犯罪分子在进行网络犯罪时利用匿名技术，通过频繁地改变身份和使用代理服务器，并在离线时抹去计算机中留下的踪迹，以防止计算机安全部门的追查。

(3) 法律和相应部门需要深入了解信息隐藏技术的原理及其弱点，以便对妨碍国家和公共安全的秘密信息传递及其他行为进行检测和追踪。

(4) 为避免未经授权的拷贝和发行，出品人可以将不同用户的 ID 或序列号作为不同的指纹嵌入作品的合法拷贝。一旦发现未经授权的拷贝，可以从此拷贝中恢复指纹来确定它的来源。因为单个加入水印的拷贝会受到共谋攻击(Collusion Attacks)，嵌入的水印必须被设计成共谋安全(Collusion Secure)的。在一些应用场合，例如，在 WWW 上用特定的网络搜索器搜索盗版图像时，指纹的提取必须要简单、快捷。

(5) 医疗领域中的医学图像系统可以使用信息隐藏技术。在医用数字图像与通信(DICOM)的标准中，图像数据与患者姓名、图像拍摄日期和诊断医生等说明内容是相互分离的。有时候会发生患者的个人资料与图像的连接关系丢失的现象，利用信息隐藏技术将患者的个人资料嵌入到图像数据中，就可以避免这种情况的发生。

1.4　研 究 现 状

自 1993 年以来，公开发表的有关信息隐藏和数字水印的文章日渐增多。Van Schyndel 在 ICIP'94 会议上发表了题为"A digital watermark"的文章，它是第一篇在主要会议上发表的关于数字水印的文章，其中阐明了一些关于水印的重要概念。这篇文章被认为是一篇具

有历史价值的文献。1996 年在英国剑桥举行的第一届信息隐藏学术研讨会标志着信息隐藏作为一个新的学科的诞生。1998 年在美国波特兰、1999 年在德国德雷斯顿、2001 年在美国匹兹堡分别召开了第二至第四届研讨会。第五届会议将在荷兰的 Noordwijkerhout 举行。此外，一些信息安全、密码学和信息处理领域的国际会议也都有关于信息隐藏技术的专题和文章。一些著名的杂志，如 IEEE 会报、SPIE 等都出版了有关信息隐藏技术的专题。1999 年 12 月 Stefan Katzenbeisser 和 Fabien A. P. Petitcolas 等人出版了该领域的第一本专业论著“Information hiding techniques for steganography and digital watermarking”，其中文译本于 2001 年由人民邮电出版社出版。Neil F. Johnson 等人于 2000 年 12 月出版了“Information hiding steganography and watermarking attacks and countermeasures”一书，Ingemar Cox 等人于 2001 年 10 月出版了关于数字水印的专著“Digital watermarking”。

国内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，于 1999 年开始每年召开一届研讨会，并于 2000 年召开了第一届数字水印技术研讨会。期刊杂志上相关文章的数量从 2000 年开始迅速增加。

随着理论研究的进行，相关的软件不断推出。信息隐藏应用技术的研究主要集中在数字水印上，国际上一些大公司正在致力于以保护音像制品知识产权的数字水印技术的标准化和实用化研究，也有国家在研究使用水印保护和防止伪造电子照片的工作。关于这方面的详细情况将在后续章节中进一步介绍。

1.5 研究课题

信息隐藏技术的研究课题非常广泛，我们认为主要可分为以下几个方面。

1. 信息容量

信息容量问题是信息隐藏技术中的一个关键技术。到目前为止，还没有对某种信息载体可以隐藏多少信息量进行准确计算的理论方法。根据传统的信息理论，任何信源都可以被理想压缩，即信源都存在一定的冗余，这也是进行信息隐藏的前提之一。但是，从隐藏信息不可感知的要求出发，不同载体的冗余度是不同的。比如，由于人耳对声音改变的感知要比人眼对图像改变的感知敏感，在载体文件大小相同的前提下，音频信号可隐藏的数据量比图像信号要少得多。对同一信息载体，不同的隐藏算法可嵌入的信息量也是不同的，一般来讲，变换域算法比时空域算法嵌入的信息量小。当前信息容量的研究大多集中于以静止图像为载体的信息隐藏中。

2. 安全嵌入方法

由于隐藏信息稳健性的要求，对安全嵌入方法的研究一直都是信息隐藏技术研究的目标之一。除非有特殊用途，很难想象对简单的攻击缺乏稳健性的隐藏算法可以实用化。随着信息隐藏攻击方法研究的深入，如何使隐藏的信息可以避免有意或无意的攻击，寻找对尽可能多的攻击算法有免疫性的研究将会持续成为研究的主要方向之一。当前学术界对算法安全性基本达成了一个共识：在隐藏算法公开的前提下，算法的安全性依赖于密钥的使用。

3. 攻击方法

对隐藏信息进行攻击的研究可以促进信息隐藏的发展。它包括对信息隐藏算法的评价标准的研究。目前，学术界还缺少对隐藏算法进行合理评价的通用标准，而这样一个标准必须包括对隐藏信息的稳健性进行的各种攻击测试。对攻击方法和安全嵌入方法的研究是两个互相竞争的过程。一方面研究者希望找到更加安全的嵌入方法；另一方面，攻击研究者则希望找到合理的攻击方法，在不影响载体感知的前提下，对隐藏信息进行破坏或使其不可检测。

4. 对隐藏信息的检测及提取

正如密码学中的加密和解密一样，对隐藏信息进行检测及提取的研究方兴未艾。该技术与攻击方法的研究的不同之处是，后者在研究过程中知道载体中含有隐藏信息，而且不要求对信息进行提取，研究目的是要使其不被检测到；前者则需要对载体中是否含有隐藏信息进行判定。由于隐藏信息不可感知的特性，使得在大量信息载体中对含有隐藏信息的载体进行定位的研究非常困难。如果定位技术的研究获得突破，在隐藏信息算法公开的前提下，对信息进行提取和恢复的研究则类似于密码学中解密的研究。

1.6 小　结

信息隐藏是目前学术界普遍关注的一个交叉性研究领域。本章简要介绍了信息隐藏的概念，描述了相关的术语并且给出信息隐藏的通用模型和分类。随着研究的不断深入，信息隐藏技术的应用也愈加广泛。本章最后给出了当前信息隐藏技术的研究课题和领域。

[参考文献]

[1] Petitcolas F A P, Anderson R J, Kuhn M G. Information hiding—a survey. Proceedings of IEEE, 1999, 87(7): 1062～1078

[2] Bender W, et al. Techniques for data hiding. IBM Systems Journal, 1996, 35(3&4): 313～336

[3] Cox I J, Miller M L. The first 50 years of electronic watermarking. EURASIP J. of Applied Signal Processing, 2002, 2: 126～132

[4] 陈琦，王炳锡. 网络环境下的信息隐藏与数字水印技术. 网络安全技术与应用，2001(7): 19～22

第 2 章　数字水印技术概述

2.1　研 究 背 景

随着数字技术和因特网的发展，各种形式的多媒体数字作品(图像、视频、音频等)纷纷以网络形式发表，然而数字作品的便利性和不安全性是并存的，它可以低成本、高速度地被复制和传播，这样就为创造者和使用者都提供了很大的便利，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十分迫切的工作。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本身的特点为其提供技术上的保护。数字水印技术的研究就是在这种应用要求下迅速发展起来的。

数字水印是一种有效的数字产品版权保护和数据安全维护技术，是信息隐藏技术研究领域的一个重要分支。它将具有特定意义的标记(水印)，利用数字嵌入的方法隐藏在数字图像、声音、文档、图书、视频等数字产品中，用以证明创作者对其作品的所有权，并作为鉴定、起诉非法侵权的证据，同时通过对水印的检测和分析来保证数字信息的完整可靠性，从而成为知识产权保护和数字多媒体防伪的有效手段。在本文中，我们将待嵌入水印的数字产品称为掩体对象或载体，将嵌入水印后的数字产品称为隐藏对象或含水印载体。

数字水印技术除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。例如，从信息安全的保密角度而言，如果隐藏的信息被破坏掉，系统可以视为安全的，因为秘密信息并未泄露；但是，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，从而失去了版权保护的功能，这一系统就是失败的。因此数字水印技术必须具有较强的稳健性、安全性和透明性，这些特性我们将在后续章节介绍。

在现实生活中，以下几个引起普遍关注的问题构成了数字水印的研究背景[1-4]。

1. 数字作品的知识产权保护

数字作品(如电脑美术、扫描图像、数字音乐、视频、三维动画)的版权保护是当前的热点问题，而对数字作品的版权保护可能是水印最主要的应用。由于数字作品的拷贝、修改非常容易，而且可以做到与原作完全相同，所以原创者不得不采用一些严重损害作品质量的办法来加上版权标志，而这种明显可见的标志很容易被篡改。

数字水印利用数据隐藏原理使版权标识不可见或不可听，既不损害原作品质量，又达到了版权保护的目的，这种应用要求非常高的稳健性。包含很多图像和数字音乐的因特网站是该应用的推动力量，网站所含的这些图像和音乐是可随意使用的，但是它们的所有者却要保护它们。目前，用于版权保护的数字水印技术已经进入了初步实用化阶段，IBM 公司在其“数字图书馆”软件中就提供了数字水印功能，Adobe 公司也在其著名的 Photoshop 软件中集成了 Digimarc 公司的数字水印插件。然而实事求是地说，目前市场上的数字水印产品在技术上还不成熟，很容易被破坏或破解，距离真正的实用还有很长的路要走。

2. 商务交易中的票据防伪

随着高质量图像输入/输出设备的发展，特别是精度超过 1200 dpi 的彩色喷墨、激光打印机和高精度彩色复印机的出现，使得货币、支票以及其他票据的伪造变得更加容易。

据美国官方报道，仅在 1997 年截获的价值 4000 万美元的假钞中，用高精度彩色打印机制造的小面额假钞就占 19%，这个数字是 1995 年的 9.05 倍。目前，美国、日本以及荷兰都已开始研究用于票据防伪的数字水印技术。其中麻省理工学院媒体实验室受美国财政部委托，已经开始研究在彩色打印机、复印机输出的每幅图像中加入惟一的、不可见的数字水印，在需要时可以实时地从扫描票据中判断水印的有无，快速辨识真伪。

另一方面，在从传统商务向电子商务转化的过程中，会出现大量过渡性的电子文件，如各种纸质票据的扫描图像等。即使在网络安全技术成熟以后，各种电子票据也还需要一些非密码的认证方式。数字水印技术可以为各种票据提供不可见的认证标志，从而大大增加了伪造的难度。

3. 声像数据的隐藏标识和篡改提示

数据的标识信息往往比数据本身更具有保密价值，如遥感图像的拍摄日期、经/纬度等。没有标识信息的数据有时甚至无法使用，但直接将这些重要信息标记在原始文件上又很危险。数字水印技术提供了一种隐藏标识的方法，标识信息在原始文件上是看不到的，只有通过特殊的阅读程序才可以读取。这种方法已经被国外一些公开的遥感图像数据库所采用。

此外，数据的篡改提示也是一项很重要的工作。现有的信号拼接和镶嵌技术可以做到“移花接木”而不为人知，因此，如何防范对图像、录音、录像数据的篡改攻击是重要的研究课题。基于数字水印的篡改提示是解决这一问题的理想技术途径，通过隐藏水印的状态可以判断声像信号是否被篡改。

2.2　数字水印基本框架

从信号处理的角度看，嵌入载体对象的水印信号可以视为在强背景下叠加一个弱信号，只要叠加的水印信号强度低于人视觉系统(HVS)对比度门限或听觉系统(HAS)对声音的感知门限，HVS 或 HAS 就无法感知到信号的存在。由于 HVS 和 HAS 受空间、时间和频率特性的限制，因此通过对载体对象作一定的调整，就有可能在不引起人感知的情况下嵌入一些信息。

从数字通信的角度看，水印嵌入可理解为在一个宽带信道(载体对象)上用扩频通信技术传输一个窄带信号(水印)。尽管水印信号具有一定的能量，但分布到信道中任一频率上的能量是难以检测到的。水印的译码(检测)则是一个有噪信道中弱信号的检测问题。

下面我们根据 Voyatzis 和 Pitas[5]提出的思想，对数字水印的基本框架进行介绍。

尽管数字水印有各种形式，通常我们可以定义水印为如下的信号 W

$$W = \{w(k) \mid w(k) \in U,\ k \in \hat{W}^d\} \tag{2-1}$$

这里，$\hat{W}^d$ 表示维数为 d 的水印信号域，$d=1, 2, 3$ 分别表示声音、静止图像和视频中的水印。水印信号可以是二值形式($U=\{0,1\}$或$U=\{-1,1\}$)或高斯噪声形式。有时称 W 为

“原始水印”，以便把它和变换域水印形式 $F(W)$（这种形式的水印往往在许多水印嵌入和检测算法中出现）区分开来。

水印处理系统的基本框架可以定义为六元体($\boldsymbol{X}$, $\boldsymbol{W}$, $\boldsymbol{K}$, $\boldsymbol{G}$, $\boldsymbol{E}$, $\boldsymbol{D}$)，其中：

(1) $\boldsymbol{X}$ 代表所要保护的数字产品 X 的集合。

(2) $\boldsymbol{W}$ 代表所有可能水印信号 W 的集合。

(3) $\boldsymbol{K}$ 是标识码（也称为水印密钥）的集合。

(4) $\boldsymbol{G}$ 表示利用密钥 $\boldsymbol{K}$ 和待嵌入水印的 $\boldsymbol{X}$ 共同生成水印的算法，即

$$\boldsymbol{G}: \boldsymbol{X} \times \boldsymbol{K} \rightarrow \boldsymbol{W}, W = G(X,K) \tag{2-2}$$

(5) $\boldsymbol{E}$ 表示将水印 $\boldsymbol{W}$ 嵌入数字产品 X_0 中的嵌入算法，即

$$\boldsymbol{E}: \boldsymbol{X} \times \boldsymbol{W} \rightarrow \boldsymbol{X}, X_w = E(X_0, W) \tag{2-3}$$

这里，X_0 代表原始的数字产品，X_w 代表嵌入水印后得到的数字产品。

(6) $\boldsymbol{D}$ 表示水印检测算法，即

$$\boldsymbol{D}: \boldsymbol{X} \times \boldsymbol{K} \rightarrow \{0,1\} \tag{2-4}$$

$$D(X,K) = \begin{cases} 1, & \text{如果 } X \text{ 中存在 } W(H_1) \\ 0, & \text{如果 } X \text{ 中不存在 } W(H_0) \end{cases} \tag{2-5}$$

这里，H_1 和 H_0 代表二值假设，分别表示水印的有无。

我们再引入两个基本定义：

(1) 感知相似性：设数字产品 $X,Y \in \boldsymbol{X}$，则符号 $X \sim Y$ 表示 X 和 Y 具有相同的感知形式。而符号 $X \neq Y$ 表示 X 和 Y 是完全不同的数字产品，或表示 Y 是相对于 X 质量下降的数字产品。

感知相似性通常是以人类知觉系统的主观标准为基础的。但是，客观误差估计也可以用来确定感知相似性。

(2) 水印等价性：若水印 W_1 和 W_2 满足

$$D(X,W_1) = 1 \Rightarrow D(X,W_2) = 1 \tag{2-6}$$

则称 W_1 和 W_2 是等价的，表示为 $W_1 \cong W_2$。

通常情况下，水印的等价性是指水印间的高度相关性。显然，相同的水印是等价的。反之不然，等价的水印可能相差很大。

水印处理系统的基本框架必须满足一些特定的条件，以便形成一套适用于版权保护和产品内容鉴定的值得信赖的根据，这些基本条件是：

(1) 不可感知性：对于不可见水印处理系统，水印嵌入算法不应产生可感知的数据修改，也就是加水印后的产品必须相似于原始产品，即 $X_0 \sim X_w$。

(2) 密钥惟一性：不同密钥应产生不等价的水印，即对于任何产品 $X \in \boldsymbol{X}$ 和 $W_i = G(X,K_i)$，$i=1,2$，满足 $K_1 \neq K_2 \Rightarrow W_1 \neq W_2$。

(3) 水印有效性：在水印处理算法中只采用有效的水印。对于特定的产品 $X \in \boldsymbol{X}$，当且仅当存在 $K \in \boldsymbol{K}$ 使得 $G(X,K) = W$，则称水印 W 是有效的。

(4) 不可逆性：函数 $W = G(X,K)$ 应该是不可逆的，即 K 不能根据 W 和函数 G 逆推出来。不满射的函数 G 直接满足这个条件，但这在水印处理算法中并不是必要条件。在实际应用中，不可逆意味着对于任何水印信号 W，很难再找到另一个与 W 等价的水印信号。

(5) 产品依赖性：在相同的密钥条件下，当水印算子 $\boldsymbol{G}$ 用在不同的产品时，应该产生不同的水印信号。即对于任何特定的密钥 $K\in\boldsymbol{K}$ 和任何 $X_1,X_2\in\boldsymbol{X}$，满足 $X_1\neq X_2\Rightarrow W_1\neq W_2$，其中 $W_i=G(X,K_i)$，$i=1,2$。

(6) 多重水印：通常对已嵌入水印信号的产品用另一个不同的密钥再作水印嵌入是可能的。这也往往是盗版者或侵权者在重销时可能做的工作。但在某些场合，利用这种特性可以对产品的发布渠道进行跟踪。若 $X_i=E(X_{i-1},W_i)$，$i=1,2,\cdots$，那么对于任何 $i\leqslant n$，原始水印必须在 X_i 中还能检测出来，即 $D(X_i,W_1)=1$，这里 n 是一个足够大的整数，使得 $X_n\sim X_0$，而且 $X_{n+1}\neq X_0$。

(7) 检测可靠性：肯定检测的输出必须有一个合适的最小的置信度。如果 P_{fa} 是检测的虚警概率，则它满足 $P_{\text{fa}}<P_{\text{thres}}$，这里 P_{thres} 是产品供应者所选择的合适的概率阈值。

(8) 稳健性：设 X_0 是原始的产品，而 X_{w} 是加水印的产品，并且 $D(X_{\text{w}},W)=1$，M 是一个多媒体数据处理操作算法，则对于任何 $Y\sim X_{\text{w}}$，$Y=M(X_{\text{w}})$ 满足 $D(Y,W)=1$，而且对于任何 $Z=M(X_0)$，满足 $D(Z,W)=0$。

(9) 计算有效性：水印处理算法应该比较容易用软件或硬件实现。尤其需要注意的是，水印检测算法对某些应用(比如产品发行网络上对多媒体数据进行监视)来说必须足够快。

以上介绍了通用水印框架的基本要素和它在通常情况下需要满足的一些基本条件，在实际应用中，一个完整水印系统的设计必然包括水印的生成、嵌入和提取三部分。

1) 水印生成

水印信号的产生通常基于伪随机数发生器或混沌系统。产生的水印信号 W 往往需要进一步的变换以适应水印嵌入算法。为了分析方便，我们把算子 $\boldsymbol{G}$ 分解为算法 $\boldsymbol{R}$ 和算法 $\boldsymbol{T}$ 两个部分：

$$\begin{gathered}\boldsymbol{G}=\boldsymbol{T}\circ\boldsymbol{R}\\ \boldsymbol{R}:\boldsymbol{K}\to\widetilde{\boldsymbol{W}},\ \boldsymbol{T}:\widetilde{\boldsymbol{W}}\times\boldsymbol{X}\times\boldsymbol{K}\to\boldsymbol{W}\end{gathered}\tag{2-7}$$

子算法 $\boldsymbol{R}$ 输出原始水印 $\widetilde{W}\in\widetilde{\boldsymbol{W}}$，该原始水印只由密钥 $K\in\boldsymbol{K}$ 产生。当 $\boldsymbol{R}$ 基于伪随机数发生器时，密钥 $\boldsymbol{K}$ 直接映射为伪随机数发生器的种子。当 $\boldsymbol{R}$ 基于混沌系统时，密钥集由许多初始条件的适当变换而产生。这两种方法所产生的密钥集足够大并且满足密钥惟一性条件，而且由 $\boldsymbol{R}$ 产生的水印是有效的水印。此外，$\boldsymbol{R}$ 是不可逆的。

子算法 $\boldsymbol{T}$ 对原始水印进行修改以获得最后的依赖于产品的水印 $\boldsymbol{W}$。$\boldsymbol{T}$ 应满足：

$$\boldsymbol{T}(\widetilde{W},X_0)\cong\boldsymbol{T}(\widetilde{W},X_{\text{w}})\cong\boldsymbol{T}(\widetilde{W},X'_{\text{w}})\tag{2-8}$$

这里 X_0 表示原始产品，而 X_{w} 表示嵌入水印的产品，并且 $X'_{\text{w}}=M(X_{\text{w}})$，$X'_{\text{w}}\sim X_{\text{w}}$，$M$ 表示多媒体数据处理操作算法。在这里需要指出的是原始水印信号也可以预先指定，而在嵌入水印前对该水印信号可以做适当的变换或者不做变换，密钥可以在水印嵌入过程中产生。

2) 水印嵌入

水印的嵌入过程如图 2-1 所示。

水印嵌入就是把水印信号 $W=\{w(k)\}$ 嵌入到原始产品 $X_0=\{x_0(k)\}$ 中，一般的水印嵌入规则可描述为

$$x_{\text{w}}(k)=x_0(k)\oplus h(k)w(k)\tag{2-9}$$

其中⊕为某种叠加操作，也可能包括合适的截断操作或量化操作。$H=\{h(k)\}$ 称为 d 维