信息安全国家重点实验室信息安全丛书

数字水印原理与技术

王　颖　肖　俊　王蕴红　编著

国家高技术发展计划项目(项目编号:2003AA144080)

科学出版社

北　京

内 容 简 介

本书从技术角度对数字水印的基本状况、理论模型、主流算法、性能、检测技术和典型应用进行了全面介绍，对水印研究应用中遇到的主要问题进行了系统阐述，并辅以丰富的例子，还在附录部分给出了主要算法的源代码。此外，书中对数字水印技术的主要产品和实际应用案例进行了介绍。

本书可作为高等院校信息与通信工程、计算机科学与技术等专业高年级本科生和研究生的教材或参考书，也可供从事信息安全和数字版权管理的有关人员阅读。

图书在版编目(CIP)数据

数字水印原理与技术/王颖，肖俊，王蕴红编著 .—北京：科学出版社，2007

(信息安全国家重点实验室信息安全丛书)

ISBN 978-7-03-018530-3

Ⅰ.数… Ⅱ.①王…②肖…③王… Ⅲ.电子计算机－密码术

Ⅳ.TP309.7

中国版本图书馆 CIP 数据核字(2007)第 015566 号

责任编辑：鞠丽娜/责任校树：赵 燕

责任印制：吕春珉/封面设计：王 浩

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

CB 印刷

科学出版社发行 各地新华书店经销

*

2007 年 3 月第 一 版 开本：B5(720×1000)

2007 年 3 月第一次印刷 印张：15 1/2

印数：1—3 500 字数：309 000

定价：31.00 元

(如有印装质量问题，我社负责调换〈科印〉)

销售部电话 010-62136131 编辑部电话 010-62138978-8002(BI08)

《信息安全国家重点实验室信息安全丛书》编委会

序　言

人类的进步得益于科学研究的突破、生产力的发展和社会的进步。

计算机、通信、半导体科学技术的突破，形成了巨大的新型生产力。数字化的生活方式席卷全球。农业革命、工业革命、信息革命成为人类历史生产力发展的三座丰碑。古老的中华大地，也正在以信息化带动工业化的国策下焕发着青春。电子政务、电子商务的各种信息化应用之花，在华夏沃土上竞相开放，炎黄子孙们在经历了几百年的苦难历程后，在国家崛起中又迎来了一个运用勤劳和智慧富国强民的新契机。

科学规律的掌握，非一朝一夕之功。治水、训火、利用核能都曾经经历了非常漫长的岁月。不掌握好科学技术造福人类的一面，就会不经意地释放出它危害人类的一面。

生产力的发展，为社会创造出许多新的使用价值。但是，工具的不完善，会限制这些使用价值的真正发挥。信息化工具也和农业革命、工业革命中人们曾创造的许多工具一样，由于人类认识真理和实践真理的客观局限性而存在许多不完善的地方，从而形成信息系统的漏洞，造成系统的脆弱性，在人们驾驭技能不足的情况下损害着人们自身的利益。

世界未到大同时，社会上和国际间存在着竞争、斗争、战争和犯罪。传统社会存在的不文明、暴力，在信息空间也同样存在。在这个空间频频发生的和被有些人利用系统存在的脆弱性运用其“暴智”来散布计算机病毒，制造拒绝服务的事端，甚至侵入他人的系统，盗窃资源、资产，以达到其贪婪的目的。人类运用智慧开拓的信息疆土正在被这些暴行蚕食破坏着。

随着信息化的发展，信息安全成为全社会的需求，信息安全保障成为国际社会关注的焦点。因为信息安全不但关系国家的政治安全、经济安全、军事安全、社会稳定，也关系到社会中每一个人的数字化生存的质量。

信息革命给人类带来的高效率和高效益是否真正实现，取决于信息安全是否得以保障。什么是信息安全？怎样才能保障信息安全？这些问题都是严肃的科学和技术问题。面对人机结合和非线性、智能化的复杂信息巨系统，我们还有许多科学技术问题需要认真研究。我们不能在研究尚处肤浅的时候，就盲目乐观地向世人宣称，我们拥有了全面的解决方案；我们也不能因为面对各种麻烦，就灰头土脸，自暴自弃，我们需要的是革命的乐观主义精神、坚忍不拔的奋勇攀登科学技术高峰的坚定信念。

人是有能力认识真理的，今天对信息安全的认识，就经历了一个从保密到保护，又发展到保障的趋近真理的发展过程。因为信息安全的问题不仅仅是因为技术原因引起的，它涉及人、社会和技术等因素，因此，仅仅靠技术是不能有效地实施信息安全保障的。从社会学的观点来看，只有依靠有信息安全觉悟和技能的人及科学有效的管理来实施综合的技术保障手段，才能取得良好的效果。

为了推动我国信息化发展的进程，信息安全国家重点实验室组织编写了《信息安全国家重点实验室信息安全丛书》。在本丛书的编写过程中，我们既注重学术水平，又注意其实用价值。本丛书从信息安全保障体系、操作系统安全、数据库安全、网络安全、无线网络安全、网络攻击、密码技术、PKI 技术、信息隐藏、安全协议、安全事件应急响应、量子密码通信等多个角度，分析和总结信息安全的科学问题以及信息安全保障的理论与技术，因此，这套丛书有较大的适用范围。我们将努力把国内外信息安全的最新研究成果写进书中，以使读者阅读本丛书后在理论、方法、技术上得到新的启发和收获，从而切实解决工作中的实际问题。

本丛书的组织方式是开放式的，今后将根据学科发展陆续组织出版信息安全领域的优秀图书。

信息安全只能是相对而言，它是动态发展的。任何人都不能宣称自己终极了对信息安全的认识。让我们一起努力，不断地深化自己的研究，借鉴国外先进的科学技术，结合国情，与时俱进地推出信息安全保障的新理论、新办法和新手段，用我们的智慧保卫我们的信息疆土，使我们的信息家园尽量祥和安宁。

限于作者的水平，本丛书难免存在不足之处，敬请读者批评指正。

《信息安全国家重点实验室信息安全丛书》编委会

2003 年 7 月

前　言

随着互联网的飞速发展以及媒体资源的数字化，数字作品如图像、音频、视频和文件等的盗版问题突现，使得数字水印技术成为重要的研究热点，并引起了信息安全领域、计算机技术领域和信息处理领域学者的广泛关注。

数字水印是一种将可识别的数据嵌入到数字作品中的技术，用人类感觉器官（如眼、耳）无法识别，而使用专门的检测软件则可以方便地识别。数字水印是数字内容的唯一标识，即使数字内容经过拷贝、编辑处理、压缩/解压缩、加密/解密或广播等操作，数字水印仍能保持不变，同时数字水印的存在对数字作品质量没有影响。正是由于数字水印的这些特点，它已经成为数字媒体版权保护的重要手段之一。

数字水印从正式提出到现在的十几年间，已经成为了学术界和国内外一些大公司关注的焦点。从 1994 年开始，国际学术界陆续发表有关数字水印的文章，且文章数量呈快速增长趋势，几个有影响的国际会议（如 IEEE ICIP、IEEE ICASSP、ACM Multimedia 等）以及一些国际权威杂志（如 Proceedings of IEEE、Signal Processing、IEEE Journal of Selected Areas on Communication、Communications of ACM 等）相继出版了数字水印的专辑。国外已有一些著名大学和研究机构，如美国的 MIT 大学、Purdue 大学、IBM 研究所，英国的剑桥大学，德国的 Erlangen Nuremberg 大学以及日本的 NEC 研究所等都已开展了该项技术的研究，并取得了一定的成果。一些公司相继推出了数字水印的软件产品，具有代表性的有美国的 Digimarc 公司、Alpha 公司、MediaSec 技术公司、Verance 公司、Activated Content 公司，英国的 Signum 技术公司，以色列的 Aliroo 公司，荷兰的 Philips 公司研发中心和瑞士的 Alpvision 公司等。此外，IBM 公司和 Microsoft 公司等都在数字水印的应用方面进行了研究。

到目前为止，数字水印从研究对象上看主要涉及图像水印、视频水印、音频水印、文本水印和三维网格数据水印等几个方面，其中大部分的水印研究和论文都集中在图像研究上，其原因在于图像是最基本的多媒体数据，且互联网的发展为图像水印提供了直接大量的应用需求。近几年关于视频水印和音频水印的研究呈上升趋势。数字水印的基础研究主要集中在数字水印理论模型、鲁棒水印算法、水印系统性能分析等方面。数字水印应用研究的大部分工作致力于寻求同时满足保真度、鲁棒性和经济约束的平衡点。数字水印的主要应用方向包括数字版权保护、广播监视、内容认证、使用控制、隐蔽通信和电子商务等方面。

随着技术交流的加快和水印技术的迅速发展，国内的一些研究单位也逐步从技术跟踪转向深入的系统研究，从1999年开始的六届“全国信息隐藏及多媒体信息安全学术研讨会”都有数字水印专题。2000年1月，由国家863计划智能计算机专家组织召开了“数字水印技术学术研讨会”，会上20多个学术报告反映了我国学术界和应用部门对这一问题的浓厚兴趣。目前在国内出版的关于数字水印技术方面的书籍有十余种，它们分别从不同的角度对数字水印的算法及特性进行了介绍。本书是为从事水印研究和应用的工作者介绍数字水印的基本原理和关键技术，目的是分析和总结水印的理论框架和该领域的最新研究成果，为进一步研究和应用水印技术提供帮助。

本书从数字水印技术的角度对数字水印的基本状况、数字水印的理论模型、数字水印的算法设计、数字水印系统的性能分析、数字水印的检测和水印的典型应用进行了系统全面的介绍，全书共包括6章。第1章对数字水印的发展历史、基本原理、特性、分类和典型的攻击方法进行了介绍；第2章介绍了数字水印系统的理论模型，重点介绍了基于通信理论的水印模型，对其中的基于边信息的水印系统模型进行了分析，包括含边信息的嵌入、含边信息的编码和基于人类感知模型的含边信息的水印系统，给出各类系统的原理和特性；第3章介绍了几类主流的数字水印嵌入算法，比较和分析了各种算法的性能；第4章对数字水印系统的信道容量、保真度和鲁棒性等性能进行了分析，对第2章介绍的模型容量进行了分析，对第3章介绍的典型算法的鲁棒性进行了比较，此外还介绍了几何失真鲁棒性；第5章介绍了数字水印的检测技术，包括通用盲检测和有针对性的信息隐藏检测；第6章综述介绍了数字水印的应用情况，同时给出了三个数字水印的应用案例。

本书同已有的有关数字水印方面的专著相比具有如下特点：

1）内容安排合理，系统性强。本书先给出系统模型，让读者对水印有一个基本的认识，然后给出具体的算法，并对采用这些算法的水印系统性能进行分析，使读者对算法有一个比较清楚的了解，最后对数字水印的应用进行全面介绍，同时给出几个应用案例。

2）理论性强。本书利用通信原理和信息论对数字水印系统进行建模和性能分析，对数字水印技术的进一步研究和实际系统设计将有一定的指导意义。

3）从一种新的视角对水印算法进行分类，且全面研究水印算法性能。书中对典型算法经过各种信号处理后以及不同变化域中算法的鲁棒性进行了比较，对实验结果给出了详细的说明，并附有各种算法的源程序。

4）本书给出了目前的典型应用系统的案例，介绍了应用系统的原理、框架和效果，对其他应用系统的设计具有借鉴作用。

本书由中国科学院研究生院王颖教授主持编著和审校。中国科学院研究生院肖俊博士执笔第3章，参与了第1章、第2章、第4章、第6章的写作，并提供了书

中各类算法的源程序；北京航空航天大学王蕴红教授负责第 5 章的写作；中国科学院研究生院黄志蓓老师负责第 2 章的写作；北京航空航天大学洪飞博士参与了第 4 章的写作。

此外，中国科学院研究生院计算与通信工程学院袁大洋同学、钱洪宝同学、张弘同学和李峥同学为本书的写作提供了源程序和研究结果，在此致谢。同时，还要感谢上海阿须数码技术有限公司为本书提供了应用案例。

本书的出版得到了国家高技术发展计划项目(编号：2003AA144080)的资助，在此致谢。此外，感谢信息安全国家重点实验室对本书的出版所给予的大力支持，特别感谢冯登国教授在本书写作的整个过程中所给予的指导和关心。

由于作者水平有限，书中难免有不妥之处，敬请读者批评指正。

作　者

2006 年夏于北京

目　录

第1章 绪 论

1.1 引 言

随着数字时代的到来,媒体内容的形式逐渐由模拟向数字转变,而模拟内容和数字内容的本质区别主要体现在以下三个方面:

1) 模拟内容和介质是紧密相连的,而数字内容和介质无关;

2) 数字技术可以有效地克服内容短缺,复制非常简单,不会降低内容质量,而且内容传输需要的带宽较低;

3) 数字技术大大促进了新商务模式的产生和发展。

数字技术使多媒体信息(图像、文本、音频和视频等)的存储、复制与传播变得非常方便。人们不但可以通过互联网和 CD-ROM 方便快捷地获得多媒体信息,还可以得到与原始数据完全相同的复制品,而对模拟信息的每一次拷贝都会存在不同程度上的失真,图 1.1 展示了这样一个过程。但是由此引发的盗版问题和版权纷争也成为日益严重的社会问题。据美国唱片行业协会估计,全世界每年因盗版而造成的经济损失高达 50 亿美元;美国电影行业协会估计,盗版使美国电影业的年收入减少了 25 亿美元。

现有版权保护系统多采用密码认证技术如 DVD 光盘的安全密码。然而,遗憾的是,仅仅采用密码技术并不能完全解决版权保护问题,密码技术仅能在数据从发送者到接收者的传输过程中进行数据的加密保护,它并不能帮助销售者监视合法用户如何处理解密后的内容。这样,盗版者可以购买产品,使用密钥获取无保护的内容副本,然后继续发行非法副本。换言之,密码技术只能保护传输中的内容,内容一旦被解密就不再具有保护作用了。

为了解决密码技术在数据保护方面的不足,一种新的有效的数字版权保护和数据安全维护技术——数字水印技术得到了发展。与钞票水印类似,这是一种将特殊的不可见标记,利用数字内嵌的方法嵌入在数字媒体(图像、声音、文档和视频等)中,它可以用于证明原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,同时可以通过对水印的检测和分析保证数字信息的完整性,从而成为知识产权保护和数字多媒体防伪的有效手段。

虽然版权保护和防止拷贝是水印技术发展的源动力和主要驱动力量,但是目前在很多其他应用中也都在使用或者建议使用水印技术。这些应用包括广播监

视、操作跟踪、数字认证、拷贝控制和设备控制等。

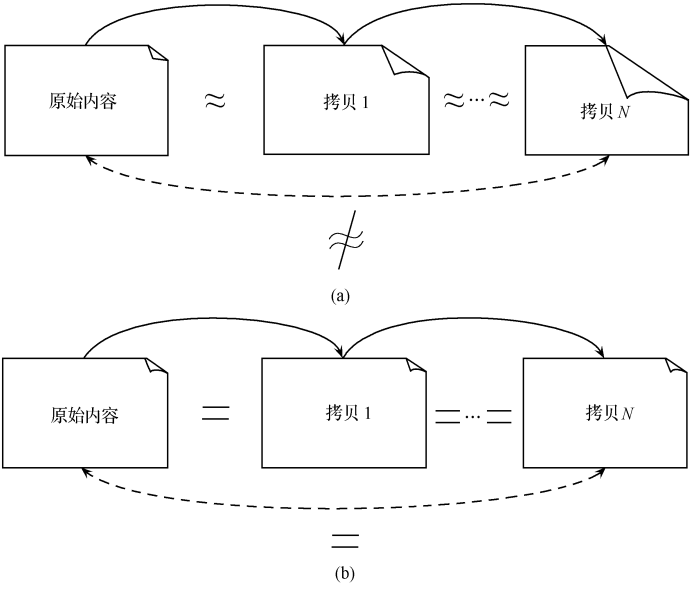


图 1.1 模拟形式内容与数字形式内容的拷贝效果

(a) 模拟形式内容的有损拷贝;(b) 数字形式内容的无损拷贝

由于这样的一些应用,数字水印技术是当前多媒体信息安全研究领域发展最快的热点技术之一,已经受到国际学术界和企业界的高度关注。数字水印技术是一门新兴的多学科交叉的应用技术,它涉及不同学科领域的理论和技术,如信号处理、图像处理、信息论、编码理论、密码学、检测理论、数字通信和网络技术等。水印技术的发展在一定程度上也带动了这些相关领域的进一步发展。因此,无论从理论角度还是应用角度来看,开展对数字水印技术的研究,不但具有重要的学术意义,还具有极为重要的实用价值。

1.2 数字水印发展的历史与现状

大约在 700 年前,在手工造纸技术中出现了纸张上的水印。尽管中国在一千多年前就发明了造纸术,但是纸水印直到 1282 年才在意大利出现。这些水印是通过在纸模中加上细线模板制造出来的。纸在存在细线的区域会略薄一些,这样也会更透明些。这种带水印的纸起源于意大利 Fabriano 的一个城镇[1],该城镇在造纸工业发展中扮演了重要的角色。在 13 世纪末,大约有 40 家造纸厂共享Fabriano

的纸业市场,并生产具有不同式样、质量和价格的纸。那时造纸厂生产的生纸表面粗糙,不适合直接使用。这种生纸材料被送给其他工匠,他们利用一种叫研光机的硬石块将纸表面弄光滑,接着经过处理的纸张被清点、折叠,最后卖给商人。这些商人将它们存放在大仓库中以备转卖,以获取高额利润。不但40家造纸厂之间的竞争很激烈,工匠之间以及商人之间的竞争也很激烈。对任何一方来说,跟踪纸的来源以及对式样和质量进行鉴定都不是一件容易的事。水印的使用是一种完美的解决方法,它能消除任何可能的冲突。因此,那时水印主要用于识别生产纸张的工厂,作为保证纸张质量的一种手段。

将近18世纪末期,"水印"这个术语似乎已经形成,它可能起源于德国词汇wassermarke。这个术语其实是一个误称,因为在水印造纸中水并不是特别重要。可能是因为水印有类似于水在纸上的效果,就形成了这个词。

大概在"水印"这个术语形成的同时,伪币制造者开始开发一种技术,来伪造用于纸币防伪的水印。而伪造促进了水印技术的发展。英国人威廉·康格里夫发明了一种制造有色水印的技术,方法是在造纸币的过程中把经过染色的物质插入到纸币中。

1954年,出现了第一个与"数字水印"方法类似的技术实例。当时,美国Muzac公司的Emil Hembrooke申请了一项名为"Identification of Sound and Like Signals"的专利。该专利描述了一种将标识码不可感知地嵌入到音乐中而证明所有权的方法。这是迄今为止所知道的最早的电子水印(electronic watermarking)技术。此后,一些水印技术被提出并根据不同的应用而得以发展。但是,直到20世纪90年代初期术语"数字水印"才真正流行起来。

随后,数字水印进入了其飞速发展时期,其进展体现在基础研究领域和应用研究领域。下面我们首先对水印技术发展的历史进行简单介绍,然后分析当前水印技术的现状和未来的发展趋势。

1.2.1 数字水印发展的历史

早期,关于数字水印的研究只是探索性的,出现的成果主要是各种水印算法。但是随着大量水印算法的出现,水印的研究状况开始改变。从20世纪90年代后期开始,对水印的研究更加深入,更重要的进展可能更多地体现在日益准确的水印模型上。

(1) 数字水印算法的发展

早期的数字水印算法主要在空域实现,而且大都针对图像进行研究。1993年,Tirkel等[2]发表了一篇文章,他们首先提出了电子水印的说法,而随后发表的另一篇文章[3]则正式提出了"数字水印"这一概念。当时,他们已经意识到了数字水印的重要性,指出了一些可能的应用,并针对灰度图像提出了两种在图像的最低有效位中添加水印的方案,这些方案将在3.2.1节进行详细介绍。

为了提高水印的鲁棒性,1996 年 Cox 等[4]提出了一种基于扩频通信思想的水印方案。该方案相对于空域算法具有较好的鲁棒性,已经成为数字水印技术中一个比较经典的方案。但它也存在一些缺陷,其中最重要的一点就是提取水印信息时必须有原始图像的参与。我们将在 3.3 节对此类方案进行详细介绍。

随后,Chen 等[5]于 1998 年提出了一类盲水印方案。该方案采用量化器来实现水印信息的嵌入,在容量和鲁棒性等方面都具有较好的性能,并已成为数字水印技术中一个比较典型的方案。我们将在 3.4 节对此类方案进行详细介绍。

在图像水印的发展过程中,音频、文本和视频水印也逐渐得到发展。关于音频水印技术的研究最早见于 1996 年,Bender 在文献[6]中提出了 LSB 编码、回声编码、扩频编码和相位编码等四种算法;Boney 等[7]将 Cox 等的扩频水印方案应用到音频信号中,取得了很好的实验结果。对文本水印的研究始于 1994 年,贝尔实验室的 Maxemchuk 首先提出在数字文档中嵌入标记的方法,用于保护电子出版物所有者的利益[8]。而视频水印的研究也始于 1994 年,当时 Matsui 等[9]提出了一种类似于图像水印的视频水印算法,它将视频信号的每一帧简单地视作图像进行处理。

此外,在图形和三维动画等载体中嵌入水印信息的水印算法也已有报道。本书在对数字水印进行介绍的过程中将以图像水印为主。

(2) 数字水印模型的发展

20 世纪 90 年代初期的基本水印模型是把水印系统看成某种通信信道,载体作品和传输过程中经历的各种失真和变换都被当做噪声。其不可感知性约束是通过在嵌入端施加全局能量限制来得到满足的。在这类早期系统中,嵌入的水印信号与载体作品无关,我们称之为盲嵌入[10]。此类模型将在 2.1 节进行详细介绍。

1999 年,文献[11]~[13]共同指出将水印系统看做带边信息的通信模式更为准确。这样的水印算法要用含辅助信息的嵌入器和检测器。因为加入的水印模板是载体作品的一个函数。在文献[14]~[17]中对这类水印模型有更精确的介绍。尤其是 Costa[17]在考察信道容量时,假设该信道有两个高斯白噪声源,且第一个噪声源已知。他把第一个噪声源比作脏纸,水印嵌入功率受限相当于在纸上书写信息的墨水数量有限;第二个噪声源未知,它相当于脏纸在传送过程中沾上的更多脏点;检测器对这两个噪声都是未知的。Costa 给出了令人惊奇的结果:信道容量与第一个噪声源无关。这个结论对水印研究有着深远的意义:如果把载体看做第一个已知的噪声源,那么就意味着采用恰当的编码,水印系统的容量将可能不依赖于载体。我们将在 2.2 节和 2.3 节对这一模型进行详细介绍。

使用水印技术不仅要传输信息,而且还必须要在保持载体的保真度的同时抵抗载体作品可能遇到的失真,因此通常系统的保真度和鲁棒性要求是矛盾的。如前所述,早期的水印系统利用全局能量限制来满足保真度约束。1995 年,研究指出为了满足保真度要求需要建立一个感知模型,该模型允许嵌入的水印信号根据

载体局部特性做相应的局部变化。大多数水印系统采用了各种感知模型后性能都比未采用感知模型的水印算法有所提高。这种基于感知模型的水印嵌入器是含辅助信息嵌入的早期模式。基于感知系统的模型将在2.4节进行介绍。

(3) 数字水印技术应用的发展

伴随水印基础理论研究的不断进步,许多公司和大学也在为推进水印实现的工程技术做出努力,并使其在很多实际场合得到了应用。这些应用设计主要关注如何满足保真度、鲁棒性和经济性约束条件。

水印的早期应用主要是版权保护,包括所有者鉴别、所有权验证、操作跟踪和拷贝控制。

所有者鉴别最早是由 Muzak 公司提出的[10]。他们的系统使用莫尔斯电码对认证信息进行编码,该系统使用持续时间可变的陷波滤波器来滤除 1kHz 的音频信号。该系统一直沿用到 20 世纪 80 年代早期 Muzak 公司改变其经营方向为止。

广播监视公司也常常使用这种嵌入信号的方式。纽约尼尔森媒体研究中心和泰勒纳尔逊旗下的竞争媒体报告机构都采用水印技术进行广告监视服务,这些系统都已使用了近 10 年。

随着水印技术的不断发展,水印的应用范围逐渐扩展。到目前为止,水印技术已经应用于数字版权保护、广播监视、内容认证、使用控制,隐蔽通信等诸多方面。1.6节和6.1节将对数字水印的主要应用领域和主要研究机构及其产品做更详细的介绍。

1.2.2 数字水印技术的发展现状与趋势

尽管在水印发展过程中出现了很多研究成果,但数字水印技术仍然是一个不成熟的研究领域,还有许多有意义的工作要完成。一方面,我们相信即将出现令水印研究界为之振奋的重要研究成果;另一方面,虽然尚未看到这一领域的突破性进展,但是这些重要的研究结果会推进水印在更大范围内的应用,值得我们深入研究下去。数字水印技术的现状和未来的发展趋势如下:

首先,含辅助信息的水印技术的出现是数字水印领域的一大进步。然而,含辅助信息的嵌入所采用的编码虽能满足计算效率,但对大尺度变换不够鲁棒,还需要深入研究,以寻找既有计算效率又有鲁棒性的编码。

其次,尽管很多论文都阐述了各种各样的算法,但还没有找到既能满足保真度又能满足鲁棒性要求的最佳的水印嵌入方法。我们期待这一研究领域硕果累累。

再者,盲检测器的几何和时间失真问题依然是没有解决的难点。不过,研究者们已经提出了许多不同的处理方法,并已取得了一定的进展。虽仍有不足,但对这一领域的深入研究显然会提高系统的鲁棒性。

最后,虽然并非所有的水印都有安全性要求,尤其是对于那些没有敌手攻击的

应用，而且大部分商业应用也只有很低的安全性要求。但设计既能允许公开检测器检测水印又能防止敌手去除水印的水印系统依然是一个开放的研究课题。众多研究者都在努力，希望设计出一个安全、通用的水印系统，但现有的水印系统还很容易受到攻击。能否实现这样的系统值得期待。

此外，数字水印技术在各个领域的进一步应用也是很多研究者关注的焦点之一，尤其是产业界的学者，我们期待数字水印技术能够在更多的领域得到应用。

1.3 数字水印的基本原理和框架

所谓数字水印，就是在数字媒体信息（如图像、声音、视频等）中添加某些数字信息，以便保护数字媒体的版权，证明产品的真实可靠性，跟踪盗版或者提供产品的附加信息。水印信息嵌入在载体文件中，不影响原始文件的可观性和完整性。

从信号处理的角度看，数字水印可以视为在载体对象的强背景下叠加一个作为水印的弱信号。从数字通信的角度看，数字水印可理解为在一个宽带信道（载体）上用扩频等通信技术传输一个窄带信号（水印）。但是，不论如何，粗略地讲，数字水印系统都包含水印嵌入器和水印检测器两大部分[18]。嵌入器至少具有两个输入量：一个是原始水印信息，它通过适当变换后作为待嵌入的水印信号；另一个就是要在其中嵌入水印的载体作品。水印嵌入器输出的含水印作品通常用于传播。而检测器的输入至少有一个量，即经过传输之后的作品，当然这取决于水印嵌入器，如果检测器在提取水印时需要原始载体或者原始水印，那么其输入还应该包括原始载体作品或原始水印。另外，在检测器端可以有两个操作，一个是水印检测，它用于判断水印的存在与否；另一个是水印提取，它用于从含水印的载体中提取水印信息，这与检测器的设计和应用场合有关。

图 1.2 所示为数字水印处理系统的基本框架。其中：

① $\boldsymbol{m}$——原始水印信息；

② $\boldsymbol{C}_o$——载体作品；

③ K——嵌入和提取水印时用到的密钥；

④ $\boldsymbol{W}$——经过预处理之后待嵌入的水印编码信息，如果原始信息没有经过处理，则 $\boldsymbol{W}=\boldsymbol{m}$；

⑤ $G(\cdot)$——水印预处理函数，$\boldsymbol{W}=G(\boldsymbol{m},\boldsymbol{C}_o,K)$或者 $\boldsymbol{W}=G(\boldsymbol{m},K)$，如果预处理过程中利用了载体 $\boldsymbol{C}_o$，则认为它是一个利用了边信息的过程，而 $G^{-1}(\cdot)$表示逆处理函数；

⑥ $\boldsymbol{S}$——嵌入水印之后的含水印作品；

⑦ $s(\cdot)$——水印嵌入函数，并且 $\boldsymbol{S}=s(\boldsymbol{W},\boldsymbol{C}_o)$；

⑧ $A(\cdot)$——攻击函数；

⑨ $\boldsymbol{Y}$——检测器接收到的待检测数据，并且 $\boldsymbol{Y}=A(\boldsymbol{S})$；

⑩ $D(\cdot)$——水印检测函数

$$D(Y,K)=\begin{cases}1 & \text{有水印}\\ 0 & \text{无水印}\end{cases}$$

⑪ $\hat{\boldsymbol{W}}$—— 从接收到的数据中提取出的水印编码信息；

⑫ $E(\cdot)$—— 水印提取函数，并且 $E(\boldsymbol{Y},K)=\hat{\boldsymbol{W}}$；

⑬ $\hat{\boldsymbol{m}}$—— 恢复的水印信息，且 $\hat{\boldsymbol{m}}=G^{-1}(\hat{\boldsymbol{W}},K,\boldsymbol{C}_o)$。

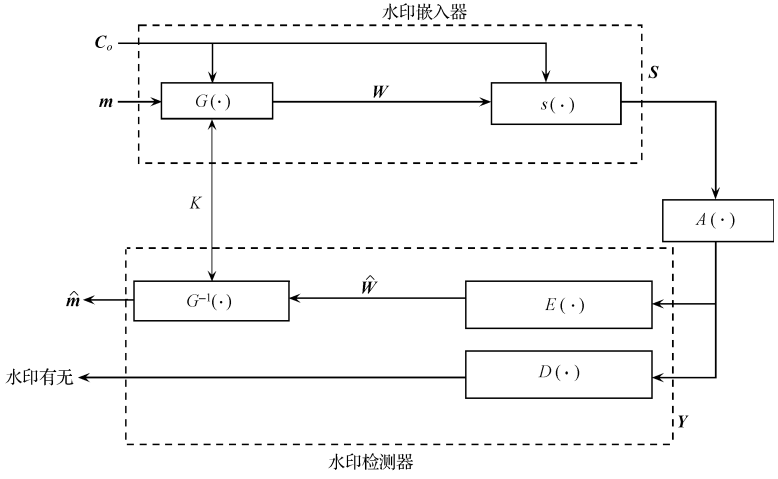


图 1.2 数字水印系统基本框架

此基本框架包含了数字水印系统的所有可能组成部分，以及各个部分之间的关系。在此基本框架下，演变出了很多具体的数字水印系统。例如，基于通信模型的数字水印系统、基于边信息的数字水印系统和基于矢量空间的数字水印系统等。这些系统模型将在第 2 章进行详细介绍。数字水印系统中的载体作品可以是图像、声音、视频等多种形式，但无论哪种载体形式其基本原理都是相同的。本书主要以数字图像为例介绍数字水印的基本原理和技术，对于不同的载体形式需要特别考虑的地方，我们将分别指出。

1.4 数字水印的特性和分类

1.4.1 数字水印的特性

数字水印有很多特性，其中最主要的三个特性是保真度、鲁棒性和容量。一般

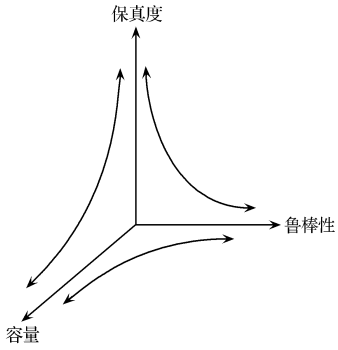


图 1.3 容量、鲁棒性和保真度之间的关系示意图

来说，容量、鲁棒性和保真度三者是相互制约的，不可能设计一个使三者都达到最优的水印系统，我们只能根据实际需要在三者中进行折中，其关系如图 1.3 所示。例如，在设计鲁棒水印时，一般在容量和保真度满足一定要求的情况，尽量提高系统的鲁棒性；而对载体图像的保真度要求较高时，系统的有效载荷或鲁棒性就不可能太高。下面对数字水印的保真度、鲁棒性和容量等特性进行介绍。

(1) 保真度

保真度(fidelity)是衡量信号在被处理前后的相似性，也称为不可感知性。载体作品在嵌入水印信息之后在感知上要达到一定的要求，这个要求并不一定是水印不可见或者可见，要根据水印的应用场合来确定。从水印是否可感知的角度来分，可以分为可见水印和不可见水印两类。例如，水印用于隐藏信息时要求不可见，如果作为可见标记使用时，则要求可见。但是本书主要讨论不可见水印，它一方面要求知觉上的不可见性，即因嵌入水印导致作品的变化对观察者的感知系统来讲应该是不可察觉的，最理想的情况是含水印作品与原始作品在知觉上一样；另一方面要求用统计方法也不能检测到水印，如针对大量的用同样方法嵌入水印的作品，使用统计方法无法提取水印或确定水印的存在。此外，也有研究者用嵌入水印之后的载体作品的质量(quality)来衡量水印这方面的特性。

(2) 鲁棒性

数字水印的鲁棒性(robustness)是指作品在经历了各种信号处理或者各种攻击后，数字水印的可提取性或可检测性。衡量数字水印这类性能的指标包括鲁棒性、脆弱性、有效性和安全性。鲁棒性是指在经过常规信号处理操作之后，水印系统仍能够检测到水印的能力。以图像载体为例，常见的操作包括空间滤波、有损压缩、打印和扫描，以及几何失真(旋转、平移和图像缩放等)。这些处理都是非恶意攻击，经过这些处理后水印仍能被检测到或提取出来，表明水印的鲁棒性强；脆弱性则相反，它要求水印系统尽量不具有鲁棒性，对作品的任何改动都可以通过检测水印来发现并准确定位；有效性是指嵌入水印之后的作品在不经受任何攻击的情况下，水印信息是否可以被有效检测或者提取；安全性则主要是指水印抵抗恶意攻击的能力，恶意攻击主要包括未经授权的删除、未经授权的嵌入和未经授权的检测。

(3) 容量

容量(capacity)也称嵌入率、加载率或者有效载荷，指的是在单位时间内或在一个作品中最多可以嵌入水印的比特数。一般要求水印容量尽量大，这样，一方面

可以嵌入尽量多的水印信息,另一方面当预嵌入的水印信息较少时,可以采用纠错编码等技术来减少提取水印的误码率。

除以上基本特征之外,在实际应用中,数字水印还应该尽量满足以下要求。

(1) 嵌入位置的安全性

指将水印信息嵌入于目标数据的内容之中,而非文件头等处,防止因格式变化而遭到破坏。

(2) 通用性

好的水印算法适用于多种文件格式和媒体格式。通用性在某种程度上意味着易用性。

(3) 计算效率高

水印算法应能用硬件或软件有效地实现。需要特别注意的是,水印检测算法的速度对分布式网络上的多媒体数据监视来说应该足够快。

1.4.2 数字水印的分类

数字水印的分类方法有很多种,不同的出发点导致了不同的分类,它们之间既有联系又有区别。最常见的分类方法包括以下几类。

(1) 按感知特性划分

根据水印特性可将水印分为可见水印和不可见水印。可见水印(visible watermark)是指知觉上可见的水印,就像插入或者覆盖在图像上的标识,它与可视的纸张中的水印相似。可见水印主要应用于图像和视频,比如用来可视地标识那些可在图像或视频数据库中得到的或在 Internet 上得到的图像或视频的预览来防止这些图像被用于不法商业用途。当然也可以用于音频中,即可听水印。比如,电台播放广告,广告商为了维护自己的权益,在录音带中加入某一特殊的声音,进而从播放的广告中检测这一声音出现的次数,可以知道电台是否执行了合同。

不可见水印(invisible watermark)是一种应用更加广泛的水印,与可见水印相反,它直观上是不可察觉的,但是当需要时,所有者可以从作品中提取出水印,从而证明该作品的所有权或者完整性等。不可见水印又可以分为脆弱水印和鲁棒水印两种。脆弱水印可以通过对水印的检测来判断载体是否已被修改或者进行了何种修改。而鲁棒水印则指加入了水印的作品在经历了非恶意攻击或一定失真内的恶意攻击后,水印仍可被提取的能力。

图 1.4 中(c)和(d)给出了以不可见方式和可见方式嵌入水印信息之后的含水印图像,(a)和(b)显示的是原始图像和原始水印信息。

(2) 按水印内容划分

按水印信息的内容可以将水印划分为有意义水印和无意义水印。有意义水印是指水印本身也是某种数字作品,如数字图像、数字视频片断或数字音频片段等,

如图 1.4(b)中所示的水印信息;无意义水印则只是对应于一串随机数。有意义水印的优势在于,如果由于受到攻击或其他原因致使解码后的水印破损,人们仍然可以通过直观观察或信号处理手段确认有无水印。但对于无意义水印来说,如果解码后的水印序列有若干码元错误,则只能通过统计决策来确定信号中是否含有水印。

(a)

(b)

(c)

(d)

图 1.4 可见水印与不可见水印示意图

(a) 原始图像;(b) 水印信息;(c) 以不可见方式嵌入水印之后的图像;
(d) 以可见方式嵌入水印之后的图像

(3) 按用途划分

不同的应用需求产生了不同的水印技术。按水印用途,我们可以将水印划分为数字版权管理水印、广播监视水印、内容认证水印和使用控制水印等,1.5 节和第 6 章将对这些应用进行更详细的介绍和分析。

(4) 按嵌入与提取中使用的密钥划分

类似密码术,根据嵌入和提取水印时使用的密钥不同可以将水印分为对称水印和非对称水印。当水印嵌入所使用的密钥 K_1 与水印提取或检测过程所使用的密钥 K_2 相同时,相应的水印(算法)称为对称水印(算法);当 K_1 与 K_2 不同时,相应的水印(算法)称为非对称水印(算法),如图 1.5 所示。

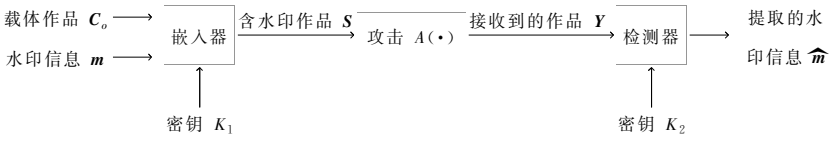


图 1.5 对称水印算法与非对称水印算法

(5) 按载体类型划分

按承载水印的载体类型,可以将水印划分为数字图像水印、数字音频水印、数字视频水印、文本水印和用于三维网格模型的网格水印等。随着数字技术的不断发展,会有更多种类型的数字媒体出现,同时也会产生相应载体的水印技术。

(6) 按水印检测器的类型划分

按水印检测器的类型来划分或者按水印的检测过程来划分,可将水印分为非盲水印、半盲水印和盲水印。非盲水印在检测过程中需要原始载体和原始水印的信息,如图 1.6 中开关 1 和开关 2 均闭合时的情况;半盲水印检测时则不需要原始载体信息,但是需要利用原始水印信息进行检测,如图 1.6 中开关 2 闭合而开关 1 打开的情况;盲水印检测时只需要密钥,不需要原始载体信息,也不需要原始水印信息,如图 1.6 中开关 1 和开关 2 均打开时的情况。

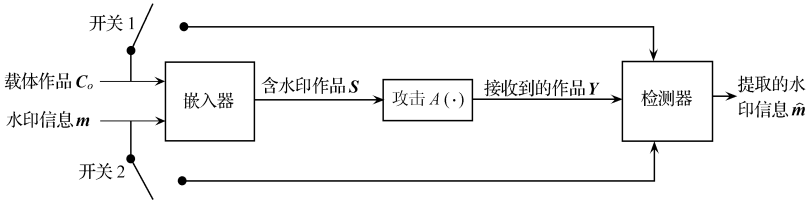


图 1.6 盲检测与非盲检测水印

(7) 按水印的嵌入域划分

按水印的嵌入位置,可以将其划分为时/空域水印和变换域水印,其中根据变换域的不同,可进一步分为离散余弦变换(discrete cosine transform,DCT)域水印、离散傅里叶变换(discrete Fourier transform,DFT)域水印和离散小波变换(discrete wavelet transform,DWT)域水印,以及哈德码变换域水印、Fresnel 变换域水印、Zernike 变换域水印和奇异值分解(singular value decomposition,SVD)域水印等。

时/空域水印是直接在载体信号的时间或空间域中叠加水印信息,如图 1.7(a)所示;而变换域水印则是在变换域中嵌入水印信息,如图 1.7(b)所示,此时,水印提取也应该在变换域进行。时(空)域水印算法在水印技术出现的早期研究的较多,一般具有复杂度低、实时性好等特色,但是鲁棒性较差,主要用于设计脆弱水印

或半脆弱水印;变换域水印算法的鲁棒性较强且容量较大,主要用于设计鲁棒水印,也可以与人类的知觉模型结合从而设计保真度好的水印。目前,针对变换域的水印算法研究较多。

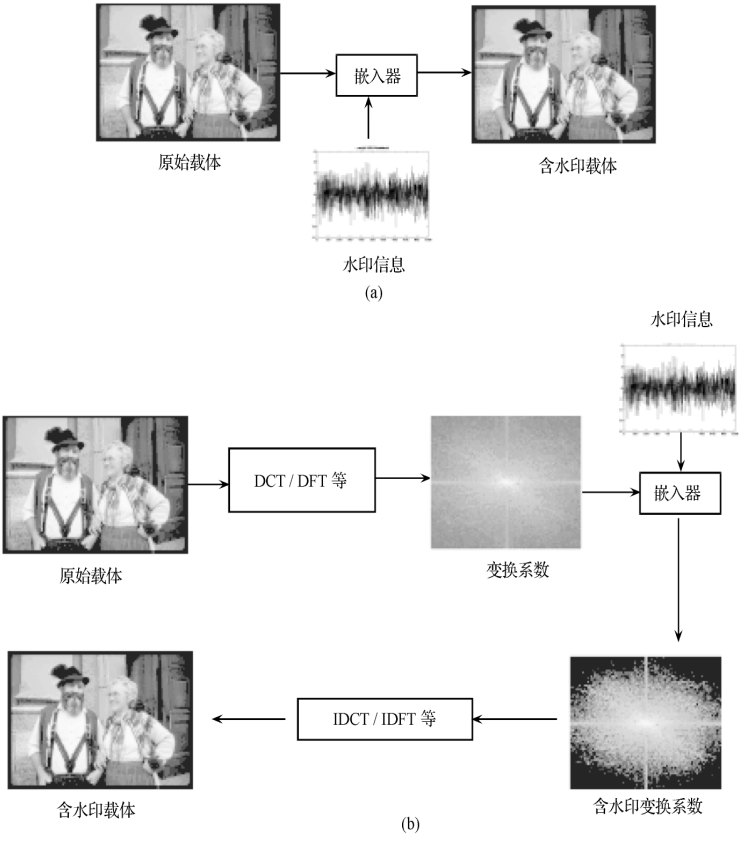


图 1.7 时/空域和变换域水印嵌入算法

(a) 时/空域水印嵌入算法;(b) 变换域水印嵌入算法

(8) 按嵌入方式进行划分

嵌入方式指嵌入水印信息时,对载体数据进行修改的方式,最为典型的是扩频方式和量化方式。扩频水印算法可以被认为是水印信息经过简单的缩放,然后加到载体作品上;量化水印方法不是将水印信号简单地加在原始信号上,而是根据不同的水印信息用不同的量化器去量化原始载体信号,从而实现水印信息的嵌入。

值得注意的是,上述提到的各种分类方法并不是孤立的,它们经常互相交叉。例如,一个鲁棒水印算法可以采用盲检测也可以采用非盲检测;一个可见水印算法

或者不可见水印算法可以采用盲检测也可以采用非盲检测;一个鲁棒水印算法可以采用扩频方式实现,也可以采用量化方式实现,当然脆弱水印算法或者鲁棒水印算法都可以应用于不同的载体。

1.5 数字水印的攻击方法

所谓"攻击"是指对嵌入的水印进行各种操作以此来削弱、破坏或移除水印。数字水印技术在实际应用中必然会遭到各种各样的攻击。人们对新技术的好奇、盗版带来的巨额利润都会成为攻击的动机,这类攻击称为恶意攻击;而数字作品在存储、分发、打印、扫描等过程中,引入的各种失真,被称为无意攻击。攻击的目的在于使相应的水印系统检测工具无法正确地恢复水印信号,或不能检测到水印信号的存在。

按照攻击原理和目的可以将攻击分为简单攻击、同步攻击、分析攻击、解释攻击和拷贝攻击等五类。其中,简单攻击和部分同步攻击一般可以被看做无意攻击[1)],而分析攻击、解释攻击和拷贝攻击都是恶意攻击。 *

1.5.1 简单攻击

简单攻击[19~22]又称为波形攻击、噪声攻击。它试图对整个水印化数据(嵌入水印后的载体数据)进行操作来削弱嵌入水印的幅度,导致数字水印提取发生错误,甚至根本提取不出水印信号。对于数字图像而言,简单攻击包含了常规的信号处理操作,如线性滤波、通用非线性滤波、压缩(JPEG、MPEG)、添加噪声、漂移、像素域量化、数/模转换和 gamma 修正等。

在简单攻击中,压缩和滤波是最常用的方法,因为常规信号处理,尤其是图像处理中,经常会用到压缩和滤波。JPEG 是最常见的图像有损压缩算法之一。数字图像水印系统都必须对一定程度的压缩具有鲁棒性。一般图像的主要能量均集中于低频分量上,压缩算法会压缩掉原图中视觉上不显著的信息,通常为图像的高频分量,图 1.8(a)显示了 JPEG 压缩后的 Lena 图像,其中原始图像如图 1.4(a)所示。而水印的不可见性又要求水印要驻留于图像不显著的视觉信息中。所以图像水印要在不可见性和抗 JPEG 压缩之间进行折中,很多水印都是嵌入在图像的中频区域。此外,当前很多针对水印的攻击行为都是用滤波完成的,其实现有很多方式,可以是线性滤波,也可以是非线性滤波。但不管用何种方式实现,最常用的是低通滤波器,包括中值、高斯和均值滤波器等,图 1.8(b)显示的是 3×3 的中值滤波后的图像。因此,通常我们希望图像中的水印具有低通特性。

---

*1) 扫描过程中出现的旋转等同步失真属于无意攻击,而刻意的旋转等造成的同步失真属于恶意攻击。

(a) (b)

图 1.8 JPEG 压缩和中值滤波后的图像

(a) JPEG 压缩图像,压缩因子为 50;(b) 3×3 中值滤波后的图像

1.5.2 同步攻击

同步攻击[20]又称为禁止提取攻击。这种攻击不以完全去除水印信息为目的,而是试图破坏载体数据和水印的同步性,从而使得水印的相关检测失效或使提取嵌入的水印成为不可能。在同步攻击下,被攻击的数字作品中水印仍然存在,而且幅度没有变化,但是水印信号已经错位,不能维持正常水印提取过程所需要的同步性。这一类的攻击算法很多,主要包括几何变换、Warping、Jitter、Mosaic 攻击等。

几何变换就是通过对含水印图像做各种全局或局部仿射、投影变换等进行攻击,主要包括旋转(rotation)、缩放(scale)、平移(translation),这三项通常简称为 RST,如图 1.9 所示,其中所使用的原始图像如图 1.4(a)所示。其他的几何攻击方法还有水平反转、剪切等。由于简单易行,几何变换是目前最常见的一种攻击手段。Warping 是扭曲图像的技术,通常在对图像做局部调整和修补时使用。攻击者采用 Warping 技术攻击时是对图像施加局部或全局的随机几何失真,这种攻击曾使很多水印算法失败。图 1.10 显示的是图像扭曲的示意图。像素跳动(jitter)就是随机删除或复制某些行或列,有时这种攻击方法也被称为 Unzign 攻击。攻击者通常任意删除图像中的某几行和列,或者删除行和列后,在图像中的其他位置上复制相同数量的行和列,以保证图像的尺寸正确。这种攻击一般不会造成视觉上的影响。

此外,网络浏览器为了提高图片的传输速度,有时会在发送端把一个图像拆分成若干个小图像分别传输,接收端把这些小图像依次拼接为整个图像显示出来。马赛克(Mosaic)攻击就是把一幅含水印图像分割成足够小的图像块,分别通过水印检测器,检测算法很有可能无法在这些小图片上发现水印信息,然后攻击者再把这些小图像依次拼接为完整的图像。

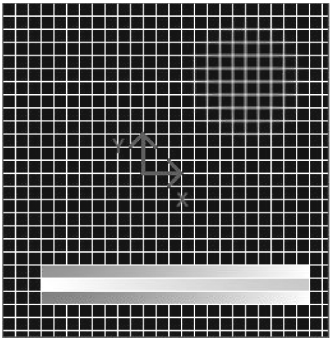
(a)

(b)

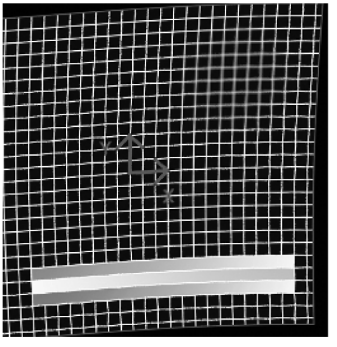
(c)

图 1.9 RST 示意图

(a) 旋转 45°后的图像;(b) 缩小后的图像;(c) 平移后的图像



(a)



(b)

图 1.10 图像扭曲示意图

(a) 扭曲前的图像;(b) 扭曲后的图像

而常见的打印、扫描也可能使水印检测失效，从而达到攻击的目的。其他的同步攻击还有数据的增减，如剪切(croping)、添加 logo 和图像拼接等。

1.5.3 分析攻击

分析攻击也被称为计算攻击或去除攻击，这种攻击方法在水印嵌入和检测阶段采用特殊方法来擦除或减弱图像中的水印，即针对某些水印方法通过分析水印数据，估计图像中的水印，之后将水印从图像中分离出来并使水印检测失效，从而达到非法盗用的目的。常见的方法有联合攻击(也称为平均攻击或共谋攻击)[23]、敏感性分析攻击[24,25]、降梯度攻击、去噪、确定的非线性滤波和采用图像综合模型的压缩(如纹理模型或者三维模型)等。

共谋攻击是一种最典型的分析攻击方法，它是利用多个含水印图像之间的统计信息进行攻击的一种方法。攻击者设法获得几个包含同一水印的不同作品，并且将这些作品结合起来进行研究，用以了解算法如何操作。攻击者也可以通过得到水印图像的多个拷贝，即包括不同水印信息的几个相同图像，对多个拷贝进行平均来去除水印信息，或者根据多个含水印图像之间的统计信息，从每个拷贝中提取一小部分图像，再把这些小图像合并为一个完整的不含水印的图像。研究表明，如果非法用户能够得到 10 个左右的含水印图像拷贝，就可以成功地利用平均/共谋攻击去除水印信息。

此外，敏感性分析攻击和降梯度攻击也是比较典型的分析攻击方法。在敏感性分析攻击中，攻击者使用黑匣子检测器估计从水印作品到检测区域边缘的最短路径方向。这是基于可以由检测区域表面的法线来估计最短路径，并且相对于很大一部分检测区域法线方向都基本保持不变的两个假设。降梯度攻击与敏感性分析攻击不同，它要求攻击者拥有可以报告确切检测值而不是最终二值判决的检测器，攻击者使用随着作品缓慢变更而不停变化的检测值来估计水印作品检测统计量的梯度。假设检测区域最短路径的方向是下滑最急剧的方向，给定一个水印作品后，可以使用任何搜索战略来确定局部的最大下降梯度，从而可以沿着该路径对作品进行少许平移，并且不断重复该处理直至得到的作品刚好移出检测区域边界。

1.5.4 解释攻击

解释攻击[22,26]是由 IBM 公司的水印研究小组针对可逆水印算法而提出来的一种水印攻击方案，因而也称为 IBM 水印攻击[27]，或称之为混淆攻击、逆镶嵌水印攻击、死锁攻击、倒置攻击、伪水印攻击、伪源数据攻击或歧义攻击。这种攻击在面对检测到的水印证据时，试图捏造出种种解释来证明其无效。一种通用的方式是攻击者试图生成一个伪源数据或伪水印化数据来混淆含有真正水印的数字作品版权。例如，攻击者在存在原始水印信息的真实载体数据中，嵌入一个或者多个伪

造的水印信息,从而混淆第一个含有主权信息的水印,使提取出来的水印失去唯一性。

解释攻击中,攻击者并没有除去水印而是“引入”了他自己的水印,载体作品或许被改变或许不被改变。例如,攻击者通常可以将水印嵌入过程逆过来运用,即他的攻击是“减去”一个水印。假设数字作品 $\boldsymbol{C}_o$ 的所有者为了保护其版权,在 $\boldsymbol{C}_o$ 上加入一个水印信息 $\boldsymbol{W}_1$ 得到含水印的作品 $\boldsymbol{C}_w$,即 $\boldsymbol{C}_w = \boldsymbol{C}_o + \boldsymbol{W}_1$。攻击者获得 $\boldsymbol{C}_w$ 后,计算伪造的原始作品 $\boldsymbol{C}_o' = \boldsymbol{C}_w - \boldsymbol{W}_2$,声称 $\boldsymbol{C}_o'$ 是他的原始作品,$\boldsymbol{W}_2$ 是嵌入的水印信息。此时攻击者和作品所有者都可以声称他们用各自的原始作品和水印产生了含水印的作品 $\boldsymbol{C}_w$。

1.5.5 拷贝攻击

拷贝攻击[23]要估计出水印信息,然后把估计出的水印拷贝到其他图像中。在拷贝攻击中,首先攻击者需要在没有密钥信息和水印嵌入算法信息的情况下,利用极大似然(ML)、最大后验概率(MAP)、最小均方差(MSE)等方法估计原始图像或水印信息。得到估计出的水印后,再把这个伪造的水印拷贝到其他的图像上。拷贝过程中要对水印和目标数据作些调整以满足不易察觉的要求。这些调整可以根据人的视/听觉系统特性(HVS/HAS)进行,如对比度和纹理屏蔽等。

1.6 数字水印技术的应用领域

版权保护是数字水印发展的源动力,也是数字水印技术的一个重要的应用方面,但除此之外,数字水印技术的应用还包括广播监视、内容认证和使用控制等[25,28]。

数字版权保护可以被细分为所有者鉴别、所有权验证和操作跟踪。随着计算机和互联网的发展,版权保护的意义越来越重大,因为越来越多的艺术作品、发明或创意都开始以多媒体数据的形式表达,如数码照片、数字电影、MP3 音乐、计算机绘画等,并且所有活动所涉及的多媒体数据都蕴含了大量价值不菲的信息,与作者创作这些多媒体数据所花费的艰辛相比,篡改、伪造、复制和非法发布原创作品在信息时代变成了一件轻而易举的事情。任何人都可以轻而易举地创建多媒体数据的拷贝,与原始数据比较,复制出的多媒体数据不会有任何质量上的损失,即可以完整地“克隆”多媒体数据。因此如何保护这些数据上附加的“知识产权”是一个亟待解决的问题。那么数字水印则正好是解决这类“版权问题”的有效手段。过去,画家用印章或签名标识作品的作者,那么今天,他们可以通过数字水印将自己的名字添加到作品中来完成著作权的标识。同样,音像公司也可以把公司的名字、标志等信息添加到出版的磁带、CD 碟片中。这样,可以通过跟踪多媒体数据中的

数字水印信息来保护多媒体数据的版权。

数字水印技术在图像、文档(印刷品、电子文档等)等的真伪认证和完整性鉴别方面也有很大的用途。例如,对政府部门签发的红头文件,文件认证的传统方法是鉴别文件的纸张、印章或钢印是否符合规范和标准,缺点是纸张、印章或钢印都容易被伪造。将数字水印信息添加到文档中,也意味着某些信息可以在文档中被写入两次。例如,护照持有人的名字在护照中被明显地印刷出来,也可以在头像中作为数字水印嵌入,如果某人想通过更换头像来伪造一份护照,那么通过扫描护照就有可能检测出嵌入在头像中的水印信息与打印在护照上的姓名不符,从而发现被伪造的护照。

广播监视中也可以应用数字水印技术,而且与其他广播监视技术相比,数字水印技术的优点是它存在于被监视的内容之中,优于采用广播信号中的特定片断,因此它与广播设备的安装基础(包括数/模、模/数转换)完全协调一致。目前,已有数家公司可以提供基于水印的广播监视服务。

此外,数字水印还用来做多媒体数据的访问控制和复制控制。例如,CD 数据盘中秘密的数字水印信息可以有条件地控制某些人对该 CD 盘中内容的访问权。目前,DVD 已经火暴国内电子市场,很多大公司已开始研究如何应用数字水印系统改进 DVD 的访问与复制控制。例如,希望消费者手中的 DVD 播放器允许无限制地复制家庭录像或过期的电视节目,家庭录像中所添加的数字水印不含任何控制标识,电视节目里的数字水印标识为“复制一次”、“复制多次”,而商业的视频节目则标识为“不允许复制”,相关的播放设备将对这些数字水印标识进行判别并起相应作用。这样就既保证了消费者私下复制、交换节目的自由,又有效控制了商业上的侵权行为。目前,全部的解决方案已经形成,问题是该解决方案的安全性、有效性、简洁性还须经受进一步的考验,暂时不能提供给 DVD 制造商和用户。

数字水印技术还可以应用于信息的安全通信。由于人们很难觉察到数字水印信息在多媒体数据中的存在,某些重要信息在传输的过程中就可以嵌入在普通的多媒体数据中,从而避开第三方的窃听和监控。这种做法与普通的电话通信、电子邮件通信以及加密通信相比,隐蔽性高,不容易监控,而且很难被察觉。

总之,数字水印技术有着宽广的应用范围,对数字水印技术和数字水印技术的应用研究具有重要的意义。

参 考 文 献

1 Stefan Katzenbeisser, Fabien A P Petitcolas. 信息隐藏技术——隐写术与数字水印. 吴秋新,钮心忻,杨义先译. 北京: 人民邮电出版社,2001

2 A Z Tirkel, G A Rankin, R M Van Schyndel, W J Ho, N R A Mee, C F Osborne. Electronic Watermark. Digi-