文章编号：1009-3443(2003)03-0001-05

数字水印技术及进展

张 勇[1,2]， 赵东宁[1,2]， 李德毅[2]

(1.解放军理工大学 通信工程学院,江苏 南京 210007;2.中国电子系统工程研究所,北京 100039)

摘 要：阐述了数字水印技术产生的必然性,分析了数字水印技术的研究现状,并简要叙述了云数字水印技术,探讨了数字水印技术的特点及其各种攻击方式,举例说明了目前数字水印在商业上的应用。数字水印技术的研究对数字内容的版权保护有重大实用价值和实践意义。

关键词：数字水印;信息隐藏;版权保护;云数字水印

中图分类号：TP391.41 **文献标识码**：A

Digital Watermarking Techniques and Progress

ZHANG Yong[1,2]， *ZHAO Dong-ning*[1,2]， *LI De-yi*[2]

(1. Institute of Communications Engineering, PLA Univ. of Sci. & Tech., Nanjing 210007 China;
2. Institute of China Electronic System Engineering, Beijing 100039, China)

Abstract: In this paper, the background of digital watermarking techniques is depicted. The research status of digital watermarking techniques is analyzed, with the cloud digital watermarking techniques depicted simply. The characters and the ways of attack are discussed. And the application of digital watermarking on commerce are illustrated. The study on digital watermarking techniques has important practical value and practical significance for digital content.

Key words: digital watermark; information hiding; copyright protection; clould digital watermark

近年来,随着计算机多媒体技术和因特网技术的迅猛发展,人们可以很方便地传播、拷贝、存储和处理图像、音频、视频及文本等多媒体信息。与此同时,也引发了各种多媒体信息的传输安全问题和数字产品的版权保护问题。为了解决数字内容的版权保护和信息安全问题,近年来提出了加密-解密、数字签名、数字标签、数字指纹和数字水印等多种技术[1]。其中,数字水印技术是20世纪90年代出现的一门崭新技术,它通过在数字产品中嵌入可感知或不可感知的信息来确定数字产品的所有权或检验数字内容的原始性。数字水印技术弥补了加密-解密技术不能对解密后的数据提供进一步保护的不足;弥补了数字签名不能在原始数据中一次性嵌入大量信息的弱点;弥补了数字标签容易被修改和剔除的缺陷;弥补了数字指纹仅能给出版权破坏者信息的局限。数字水印技术是信息隐藏技术研究领域的重要分支,也是当今网络信息安全和数字媒体版权保护研究的热点。

收稿日期:2002-12-23.
基金项目:国家973规划资助项目(G19980305084).
作者简介:张 勇(1976—),男,博士生.

1 数字水印技术出现的必然性

1.1 数字水印的起源

历史上，水印是指在指纸上留下轻轻的烙印，这种烙印几乎是看不见的，除非在某种合适的条件下仔细地观察。几个世纪以来,水印被用于证明物质材料的真实性,将相似的思想用于数字财产的保护。数字水印技术主要运用两个相关领域的技术:密码

术和隐写术。密码术被定义为密写的研究,如通过转换原始信息到一种不容易被观察者看出来的格式来显示秘密消息的内容;而隐写术是将一个消息隐藏于另一个消息的技术研究,不透露隐藏信息的存在或不让观察者发现消息里包含了一个隐藏信息[2]。从技术角度,数字水印技术使用的思想主要来源于隐写术而不是密码术。经典的隐写术和数字水印之间的主要区别在于:隐写术仅仅是企图在其他内容中隐藏一个消息(可能是一个水印),而数字水印还要强调阻止攻击者篡改水印。

Van Schyndel 在 ICIP'94 会议上发表了题为"A digitalwatermark"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,阐明了一些关于水印的重要概念,被认为是一篇具有历史价值的文献[3]。

1.2 密码术的局限性

许多有关数字内容版权需要解决的问题,类似于安全通信中密码术所解决的问题。如在分发传播时,需要保证数字内容的完整性才能检测到数字内容是否被修改。安全通信中,密码术已利用带有密钥的数字签名解决了消息完整性问题。需要保证数字内容与其创建者、分发商或购买者之间的关联,才能跟踪数字产品的传播。类似于安全通信中密码术所解决的不可否认性问题。然而,传统的隐秘系统有一个重大缺陷,即不能保证数字内容与秘密信息永久地关联,加密的数字内容一旦被破解,将无密可言。这就达不到版权保护的最终目的。常规上看,密码术在通信中是将信息加密隐藏,同时还提供了附加信息,从而有效地保证了信息完整性和不可否认性。但密码术不能将秘密信息嵌入到消息内容中。所以单单密码术不能保证数字内容被再次非法分发传播和随意篡改。为了保证对数字内容版权的进一步保护,需要扩展密码技术并将附加秘密信息嵌入数字内容中。解决该问题的技术称为数字水印技术[4]。数字水印是不可见的或几乎不可察觉的,可应用到数字视频、数字音频和数字图像等多媒体文档中。

2 数字水印技术研究现状

所谓数字水印技术,就是将代表数字媒体著作权人身份的特定信息、用户指定的标志或序列码等,按照某种方式嵌入被保护的信息中,在产生版权纠纷时,通过相应的算法提取该数字水印,从而验证版权的归属,确保媒体著作权人的合法利益,避免非法盗版的威胁。被保护的信息可以是任何一种数字媒体,如软件、图像、音频、视频或普通电子文档等。数字水印是嵌在数字产品中的数字信号,水印的存在要以不破坏原数据的欣赏价值和使用价值为原则。

2.1 典型数字水印系统模型

图1为数字水印信息嵌入模型,其功能是将数字水印信息嵌入原始数据中;图2为数字水印信息检测模型,用以判断某一数据中是否含有指定的水印信息或提取出数字水印信息。图2中的虚线表示在数字水印检测或提取时允许盲检。

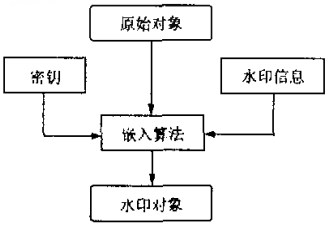

图1 数字水印嵌入模型

Fig. 1 Digital watermark embedding model

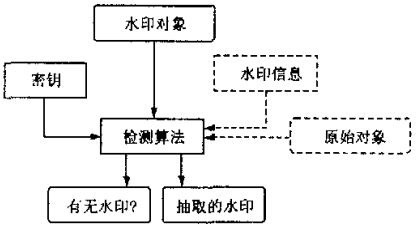

图2 数字水印检测模型

Fig. 2 Digital watermark extracting model

2.2 多媒体数字水印技术

近几年来,图像、音频、视频等多媒体的数字水印技术发展非常迅速,国内外许多大学和科研机构都热衷于数字水印技术的研究,提出了许多算法和解决方案,取得了显著的成果,有些数字水印技术已经应用于商业目的。

图像数字水印技术大体上可分为时空域和变换域数字水印技术。时空域数字水印技术中,嵌入图像的水印信息不经过任何变换,直接嵌入图像像素上。时空域的数字水印技术,主要是基于改变图像数据统计特性的水印算法。如文献[5]提出的patchwork算法,它是基于统计的数字水印嵌入方案,该算法首

先随机选择 N 对像素点，在增加一点亮度的同时，相应降低另一点的亮度值，从而隐藏水印信息。变换域的数字水印技术是将图像和水印变换到不同的域（小波变换域、频率变换域、离散傅里叶变换域、离散余弦变换域等）上实现水印的嵌入。文献[6]还提出了基于人类视觉模型(HVS)的水印技术。

音频水印技术主要集中于研究低比特位编码、相位编码、基于扩展频谱编码和回声隐藏等4个方面[7]。低比特位编码音频数字水印技术基本思想，是首先将水印编码成二进制串，然后用这些二进制串替换每个样本点的最不敏感的比特位，这就在音频信号中嵌入水印信息。低比特位编码水印技术是最简单的数字音频水印技术。从信噪比方面来说，相位编码是最有效的编码方案之一，因为实验显示，在平滑相位改变的情况下即使信号模式发生戏剧性的改变，也不会令人感到声音有所变化。相位编码水印技术中，隐藏的水印信息用特定的相位或相位谱中的相位变化来表示。如果音频信号被分解为许多节，水印信息通常仅嵌在首节中，并且要满足两个条件，一是每节之间的相位差异需要保存；二是嵌入水印信息的最后一个相位谱应该是光滑的，否则，突然的相位改变会引起听觉上的感知。基于扩展频谱编码水印技术的基本思想是，通过将加密数据扩展到尽可能大的频谱上而加密信息流。许多扩展频谱技术适于音频信号的信息隐藏。回声隐藏是通过插入回声而隐藏信息的方法。插入的回声延迟应该小于听觉可感知的限度。另外，还有基于人类听觉模型(HAS)的水印技术。

视频水印技术方面[8]，Arena 等人提出了将水印直接嵌入在MPEG-2比特流域中，避免了将水印嵌入在像素域中所必需的视频码流解码与再编码的繁琐运算；Su 等人提出了一个依赖于内容的空间嵌入视频水印方案，该方案基于两个基本思想：统计不可见性和设置内容同步；Mobasseri 等人提出了一个应用直接序列扩展频谱模型的视频水印方案；Jianhao Meng 等人提出了一种在 MPEG-1 和 MPEG-2 压缩视频流中嵌入可视水印的方案。可见水印不同于不可见水印，它是通过在图像表面半透明地显示版权信息来防止盗版。北京邮电大学戴元军博士提出了一种改进的基于扩展频谱的MPEG视频水印方案，将水印信息嵌入到视频流中 I 帧的色度的 DCT 直流系数中，不需要完全解码，大大减少了运算的复杂度，提高了实用性。

2.3　云数字水印技术

云数字水印技术主要是将李德毅院士提出的云理论思想[9]与数字水印技术结合起来，使得云水印技术较其他水印技术有更好的优势。

(1)文本云数字水印技术

文本云数字水印技术是根据云模型[9]及文本的特点，通过基本云发生器产生云滴，然后将这些云滴嵌入到需要加水印的文本中，单个云滴(水印标记)并没有实际的意义，但所有云滴的组合就构成了水印信息。每个云滴的横坐标用以调整文本当前行与上一行之间的行间距，纵坐标即云滴的确定度用以调整当前文本行字平均间距，使字平均间距等于云滴横坐标与其纵坐标乘积，这样每行的行间距和字平均间距就对应一个云滴水印标记，所有云滴(水印标记)就组成了水印。

文本云数字水印技术使得标记的行较文献[10]增加了近1倍，所以嵌入的信息量也增加了1倍。文本云数字水印的检测不需要原始文本文件，实现了盲检。当然为了增强文本云数字水印技术的鲁棒性还有许多关键技术有待解决。

(2)关系数据库云数字水印技术

目前，由于关系数据库数据本身的特殊性，这方面的研究不像其它多媒体数字水印技术研究那么活跃。关系数据库数字水印技术国内还没有研究，国外 Agrawa[11]和 Sion[12]等人也只是对关系数据库数字水印技术进行了初步研究。我们提出了关系数据库云数字水印技术，即根据关系数据库的某些数值型属性值允许一定误差的特点，给定云发生器[9]的3个参数，使得通过基本云发生器产生一定数量的水印云滴标记落在误差允许的范围内，将这些云滴嵌入到某些元组的数值型属性值上，这样既不会使得这些数值型属性值超出其误差范围，也不会影响该关系数据库数据的实际使用。运用云数字水印技术可验证关系数据库数据的所有权归属。关系数据库云数字水印技术的鲁棒性还有待更深入的研究。

3　数字水印技术的基本特征

数字水印技术是信息隐藏技术研究领域的重要分支，它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。数字水印技术基本特征主要有[3,8]：

(1)鲁棒性：指不因多媒体文件的某种改动而导致隐藏信息丢失的能力。

(2)不可见性：利用人类视觉系统或听觉系统属性，经过一系列隐藏处理，使目标数据没有明显的降质现象，而隐藏的数据却无法人为地看见或听见。

(3)不可检测性:指隐藏载体与原始载体具有一致的特性。

(4)自恢复性:由于经过一些操作或变换后,可能会使原图产生较大的破坏,如果只从留下的片断数据仍能恢复隐藏信号,而且恢复过程不需要宿主信号,这就是所谓的自恢复性。

4 数字水印技术的攻击方式

给定一个数字水印方案,要弄清其能否被成功攻击很重要。文献[4,13]定义了4种攻击方式,鲁棒性攻击、表述性攻击、解释性攻击以及法律性攻击。

(1)鲁棒性攻击,试图削弱或去除数字内容中的水印,同时保证内容不至于在攻击后失去其可用性。常见的鲁棒性攻击是噪音攻击,随机噪声被加到数字内容中试图混淆水印。其次还有合谋攻击,即在某些水印方案中,如果图像在不同的密钥下被加多次水印,就可通过"平均"这些水印图像,获得一个合成图像,与原始图像很相似但不含任何有用的水印图像。另外还有倒置攻击,即如果攻击者熟悉水印嵌入过程,就会简单地检测出水印并颠倒插入过程而较好地去除水印。为了防止这种特别的攻击,许多水印方案中都用密钥来设计水印嵌入算法,没有密钥就很难了解水印的嵌入。

(2)表述性攻击,是一种不去除水印但修改数据内容,从而破坏水印存在的攻击方式。对图像的"碎片攻击"就属于表述性攻击,其基本思想是将一幅图像分解成许多"碎片",然后再将这些"碎片"拼凑成一幅完整的图像而不影响图像的使用效果。例如在Web页中,使用原始图像和使用"碎片"拼凑起来的图像相比,用户视觉效果是一样的。

(3)解释性攻击,从水印证据中寻找伪造无意义的或多种解释。例如,在水印图像上再加第二个水印,使得第一个水印不确定。另一个解释性攻击就是将水印倒置而在插入一个新的假水印之前去除原始水印。

(4)法律性攻击,不同于其他攻击,因为它不考虑水印系统的技术细节。法律性攻击中,攻击者使用内容所有者的名誉、身份或一些其他的非技术信息等办法,使得法庭怀疑水印中是否确实包含所有者声称的证据。

没有一种攻击方式容易防护,所以,研究的水印系统应该努力使其可以经受许多已知的攻击。如果这种研究可以提高数字水印在商业上的可行性和可靠性,利润将是巨大的。商业部门已认识到水印潜在的价值,并开始用水印技术来保护数字内容所有权了。

5 数字水印技术在商业上的应用

最近数字水印技术的发展导致了商业上对水印应用范围的增大。数字水印技术已在可信数字相机、脆弱水印、标题注释、可逆可见水印、手稿数字版权和DVD拷贝控制等几个领域加以应用[4,14]。

(1)可信数字相机

Friedman[15]针对专业摄影师提出了可信数字相机的思想。照像时相机会对每一张相片嵌入一个数字水印,即在捕捉到图像的那一刻嵌入一个不可去除的标记。对摄影师来说将这种产品与某些水印注册服务结合,将有效地保证摄影师拍摄的任何图像所有权的真实性。

(2)脆弱水印

脆弱水印技术已得到了一些应用,例如货币流通和个人支票。在创建原始文档时,将一个脆弱、不可见的水印嵌入到文档中。如果文档被复制,水印将不再在复制品上重新产生。将这种技术用于数字内容上将获得同样的效果。假定存在这样一个水印系统,数字水印不会因为文档的复制而转到另一个文档上,脆弱水印可用于区别标记的数字文档和偷来的复制品。脆弱水印使得没有水印的复制品毫无价值。

(3)标题注释

不可见水印可以包含嵌入数字内容的元信息。如歌曲中包含的嵌入信息可以是作者、相册、录制日期等信息。理论上,这些信息对每个人都是有用的,不会有人试图去除它。标题注释不仅对消费者有用,而且对无线电台插放音乐的人也有用。

(4)可逆可见水印

IBM已经开发了一个水印方案,称为可逆可见水印。该水印系统中,IBM允许图像的自由拷贝,但在图像上加上可见水印,这些图像在没有去除可见水印前没有应用价值。水印图像作为样本发送给用户,如果用户想得到有价值图像版本,他们可以买付费去除程序,该程序可以去除图像上的水印而将图像恢复为原始质量。

(5)手稿数字版权

最近,梵蒂冈开始用可见水印作为他们发布到因特网上手稿的版权标识。这些标识都是插入到黑白和彩色图片上的鲁棒水印,该技术是在梵蒂冈图书馆需求下开发的。

(6)DVD 拷贝控制

1997 年 6 月成立的一个信息隐藏小组，在 DVD 版权保护技术工作组(DVD CPTWG)领导下，评估当时提出的 11 个水印技术建议的技术可行性。经过视觉质量和生存能力等一系列试验后，于 1998 年 5 月的会议上发表了一个临时报告，结果显示当前的水印技术符合 DVD 拷贝控制应用技术需求。DVD 拷贝控制的数字水印技术的应用应在 DVD 硬件制造商和 DVD 软件制造商共同合作下完成。

6 总　结

数字水印技术是近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、密码学和隐写术等均有密切关系。特别是在网络技术和应用迅速发展的今天，数字水印技术的研究更具现实意义。当前，数字水印技术有几个缺点[14]。首先，水印技术不足以禁止攻击者为了自己的利益处理水印数据对象。第二，没有相应的水印技术标准，公众还不能接受水印作为内容版权保护的合法形式。第三，还有许多与水印和因特网内容相关的法律问题没有解决。所以说数字水印技术作为保护数字内容版权的手段还不成熟，但是没有克服不了的困难，也许在不久的将来，数字水印将名副其实地成为版权保护的有力手段。数字水印技术下一步的研究主要是提高现有水印算法的鲁棒性和安全性，从而发现更好的水印算法，增强其在法庭上提供证据的可信赖性及商业上的应用。另外还要增加对其他非多媒体数字水印技术的研究，如关系数据库的非数值型属性数字水印技术等。

参考文献：

[1] 王秋生. 变换域数字水印嵌入算法研究[D]. 哈尔滨：哈尔滨工业大学，2001.

[2] ANDERSON R J，PETITCOLAS F. On the limits of steganography[J]. IEEE Journal of Selected Areas in Communications，1998，16(4)：474-481.

[3] 易开祥，石教英. 数字水印技术研究进展[J]. 中国图象图形学报，2001，6(2)：111-117.

[4] FERRILL E，MOYER M. A Survey of digital watermarking[DB/OL]. http：//Elizabeth. ferrill. com/papers/watermarking. pdf，1999-02-25.

[5] BENDER W，GRUHL D，MORIMOTO N，et al. Techniques for data hiding[J]. IBM Systems Journal，35(3，4)：313-336.

[6] BRETT T，HANNIGAN，REED A. et al. Digital watermarking using improved human visual system model[A]. In：Proceedings of SPIE 2001[C]. California：The international society for optical engineering. 2001.

[7] XU C S，WU J K，SUN Q B. Digital audio watermarking and its application in multimedia database [A]. In：ISSPA'99[C]. Brisbane，Australia，1999.

[8] 戴元军. 基于扩展频谱的视频水印技术的研究与实现[DB/OL]. http：// www-900. ibm. com/developerworks/cn/security/se-mpegdig/index. shtml，2002-08-01.

[9] 李德毅，孟海军，史雪梅. 隶属云和隶属云发生器[J]. 计算机研究与发展，1995，32(6)：15-20.

[10] BRASSIL J，LOW S，MAXEMCHUK N，et al. Electronic marking and identificatioon techniques to discourage document copying[J]. IEEE Journal on Selected Areas in Communications，1995，13(8)：1495-1504.

[11] AGRAWAL R，KIERNAN J. Watermarking relational databases [A]. In：Proceeding of the 28th VLDB Conference [C]. Hong Kong：Univ of Sci & Tech，2002.

[12] SION R，ATALLAH M，PRABHAKARL S. Watermarking Relational Databases[R]. The center for Education and Research in Information Assurance and Security of Purdue University，2002.

[13] CRAVER S. Technical trial and legal tribulations [J]. Communications of the ACM，1998，41(7)：45-44.

[14] NORISHIGE M. Digital watermarking technology with practical applications [J]. Information Science Special Issue on Multimedia Information Technologies-part 1，1999，2(4)：107-111.

[15] MEMON N，WONG P W. Protecting digital media content [J]. Communications of the ACM 1998，41(7)：35-43.

(责任编辑：程　群)