

数字水印在现代生活中的应用

宋立平

随着电子政务的广泛应用,信息安全保护问题日益突出。传统的加解密系统不能很好地解决版权保护问题,因为加密后的作品只有经过授权的解密密钥持有者才能存取数据,以致无法向更多的人展示自己的作品;而且数据一旦解开,就完全置于解密人的控制之下,原创作者无法追踪作品的复制和二次传播。数字水印技术在这种情况下应运而生。

数字水印(digital watermark)技术将特制的、不可见标记,以数字内嵌方法隐藏在数字图像、音频、视频等数字内容中,由此确定版权拥有者、识别购买者、提供关于数字内容的其他附加信息、确认所有权认证、跟踪侵权行为。数字水印的特点:首先是隐蔽性,嵌入水印后的数据与原始数据相比,感觉不到差别;其次是鲁棒性,所谓鲁棒性是指在经历多种无意或有意的信号处理后,数字水印仍能保持完整或仍能被准确鉴别;再次是密钥的唯一性,即不同密钥不产生等同的水印;最后是检测的可靠性,水印检测出错的概率应小于某一合适阈值,这一特性表明水印检测算法必须具有一定的确信度。

数字水印技术是目前国际学术界的研究热点之一。鉴于数字水印技术的应用前景和在电子商务中的重要意义,国际最著名的计算机和消费电子制造厂商 IBM、日立、NEC、Sony 等几家公司已宣布联合研究数字水印技术。著名的贝尔(Bell)实验室,MIT 信号处理实验室等也都开展了这方面的研究工作。我国的高校、研究机构和一些企业也投入极大人力物力,研究具有自主知识产权的数字水印技术和软件,并取得了可喜成果。

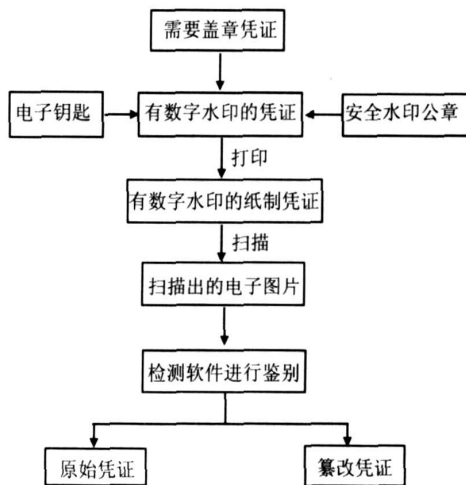
数字水印技术目前已进入初步应用阶段,IBM 公司在其“数字图书馆”软件中提供了数字水印版权保护功能,Adobe 公司在其著名的 Photoshop 软件中集成了 Digimarc 公司的数字水印插件。美国、日本、荷兰都已开始研究用于票据防伪的数字水印技术,德国已在保护和防止伪造电子照片上的技术方面取得突破。现有的数字水印技术主要用于防伪,版权保护,防止非法复制、篡改,隐蔽通信及其对抗。

一、防伪

造假自古就有,防伪也与人类文明一样久远。

许多防伪方法借用印刷技术,并在防伪打假中发挥了重要作用。但是相关的技术方法也被一些造假者用于造假活动,伪造货币、有价证券、文件、单据、证件、信用卡、合同、商标、标识、包装物、图章、名家书画、珍贵邮票、图章等犯罪活动遍及世界各地,在我国也屡禁不止。据统计,每年伪造的美元有 20 亿、假信用卡每年使美国银行损失 20 亿、每年全世界有 300 万份假护照。据估计,全球防伪市场的年总值为 2000 亿美元、国内防伪市场的年总值也达 500 多亿元人民币。利用假包装、假汇票、假证件从事违法活动的案例屡见不鲜,制假售假已成为仅次于贩毒的世界第二大公害。

数字水印技术在文档(印刷品、电子文档等)的真伪认证上用途广泛,例如验证政府部门红头文件的传统方法是鉴别所用纸张、印章或钢印是否符合规范和标准,然而纸张、印章或钢印容易伪造。特别是印章,虽然政府部门对印章的管理、制作有严格规定,但社会上还是有“一个萝卜刻一个章”的说法,这说明传统方法亟待完善。数字水印技术可有效解决这个问题,以数字水印作为信息载体,将某些信息添加到红头文件中,文件就含有难以察觉的数字水印信息,大大增加了伪造难度。再说说护照,更换头像为伪造假护照的一种常见方法,如果护照持有者的名字通过数字水印隐藏于头像之中,那么通过扫描护照检测头像中隐藏的水印信息与打印在护照上的



姓名是否相符,就能验明真伪,具体工作流程见上页。

目前从传统商务向电子商务转变过程中会出现大量过渡性电子文件,如各种纸质票据的扫描图像等。数字水印技术可为各种票据提供不可见的认证标志,大大增加伪造的难度。美国、日本、荷兰目前都已开始研究用于数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唯一的不可见数字水印,可从扫描票据中实时判断有无水印,快速辨识真伪。

二、版权保护

数字作品(如电脑美术、扫描图片、数字音乐、视频、三维动画)的版权保护是当前的热点问题。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严重损害作品质量的一些办法加上版权标志,但是这种明显可见的标志很容易篡改。“数字水印”利用数据隐藏原理使版权标志不可见或不可听,既不损害原作,又能保护版权。

例如 MP3 音乐压缩格式的编码算法取自 MPEG-1 Audio Layer 3,它是 MPEG-1 音频编码算法的一部分。MP3 不仅压缩率高,而且压缩后的音乐高保真,因此很受互联网用户的欢迎。然而 MP3 也带来版权保护方面的问题,不少公司都在为此研究有效保护版权的新的音乐压缩格式,希望开发出更为“安全”的网络音乐新格式,技术性能既要不低于 MP3,版权又要得到有效保护,从而保证版权持有者的收入。在这样的背景下,MP4 应运而生。MP4 是 Global Music Outlet 公司设计的一种格式,它不仅支持版权保护,而且每首 MP4 都内置版权信息,包括与作品、艺人或版权持有者相关的文字、图像、版权说明,以及音乐艺人或唱片公司的站点链接等。MP4 乐曲内置“Solana 技术”的数字水印,由其版权持有者发行,不仅能追踪和发现盗版发行,而且任何未经合法授权的解压缩行为都将彻底瓦解原文件。所以 MP4 是添加出版公司直接授权的知识产权协议后形成的一个全新数字音乐标准,然而市场现有的 MP4 还未达到设计要求,只是 MP3 的一种变形促销。

从目前的供应端看,无论是国外的三星、东芝、爱可视还是国内的华旗、明基都在试探性推出 MP4 产品,作为数码大鳄谁也不愿轻易放弃任何一块阵

地。现在华旗公司已推出中国人自主研发、自主设计、自主制造的一系列民族数码相机精品——爱国者数字水印数码相机。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,还未进入真正的实用阶段。

三、防止非法复制和篡改

由于数字产品本身易于拷贝和传输,如果不加以控制,每个用户都可无限复制完全相同的视频拷贝,从而威胁视频节目制造商和发售商的利益。因此付费电视节目系统采用给每个收看者一个私有水印的方案,接收者用一个装置(机顶盒)提取水印,在得到权限确认后才能进行视频解码。这种系统的好处是在接收方进行身份认证,大大降低了视频发售商的工作负担,节约的各种资源可以更好地服务于用户。

数据的标识信息往往比数据本身更具有保密价值,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看不到,只有通过特殊的阅读程序才能读取。这种方法已被国外一些公开的遥感图像数据库所采用。

防范数据的篡改攻击也是一项重要研究课题,现有的信号拼接、镶嵌技术可以“移花接木”“瞒天过海”,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判断声像信号是否已遭篡改。例如 1997 年 6 月 9 日最早公开的超级 CD 概念,在短短 3 个月后的 9 月 15 日,纽约的索尼贝尔就向音响业界宣布了相关规格提案和示范。同年 11 月的日本音响交易会上则响起了这种 CD 的声音。超级 CD 的五大特性之一就是有防盗版的数字水印。索尼和飞利浦发明的这种超级 CD,在刻录光痕的物理形成过程中会产生一种能透射过去的像水印一样的文字、图案(即“数字水印”),拷贝复制盘则做不出这种文字、图案,所以盗版片就会一目了然。

2007 年 6 月 12 日 Microsoft 也申请了一项专利,是一种用于下载版软件的防盗版水印技术,数字水印中包含的信息使软件的每一个实例都是唯一的。专利中提到:“软件通过因特网发布或出售时,例如买家姓名、地址、电话号码、信用卡号码等个人信息会被收集并编码为一串二进制序列。” Mi

icrosoft 解释道：“这个二进制序列映射到一个指令交换表，用来创建一个用于交换特定不相干指令对的序列。应用程序被下载之后，不相干指令对根据已编码的二进制序列进行有效交换，于是下载程序就会在下载之前带上由购买者个人身份信息生成的水印。盗版者可能会对比两个下载来的程序副本，但是只能找到两个程序中不同的部分——并不是所有被交换或被更改的指令对都能被侦测出来。要想正确找出所有被交换了的不相干指令对，必须对照大量已购买的应用程序副本，这样就能有效地防止盗版、非法复制。”

四、隐蔽通信及其对抗

数字水印所依赖的信息隐藏技术不仅提供了非密码的安全途径，更引发了信息战（尤其是网络情报战）的革命，产生了一系列新颖的作战方式，引起许多国家的重视。网络情报战是信息战的重要组成部分，其核心内容是利用公用网络传送保密数据。迄今为止，学术界在这方面的研究思路一直未能突破“文件加密”的思维模式，但是经过加密的文件往往混乱无序，易引起攻击者的注意。网络多媒体技术的广泛应用为利用公用网络进行保密通信提供了新思路，利用数字化声像信号相对于人的视觉、听觉冗余，可以隐藏各种时（空）域和变换域的信息，从而实现隐蔽通信。

视频水印同样也可用于军事保密或商业机密，属于信息隐藏范畴。一般情况下，为了保护同家的安全利益，政府部门都会限制公民传递秘密载体。为逃避这种限制，发送者可将秘密信息（如软件、图像、数据、文本、音频、视频）嵌入公开的视频，只有合伙人才能根据事先约定的密钥和算法提取隐藏信息，而其他（第三方）无法觉察到隐藏的水印，从而达到安全传输秘密信息的目的。

数字水印技术是国际学术界近几年来兴起的一个前沿研究领域，它与信息安全、信息隐藏、数据加密等关系密切。特别是在网络迅速发展的今天，数字水印技术的研究更具现实意义。因此数字水印研究要面向互联网上广为使用的各种数据文件（包括 JPEG 压缩图像、MPEG2 压缩视频、WAV、MIDI、MP3 音频文件、AVI 及三维动画文件、PS 和 PDF 标准文本等）。

今后的数字水印技术仍将着重于顽健性、真伪鉴别、版权证明、网络快速自动验证以及声频和视频水印等方面，并将与数据加密技术紧密结合（特别是顽健性和可证明性的研究）。然而，当前的水印算法在提供可靠版权证明方面在一定程度上并不完善，因此寻找实现完全版权保护的数字水印算法是一个重要的研究方向。

（天津工业大学理学院 300160）

科苑快讯

北京同步辐射装置新建的 X 射线小角散射站投入运行

北京同步辐射装置 (BSRF)

是利用同步辐射光源进行科学研究的装置、对社会开放的大型公用科学设施，是我国凝聚态物理、材料科学、化学、生命科学、资源环境及微电子等交叉学科开展科学研究的重要基地。随着小角 X 射线散射 (SAXS) 用户的增长，BSRF 原有的小角 X 射线散射站与 X 射线衍射站分时使用、共享 4B9A 光束线已远不能满足需求，广大用户强烈要求新建一条小角 X 射线散射站。在中国科学院和高能物理研究所的共同支持下，经过两年多的努力，新建小角 X 射线散射站已初步建成，并于 7 月初投入运行。

新的小角 X 射线散射光束线 1W2A 与蛋白质晶体学光束线 1W2B 共享前端区，从 1W2 光源点引出。小角 X 射线散射站由三角弯晶获取来自光源点水平方向约 2mrad 的同步辐射光并单色化得到

约 0.155nm 的单色光，经过聚焦镜后，聚焦光斑位于探测器上。三角弯晶距光源点距离 20.378 米，聚焦镜距光源点 22.553 米，探测器距光源点 30.378 米，样品距探测器 0.65~4 米可调。光束线与实验站初步调试已完成。全光斑强度约 1011cps，聚焦光斑大小约 $0.5 \times 2.5\text{mm}^2$ 。实验站配置有 Mar165 CCD 探测器、曝光快门、四刀狭缝、样品台等；光束线性能与实验条件较以前都有较大改观。对于已投入试运行的新建小角 X 射线散射站，实验用户反映良好，即将全面接受广大用户开展 SAXS 的研究工作。

新建小角 X 射线散射站目前投入运行的只是常规 SAXS 模式，实验站的参数还要在今后运行中不断优化、功能还在发展和完善，近期将开发出小角散射与广角衍射 (WAXS) 联合模式、秒级或亚秒级时间分辨模式、掠入射 SAXS 模式。根据用户需求和经费情况，还可开发各种特殊功能的样品环境室。

（摘编自中国科学院高能物理研究所高能新闻）

现代物理知识