文章编号:1005－0523(2005)02－0063－04

数字水印及其发展研究

石红芹,谢 昕

(华东交通大学 信息工程学院,江西 南昌 330013)

摘要:首先对数字水印的特征进行了分析,阐述了数字水印技术的基本原理,对目前比较流行的水印算法进行了分类和详细地讨论,最后指出目前水印技术存在的局限并对其发展进行了展望.

关 键 词:版权保护;数字水印;水印算法

中图分类号:TP391 **文献标识码**:A

1 引 言

近年来,随着数字化技术的进步和 Internet 的迅速发展,多媒体信息的交流达到了前所未有的深度和广度,其发布形式愈加丰富了.网络发布的形式逐渐成为一种重要的形式,伴随而来的是多媒体数据的版权保护问题.因此多媒体信息版权保护问题成了一项重要而紧迫的研究课题.为了解决这一难题,近几年国际上提出了一种新的有效的数字信息产品版权保护和数据安全维护的技术——数字水印技术.数字水印技术通过在原始媒体数据中嵌入秘密信息——水印来证实该数据的所有权归属.水印可以是代表所有权的文字、产品或所有 ID、二维图像,视频或音频数据、随机序列等.主要应用于:媒体所有权的认定.即辨认所有权信息,媒体合法用户信息; 媒体的传播跟算法研究.该子模块的研究为解决网络制造产品版权保护问题奠定了基础数字水印技术,又称数字签名技术,成为信息隐藏技术的一种重要研究分支,为实现有效的信息版权保护提供了一种重要的手段.

2 数字水印的基本原理

从图像处理的角度看,嵌入水印信号可以视为在强背景下迭加一个弱信号,只要迭加的水印信号强度低于人类视觉系统(Human Visual System ,HVS)的对比度门限,HVS 就无法感到信号的存在.对比度门限受视觉系统的空间、时间和频率特性的影响.因此通过对原始信号作一定的调整,有可能在不改变视觉效果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(载体图像)上用扩频通信技术传输一个窄带信号(水印信号).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)即是在有噪信道中弱信号的检测问题.

一般来说,为了使水印能有效地应用于版权保护中,水印必须满足如下特性:

1) 隐蔽性 水印在通常的视觉条件下应该是不可见的,水印的存在不会影响作品的视觉效果.

2) 鲁棒性 水印必须很难去掉(希望不可能去掉),当然在理论上任何水印都可以去掉,只要对水印的嵌入过程有足够的了解,但是如果对水印的嵌

收稿日期:2004－09－05

作者简介:石红芹(1970－)女,河北沧州人,硕士,讲师.

入只是部分了解的话，任何破坏或消除水印的企图都应导致载体严重的降质而不可用.

3) 抗窜改性 与抗毁坏的鲁棒性不同，抗窜改性是指水印一旦嵌入到载体中，攻击者就很难改变或伪造.鲁棒性要求高的应用，通常也需要很强的抗窜改性.在版权保护中，要达到好的抗窜改性是比较困难的.

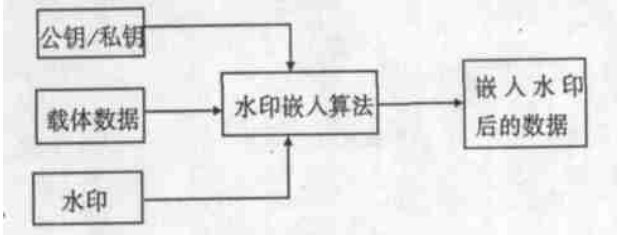

图 1 一般数字水印嵌入方案示意图

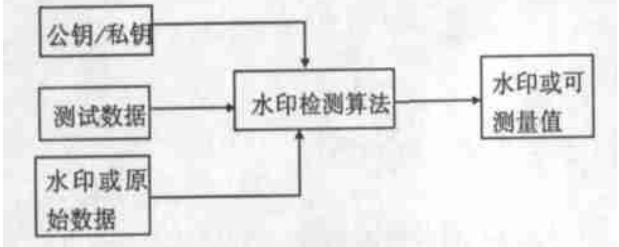

图 2 一般数字水印恢复方案示意图

4) 水印容量 嵌入的水印信息必须足以表示多媒体内容的创建者或所有者的标志信息，或是购买者的序列号.这样在发生版权纠纷时，创建者或所有者的信息用于标示数据的版权所有者，而序列号用于标示违反协议而为盗版提供多媒体数据的用户.

5) 安全性 应确保嵌入信息的保密性和较低的误检测率.水印可以是任何形式的数据，比如数值、文本、图像等.所有的水印都包含一个水印嵌入系统和水印恢复系统.水印的嵌入和提取过程分别如图 1、图 2 所示

6) 低错误率 即使在不受攻击或者无信号失真的情况下，也要求不能检测到水印(漏检、false－negative)以及不存在水印的情况下，检测到水印(虚检、false－positive)的概率必须非常小.

3 数字水印算法

近几年来，数字水印技术研究取得了很大的进步，见诸于文献的水印算法很多，这里对一些典型的算法进行了分析.

3.1 空间域算法

数字水印直接加载在原始数据上，还可以细分为如下几种方法[1~4]：

1) 最低有效位方法(LSB)这是一种典型的空间域数据隐藏算法，L·F·Tumer 与 R·G·Van Schyadel 等先后利用此方法将特定的标记隐藏于数字音频和数字图像内.该方法是利用原始数据的最低几位来隐藏信息(具体取多少位，以人的听觉或视觉系统无法察觉为原则).LSB 方法的优点是有较大的信息隐藏量，但采用此方法实现的数字水印是很脆弱的，无法经受一些无损和有损的信息处理，而且如果确切地知道水印隐藏在几位 LSB 中，数字水印很容易被擦除或绕过.

2) Patchwork 方法及纹理块映射编码方法

这两种方法都是 Bender 等提出的.Patchwork 是一种基于统计的数字水印，其嵌入方法是任意选择 N 对图像点，在增加一点亮度的同时，降低另一点的亮度值.该算法的隐藏性较好，并且对有损的 JPEG 和滤波、压缩和扭转等操作具有抵抗能力，但仅适用于具有大量任意纹理区域的图像，而且不能完全自动完成.

3.2 变换域算法

基于变换域的技术可以嵌入大量比特数据而不会导致可察觉的缺陷，往往采用类似扩频图像的技术来隐藏数字水印信息.这类技术一般基于常用的图像变换，基于局部或是全部的变换，这些变换包括离散余弦变换(DCT)、小波变换(WT)、傅氏变换(FT 或 FFT)以及哈达马变换(Hadamard transform)等等.其中基于分块的 DCT 是最常用的变换之一，现在所采用的静止图像压缩标准 JPEG 也是基于分块 DCT 的.最早的基于分块 DCT 的一种数字水印技术方案是由一个密钥随机地选择图像的一些分块，在频域的中频上稍稍改变一个三元组以隐藏二进制序列信息.选择在中频分量编码是因为在高频编码易于被各种信号处理方法所破坏，而在低频编码则由于人的视觉对低频分量很敏感，对低频分量的改变易于被察觉.该数字水印算法对有损压缩和低通滤波是稳健的.另一种 DCT 数字水印算法[5]是首先把图像分成 8×8 的不重叠像素块，在经过分块 DCT 变换后，即得到由 DCT 系数组成的频率块，然后随机选取一些频率块，将水印信号嵌入到由密钥控制选择的一些 DCT 系数中.该算法是通过对选定的 DCT 系数进行微小变换以满足特定的关系，以此来表示一个比特的信息.在水印信息提取时，则选取相同的 DCT 系数，并根据系数之间的关系抽取比

特信息.除了上述有代表性的变换域算法外，还有一些变换域数字水印方法，它们当中有相当一部分都是上述算法的改进及发展，这其中有代表性的算法是 I·Podichuk 和 ZengWenjun 提出的算法[6].他们的方法是基于静止图像的 DCT 变换或小波变换，研究视觉模型模块返回数字水印应加载在何处及每处可承受的 JND(Just Noticeable Difference，恰好可察觉差别)的量值(加载数字水印的强度上限)，这种水印算法是自适应的.

3.3　NEC 算法

该算法由 NEC 实验室的 Cox[5]等人提出，该算法在数字水印算法中占有重要地位，其实现方法是，首先以密钥为种子来产生伪随机序列，该序列具有高斯 N(0,1)分布，密钥一般由作者的标识码和图像的哈希值组成，其次对图像做 DCT 变换，最后用伪随机高斯序列来调制(叠加)该图像除直流分量外的 1 000 个最大的 DCT 系数.该算法具有较强的鲁棒性、安全性、透明性等.由于采用特殊的密钥，故可防止 IBM 攻击，而且该算法还提出了增强水印鲁棒性和抗攻击算法的重要原则，即水印信号应该嵌入源数据中对人感觉最重要的部分，这种水印信号由独立同分布随机实数序列构成，且该实数序列应具有高斯分布 N(0,1)的特征.随后 Podilchuk 等利用人类视觉模型又对该算法进行了改进，从而提高了该算法的鲁棒性、透明性等.

3.4　其他一些水印算法

1) 近年来，利用混沌映射模型实现数字水印、保密通信等成为混沌应用研究的热点.特别是自从 Cox 等借用通信技术中的扩频原理将水印信号嵌入到一些 DCT 变换系数或者多层分解的小波变换系数以来，人们已经提出了一些混沌数字水印方法.水印的嵌入与检测是基于人类视觉系统(HVS)的亮度掩蔽特性和纹理掩蔽特性，折衷水印的不可见性和鲁棒性之间的矛盾.结果表明：该方法嵌入的水印具有不可见性和鲁棒性，并且这种基于密钥的混沌水印方法更好的抗破译性能.

2) 目前比较流行的还有一种基于盲水印检测的 DWT 算法，该算法首先对原始图像进行小波变换，根据人类具有的视觉掩蔽特性对低频分量进行一定的量化，同时可不影响视觉效果，并对作为水印的图像进行压缩和二值化处理，形成一维的二值序列，根据二值序列的值对上述量化后的原始信号的低频分量进行视觉阈值范围内允许的修改，从而实现水印的嵌入.水印提取过程是对含有水印的图像进行小波变换，对低频分量同样进行量化处理，为了增大算法的安全性，可以对水印形成的二值 0，1 序列在嵌入前进一步进行伪随机序列调制，相应的在水印提取过程需要增加用伪随机序列解调的步骤.这样，不知道伪随机序列的攻击者即使推测出水印的嵌入规律，也无法提取水印.大大增加了水印系统的透明性和鲁棒性.

4　水印技术的局限

目前水印技术的局限，为了对版权保护中使用水印的成功可能性进行评估，看能否满足实际应用需求，就需要对水印技术有更多了解.下面介绍数字水印方案普遍存在的一些局限：

1) 不知道能够隐藏多少位.尽管非常需要知道指定大小载体信息上可以隐藏多少比特的水印信息，但这个问题还没有得到圆满解决.事实上，对给定尺寸的图像或者给定时间的音频，可以可靠隐藏信息量的上界，目前还不清楚.对图像水印，只能说目前使用的算法可以隐藏几百比特位的水印信息.

2) 还没有真正健壮的盲图像水印算法.对图像水印，鲁棒性还是个问题.目前还没有能够在经过所有普通图像处理变换后，仍能幸免的盲水印算法.尤其是能够抵抗几何处理的攻击，被认为是很难实现的目标.

3) 所有者能去除标记.迄今为止提出的所有盲图像水印，实际上都是可逆的.已知水印的准确内容、以及水印的嵌入和检测算法，则总能在没有严重损坏资料的前提下，使水印不可读取.目前还不清楚这个缺点在将来还是否存在；同时在设计版权保护系统时，必须考虑如下问题：一旦水印内容已知，则有可能去除水印或者部分水印.

此外，迄今为止提出的水印算法，其可逆性使人们提出极大的疑问，即设计能够抗篡改的健壮公开水印技术是否可能？事实上，如果允许任何人读取水印，则任何人只要知道水印嵌入算法，就可以消除水印.

5　结　论

随着电子商务的加速发展和网络用户的直线增长，媒体的安全要求将更加迫切，作为版权保护和安全认证的数字水印技术具有极大的商业潜力，作为一门学科交叉的新兴的应用技术，它的研究涉

及了不同学科研究领域的思想和理论，如数字信号处理、图像处理、信息论、通信理论、密码学、计算机科学及网络、算法设计等技术，以及公共策略和法律等问题，是近几年来国际学术界才兴起的一个前沿研究领域，得到了迅速的发展．但数字水印技术仍然是一个未成熟的研究领域，还有很多问题需要解决，其理论基础依然薄弱．随着一些先进的信号处理技术和密码设计思想的引进，必将日趋成熟且得到更为广泛的发展应用．

参考文献：

[1] Eepa Kundur． Dimitrios hatzinakos． Digital watermarking for telltale tamper proofing and authentication[J]． Proceeding of the IEEE．1999， 87(7)：1167～1180．

[2] 张春田，苏育挺．信息产品的版权保护技术——数字水印[J]．电信科学，1998，14(12)：15～17．

[3] Bender W， Gruhl D． Techniques for data hiding[J]．IBM system journal，1996，35(3～4)：313～336．

[4] Cox I J， Killian J，Leighton F T． Secure spread spectrum watermarking for multimedia[J]． IEEE transactions on image processing，1997，6(12)：1673～1687．

[5] Zhao J， Koch E． Embedding robust labels into images for copyright protection[A]． In：Proceedings of the knowright '95 conference on intellectual property rights and new technologies [C]． Vienna， Austria， 1995．241～251．

[6] Podilchud C I， Zeng W． Image—adaptive watermarking using visual model[J]． IEEE journal on special areas in communications，1998，16(4)：525～539．

A Review on the Development of Watermarking Technology

SHI Hong-qin，XIE Xin

(School of Information Engineering，East China Jiaotong University， Nanchang 330013， China)

Abstract：In the paper， we firstly analyze the character of watermarking technology and then set forth the principle of watermarking． Secondly we discuss the algorithms of watermarking in detail． Finally we divide and make a discussion on some limits of watermarking techniques and give the expectation of its development．

Key words：copyright protection； digital watermarking； algorithms of watermarking