数字水印综述

赵 翔， 郝 林
(云南大学 信息学院， 云南 昆明 650091)

摘 要：数字水印将感觉不到的信号嵌入到声频、视频和图像中以实现不同的目的。例如：添加标题和版权保护。首先介绍了有关数字水印的基本原理、重要属性及其主体框架。然后，将数字水印按不同角度划分为不同种类。讨论了各种各样的数字水印算法以及数字水印在不同领域的应用，并简要介绍了对数字水印的攻击。最后，给出了数字水印当前的研究现状和发展形式及前景。

关键词：数字水印； 信息隐藏； 水印嵌入； 水印提取； 水印验证
中图法分类号：TP309 **文献标识码**：A **文章编号**：1000-7024 (2006) 11-1946-05

Overview of digital watermark

ZHAO Xiang, HAO Lin
(School of Information, Yunnan University, Kunming 650091, China)

Abstract: A digital watermark embeds an imperceptible signal into data such as audio, video and images, for different purposes, including captioning and copyright control. First, the basic principle, important properties and the main frame of digital watermarks are introduced. Then the digital watermark is classified into different types according to various aspects. Further more, various digital watermarking algorithms and its applications in different fields are analyzed. And the attacks on digital watermark are also simply introduced. Finally, the recent and future research in this field and the prospect of this technology are given.

Key words: digital watermark; information hiding; watermark insertion; watermark extraction; watermark verification

0 引 言

当前，计算机的普及使得很多文学或艺术作者直接将作品以数字方式记录和存储下来，而网络的飞速发展也为数字作品的传输提供了便利。这些条件使得数字作品与传统作品相比，在创作和传播上具有很大的优越性。数字作品具有极易被理想复制的特性，这是其能够被快速传播的重要原因之一，但这一特性也会被侵权者非法利用。目前，盗版已成为对数字化产业最大的威胁，这在相当程度上阻碍了其自身的发展，对数字媒体版权所有者来说，反盗维权的要求迫在眉睫，而数字作品的版权保护不仅仅是一个立法问题，也是一个技术问题。

传统的加密方法对多媒体内容的保护和完整性认证也具有一定的局限性。首先，加密方法只用在通信的信道中，一旦被解密，则信息就完全变成明文；另外，密码学中的完整性认证是通过数字签名方式实现的，它并不是直接嵌到多媒体信息之中，因此无法察觉信息在经过加密系统之后的再次传播与内容的改变。这样，数字水印技术作为加密技术的补充，在多媒体信息的版权保护与完整性认证方面得到了迅猛的发展。

数字水印是新近提出的一种版权保护手段。它是利用数字作品中普遍存在的冗余数据与随机性把版权信息嵌入在数字作品本身，从而起到保护数字作品版权的一种技术。数字水印可以标识和验证出数字化图像，视频和声频记录的作者、所有者、发行者或授权消费者的信息，还可追溯数字作品的非法分发，是目前进行数字作品版权保护的一种较为有效的技术手段。

1 数字水印技术的基本原理

数字水印的思想源于古代的隐写术，是通过一定的算法将一些标志性信息直接嵌到多媒体内容当中，但不影响原内容的价值和使用，并且不能被人的知觉系统觉察或注意到。水印信息可以是作者的序列号、公司标志或有特殊意义的文本等，可用来识别文件、图像或音乐制品的来源、版本、原作者、拥有者、发行人或合法使用人对数字产品的拥有权。与加密技术不同，数字水印技术并不能阻止盗版活动的发生，但它可以判别对象是否受到保护，监视被保护数据的传播、真伪鉴别、非法拷贝、解决版权纠纷并为法庭提供证据。

为了给攻击者增加去除水印的难度，目前大多数水印制

收稿日期：2005-04-30。
基金项目：云南省自然科学基金项目 (2002F0010M)；云南省信息网络开发技术专项计划基金项目 (2004IT06)。
作者简介：赵翔 (1980－)，男，云南昆明人，硕士研究生，研究方向为信息安全；郝林 (1955－)，男，山东日照人，教授，研究方向为信息安全和人工智能。

作方案都采用密码学中的加密(包括公开密钥和私有密钥)体系来加强,在水印的嵌入和提取时采用一种密钥,甚至几种密钥联合使用。

数字水印的特性如下:

(1)透明性:对于以模拟方式存储和分发的信息(如电视节目),或是以物理形式存储的信息(如报刊、杂志),用可见的标志就足以表明其所有权。但在数字方式下,标志信息极易被修改或擦除。因此应根据多媒体信息的类型和几何特性,利用用户提供的密钥将水印隐藏到一系列随机产生的位置中,使人无法察觉。

(2)鲁棒性:水印必须对一般的信号处理操作(如滤波、平滑、增强和有失真压缩等)、删除攻击和迷惑攻击等具有鲁棒性。除非对数字水印具有足够的先验知识,任何破坏和消除水印的企图都将严重破坏多媒体信息的质量。

(3)不可检测性:包括两方面的含义:①水印信息与原始载体数据具有一致的特性,使攻击者无法通过信息分析手段判断多媒体数据中是否存在水印;②水印信息本身具有不可统计性,避免攻击者通过统计多个多媒体数据进而分析存在的相似性来进行攻击。

(4)安全性:指水印嵌入算法具有较强的抵抗攻击的能力,能够承受一定程度的人为攻击而使水印不会被破坏。

(5)自恢复性:经过一些操作或者变换之后,可能会使原始载体数据产生较大的破坏,如果从留下的片断数据能够恢复信号,就是所谓的自恢复性。

2 数字水印的框架

数字水印是将一些诸如水印、数字签名、标签或者商标等水印信息嵌入到多媒体对象中以至于事后水印能够被检测或提取出来的一个过程,从而能够证明多媒体对象的所有权。多媒体对象可以是图像、音频或者视频。数字水印的一个简单例子就是一个可见的印章被置于图像上来标示版权。然而,水印可能还包含一些附加信息,这些附加信息又包含了多媒体对象副本购买者的身份标示。

通常,任何一个数字水印算法都由3部分组成:①水印;②编码器(也称之为嵌入算法);③解码器和比较器(也称之为验证算法,还可以称之为提取算法或检测算法)。每一个所有者都有惟一的水印,或者一个所有者能够将不同的水印嵌入到不同的对象中。嵌入算法将水嵌入到对象中,把水印和对象合为一体。验证算法用于鉴别对象以决定其所有者和其完整性。

2.1 编码过程

我们用I来表示图像,用$S=s_1,s_2,\cdots$来表示签名,也称为水印,用I'来表示嵌入水印后的图像。E是编码函数,它接受图像I和签名S,生成新的嵌入水印的图像I',其数学描述为

$$E(I,S)=I' \tag{1}$$

值得注意的是水印S也许依赖于图像I。此时,由(1)式描述的编码过程仍然有效。图1展示了编码的过程。

2.2 解码过程

解码函数D接受输入图像J,然后从图像J恢复出水印S'。图像J可以是被嵌入水印或者未被嵌入水印的图像,也可能是被损坏的图像,其所有权有待确定。在此过程中,还包含一个

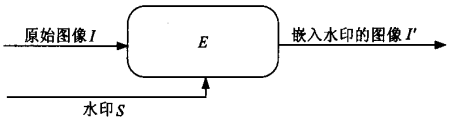

图1 编码过程

附加的图像I,图像I通常是J的未被嵌入水印的原始图像。这是由于在实际当中,一些编码策略可能会利用原始图像来提供额外的健壮性以使其能够抵抗有意或无意的像素损坏。

其数学描述为

$$D(J,I)=S' \tag{2}$$

被提取的水印S'将会通过比较函数C_Q来与所有者的签名序列比较,然后产生一位二进制输出。如果签名匹配,则输出为1,其它则输出为0,可以用公式表示为

$$1, c\leqslant Q$$

$$C_Q(S',S)=0, \text{其它}$$

这里C是相关器,$x=C_Q(S',S)$。c是两个水印S'和S的相关性,Q是确定的阀值。为不失一般性,水印策略可以被描述为一三元组(E,D,C_Q)。图2展示了解码的过程,图3展示了验证的过程。

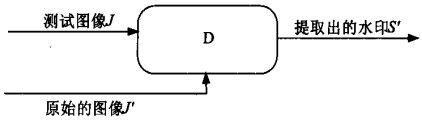

图2 解码过程

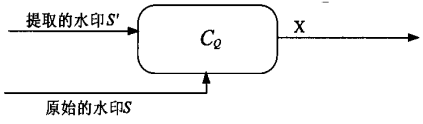

图3 验证过程

水印必须能够被检测或提取出来。根据水印嵌入的方式和水印算法的本质,各种水印策略可以是大不相同的。在一些水印策略中,水印能够从图像中提取出来,这个过程称为水印提取。在另一些策略中,仅仅只能检测出特定的水印是否被嵌入图像,这个过程称为水印检测。值得注意的是,水印提取能够证明所有权,而水印检测就仅仅只能证明所有权。

3 数字水印的类型

数字水印技术可以从不同的角度进行划分。

(1)按特性划分

按水印的特性可以将数字水印分为鲁棒数字水印和脆弱数字水印两类。鲁棒数字水印主要用于在数字作品中标识著作权信息,如作者、作品序号等,它要求嵌入的水印能够经受各种常用的编辑处理;脆弱数字水印主要用于完整性保护,与鲁棒水印的要求相反,脆弱水印必须对信号的改动很敏感,人们根据脆弱水印的状态就可以判断数据是否被篡改过。

(2)按水印所附载的媒体划分

按水印所附载的媒体,我们可以将数字水印划分为图像

水印、音频水印、视频水印、文本水印以及用于三维网格模型的网格水印等。随着数字技术的发展，会有更多种类的数字媒体出现，同时也会产生相应的水印技术。

(3)按检测过程划分

按水印的检测过程可以将数字水印划分为明文水印和盲水印。明文水印在检测过程中需要原始数据，而盲水印的检测只需要密钥，不需要原始数据。一般来说，明文水印的鲁棒性比较强，但其应用受到存储成本的限制。目前学术界研究的数字水印大多数是盲水印。

(4)按内容划分

按数字水印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个数字图像（如商标图像)或数字音频片段的编码；无意义水印则只对应于一个序列号。有意义水印的优势在于，如果由于受到攻击或其它原因致使解码后的水印破损，人们仍然可以通过视觉观察确认是否有水印。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。

(5)按用途划分

不同的应用需求造就了不同的水印技术。按水印的用途，我们可以将数字水印划分为票据防伪水印、版权保护水印、篡改提示水印和隐蔽标识水印。①票据防伪水印是一类比较特殊的水印，主要用于打印票据和电子票据的防伪。一般来说，伪币的制造者不可能对票据图像进行过多的修改，所以，诸如尺度变换等信号编辑操作是不用考虑的。但另一方面，人们必须考虑票据破损、图案模糊等情形，而且考虑到快速检测的要求，用于票据防伪的数字水印算法不能太复杂；②版权标识水印是目前研究最多的一类数字水印。数字作品既是商品又是知识作品，这种双重性决定了版权标识水印主要强调隐蔽性和鲁棒性，而对数据量的要求相对较小；③篡改提示水印是一种脆弱水印，其目的是标识宿主信号的完整性和真实性；④隐蔽标识水印的目的是将保密数据的重要标注隐藏起来，限制非法用户对保密数据的使用。

(6)按水印隐藏的位置划分

按数字水印的隐藏位置，我们可以将其划分为时(空)域数字水印、频域数字水印、时/频域数字水印和时间/尺度域数字水印。时(空)域数字水印是直接在信号空间上叠加水印信息，而频域数字水印、时/频域数字水印和时间/尺度域数字水印则分别是在DCT变换域、时/ 频变换域和小波变换域上隐藏水印。

随着数字水印技术的发展，各种水印算法层出不穷，水印的隐藏位置也不再局限于上述4种。应该说，只要构成一种信号变换，就有可能在其变换空间上隐藏水印。

4 典型数字水印算法

近年来，数字水印技术研究取得了很大的进步，下面对一些典型的算法进行了分析，除特别指明外，这些算法主要针对图像数据(某些算法也适合视频和音频数据)。

(1) 空域算法。该类算法中典型的水印算法是将信息嵌入到随机选择的图像点中最不重要的像素位 (least significant bits, LSB)上，这可保证嵌入的水印是不可见的。但是由于使用了图像不重要的像素位，算法的鲁棒性差，水印信息很容易为滤波、图像量化和几何变形等操作破坏。另外一个常用方法是利用像素的统计特征将信息嵌入像素的亮度值中。Patchwork算法方法是随机选择N对像素点 (a_i,b_i)，然后将每个a_i点的亮度值加 1，每个b_i点的亮度值减 1，这样整个图像的平均亮度保持不变。适当地调整参数，Patchwork方法对JPEG压缩、FIR滤波以及图像裁剪有一定的抵抗力，但该方法嵌入的信息量有限。为了嵌入更多的水印信息，可以将图像分块，然后对每一个图像块进行嵌入操作。

(2)换域算法。该类算法中，大部分水印算法采用了扩展频谱通信(spread spectrum communication)技术。算法实现过程为：先计算图像的离散余弦变换 (DCT)，然后将水印叠加到DCT域中幅值最大的前 k 系数上(不包括直流分量)，通常为图像的低频分量。若 DCT 系数的前 k 个最大分量表示为 $D=\{d_i\},i=1,\cdots,k$，水印是服从高斯分布的随机实数序列 $W=\{w_i\},i=1,\cdots,k$，那么水印的嵌入算法为 $d_i=d_i(1+aw_i)$，其中常数 a 为尺度因子，控制水印添加的强度。然后用新的系数做反变换得到水印图像 I。解码函数则分别计算原始图像 I 和水印图像 I*的离散余弦变换，并提取嵌入的水印 W*，再做相关检验 $W\bullet W^*/\sqrt{W\bullet W}$ 以确定水印的存在与否。该方法即使当水印图像经过一些通用的几何变形和信号处理操作而产生比较明显的变形后仍然能够提取出一个可信赖的水印拷贝。一个简单改进是不将水印嵌入到DCT域的低频分量上，而是嵌入到中频分量上以调节水印的顽健性与不可见性之间的矛盾。另外，还可以将数字图像的空间域数据通过离散傅里叶变换 (DFT)或离散小波变换(DWT)转化为相应的频域系数；其次，根据待隐藏的信息类型，对其进行适当编码或变形；再次，根据隐藏信息量的大小和其相应的安全目标，选择某些类型的频域系数序列(如高频或中频或低频)；再次，确定某种规则或算法，用待隐藏的信息的相应数据去修改前面选定的频域系数序列；最后，将数字图像的频域系数经相应的反变换转化为空间域数据。该类算法的隐藏和提取信息操作复杂，隐藏信息量不能很大，但抗攻击能力强，很适合于数字作品版权保护的数字水印技术中。

(3)压缩域算法。基于JPEG和MPEG标准的压缩域数字水印系统不仅节省了大量的完全解码和重新编码过程，而且在数字电视广播及(video on demand, VOD)中有很大的实用价值。相应地，水印检测与提取也可直接在压缩域数据中进行。下面介绍一种针对MPEG-2压缩视频数据流的数字水印方案。虽然MPEG-2数据流语法允许把用户数据加到数据流中，但是这种方案并不适合数字水印技术，因为用户数据可以简单地从数据流中去掉，同时，在MPEG-2编码视频数据流中增加用户数据会加大位率，使之不适于固定带宽的应用，所以关键是如何把水印信号加到数据信号中，即加入到表示视频帧的数据流中。对于输入的MPEG-2数据流而言；它可分为数据头信息、运动向量(用于运动补偿)和DCT编码信号块3部分，在方案中只有MPEG-2数据流最后一部分数据被改变，其原理是，首先对DCT编码数据块中每一输入的Huffman码进行解码和逆量化，以得到当前数据块的一个DCT系数；其次，把

相应水印信号块的变换系数与之相加，从而得到水印叠加的DCT系数，再重新进行量化和Huffman编码，最后对新的Huffman码字的位数 n1 与原来的无水印系数的码字 n0 进行比较，只在 n1 不大于 n0 的时候，才能传输水印码字，否则传输原码字，这就保证了不增加视频数据流位率。该方法有一个问题值得考虑，即水印信号的引入是一种引起降质的误差信号，而基于运动补偿的编码方案会将一个误差扩散和累积起来，为解决此问题，该算法采取了漂移补偿的方案来抵消因水印信号的引入所引起的视觉变形。

(4) NEC 算法。该算法由 NEC 实验室的 Cox 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(DC)分量外的 1 000 个最大的 DCT 系数。该算法具有较强的鲁棒性、安全性和透明性等。由于采用特殊的密钥，因此可防止 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，且该实数序列应该具有高斯分布 N(0,1)的特征。

(5)生理模型算法。人的生理模型包括人类视觉系统(human visual system, HVS)和人类听觉系统 HAS。该模型不仅被多媒体数据压缩系统利用，同样可以供数字水印系统利用。利用视觉模型的基本思想均是利用从视觉模型导出的(just noticeable difference, JND)描述来确定在图像的各个部分所能容忍的数字水印信号的最大强度，从而能避免破坏视觉质量。也就是说，利用视觉模型来确定与图像相关的调制掩模，然后再利用其来插入水印。这一方法同时具有好的透明性和强健性。

5 数字水印的应用

多媒体技术的飞速发展和 Internet 的普及带来了一系列政治、经济、军事和文化问题，产生了许多新的研究热点，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) 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、视频和三维动画)的版权保护是当前的热点问题。由于数字作品的拷贝或修改非常容易，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志不可见或不可听，既不损害原作品，又达到了版权保护的目的。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 1 200 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、支票以及其它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4 000万美元的假钞中，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，会出现大量过度性的电子文件，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、录音和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。

(4) 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，引起了许多国家的重视。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进行保密数据传送。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，然而，经过加密的文件往往是混乱无序的，容易引起攻击者的注意。网络多媒体技术的广泛应用使得利用公用网络进行保密通信有了新的思路，利用数字化声像信号相对于人的视/听觉冗余，可以进行各种时(空)域和变换域的信息隐藏，从而实现隐蔽通信。

6 数字水印的攻击

嵌入水印的图像常常受到某些处理。例如，压缩和传输的噪声、复制和滤波等。现归纳如下：

(1) 有损压缩：许多如同 JPEG 和 MPEG 的压缩策略会造成不可恢复的数据丢失，从而潜在地降低了数据的质量。

(2) 几何变形：几何变形尤其是对于图像视频包含了旋转、平移、缩放和复制等操作。

(3) 普通的信号处理操作：包含数/模转换、模/数转换、重采样、重量子化、抖动变形、重压缩、线性滤波、非线性滤波、色彩缩减、附加像素值偏移、附加高斯噪声、附加非高斯噪声和像素交换。

(4) 其它有意攻击：①印刷和重扫描；②重水印；③共谋：合法授权的用户用嵌入不同水印的图像副本，通过一定算法生成未嵌入水印的图像；④伪造：合法授权的用户使用有效的水

印来生成嵌入水印图像的副本;⑤IBM攻击:制作原件的赝品,使其能够像原件一样使用,其伪造水印也能够被提取。

7 数字水印技术研究现状

自 Schyndel 在 1994 年提出基于 LSB 的水印算法[5]以来,数字水印领域涌现出大量的水印嵌入和检测方法。这些方法大致可以分为空间域方法和变换域方法两种。其中,变换域算法需要先对源数据进行一个变换,然后在变换域中完成水印的嵌入和检测,因而往往会需要较大的运算量。但是,由于压缩、滤波等图像处理的过程经常也是在变换域完成,如果处理的过程和水印信号嵌入使用相同的变换域,那么这些处理对数字水印的影响将可以被大大地降低。例如,将图像进行DCT变换后再在变换域嵌入水印,就可以提高水印系统抵抗 JPEG 压缩处理的能力。因此,选择一个合适的变换操作,然后在该变换域嵌入水印,则可以提高水印嵌入系统的鲁棒性。

目前,数字水印的研究从结构层次上可分为基础理论研究、应用基础研究和应用技术研究3个层次:①基础理论研究:主要针对感知理论、信息隐藏及其数字水印模型、理论框架等;②应用基础研究:主要方向是针对声音、图像和视频等多媒体信号,研究相应的数字水印隐藏算法和检测算法,以及能够抵抗仿射变换、滤波、重采样、色彩抖动和有损压缩的鲁棒的数字水印技术;③应用技术研究:以实用化为主要目的,研究各种多媒体格式的数字水印算法。

目前,虽有一些研究算法和技术可以抵抗常见的噪声干扰、JPEG 有损压缩等,但对于抵抗剪切、缩放、旋转、最新的 JPEG 2000 压缩标准及A/D、D/A变换等处理和攻击却很少,尤其是不能抵抗信号处理和几何变换的联合攻击。

在进一步的应用中,迫切需要可以抵抗旋转、缩放和平移的数字水印技术以及不需原图像的盲检测,需要检测出的水印有数字、二值图、灰度图和彩色图,这些构成了第 2 代数字水印技术。根据数字水印技术的不可感知性和鲁棒性等特点,数字水印会在更为广阔的领域得到新的应用,如在印刷防伪中的应用。当然,这需要研究更为鲁棒的数字水印技术。在技术上除要满足第 1、第 2 代数字水印技术的特性外,还需要抵抗A/D和D/A变换、非线性量化、色彩失真、仿射变换和投影变换等攻击,且必须与打印扫描原理或印刷原理及工艺相结合。这在理论上和算法设计上都提出了更富有挑战性的课题。

总的说来,水印技术的研究已经取得了相当的成绩,但是在水印技术进一步的研究和应用方面(本文关心的是图片资产版权保护这一特定应用)还有很多的路要走。首先,目前对显式水印的研究是水印技术一个比较劣势的领域。另外,水印技术的研究应该和相关技术的研究保持紧密的联系,对于图片资产的水印技术而言,应该充分借鉴目前图片处理中用到的技术,例如小波分析的使用等。

8 结束语

数字水印技术是近几年来国际学术界兴起的一个前沿研究领域。它与信息安全、信息隐藏和数据加密等均有密切的关系。特别是在网络技术和应用迅速发展的今天,水印技术的研究更具现实意义。

今后水印技术的研究仍将着重于顽健性、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。水印的顽健性能体现了水印在数字文件中的生存能力,当前的绝大多数算法虽然均具有一定的顽健性,但是如果同时施加各种图像攻击,那么这些算法均会失效。如何寻找更加顽健的水印算法仍是一个急需解决的问题。另外当前的水印算法在提供可靠的版权证明方面或多或少有一定的不完善性,因此寻找能提供完全版权保护的数字水印算法也是一个重要的研究方向。

参考文献:

[1] Saraju P Mohanty.Digital watermarking:A tutorial review[EB/OL] *.http://citeseer.ist.psu.edu/cache/papers/cs/27454/http: zSzzSzwww.csee.usf.eduzSz~smohantyzSzresearchzSzReportszSzWMSurvey1999Mohanty.pdf/mohanty99digital.pdf.*

[2] Petitcolas F A P.Information hiding-A survey [J]. *Proceedings of the IEEE*, 1999, 87(7):1062-1078.

[3] Moulin P,Mihcak M K.A framework for evaluating the datahiding capacity of image sources[J]. *IEEE Trans on I mage Processing*, 2002, (11):1029-1042.

[4] Swanson M D. Multimedia data embeddingand watermarking technologies[J].*Proc of the IEEE*, 1998,86(6):1064-1087.

[5] Yeung M M. Digital watermarking [J]. *Communications of the ACM*, 1998,41(7):31-33.

[6] Eggers J,Buml R,Girod B.A communications approach to image steganography[C]. *San Jose,USA: Proceedings of SPIE:Electronic Imaging* 2002, *Security and Watermarking of Multimedia Contents IV*, 2002.26-37.

[7] Mintzer F.Opportunities for watermarking standards[J]. *Communications of the ACM*, 1998,41(7):57-64.

[8] P'erez-Gonz'alez F,Balado F,Hern' andez J R.Performance analysis of existing and new methods for data hiding with known host information in additive channels[J]. *IEEE Trans on Signal Processing, Special Issue on Signal Processing for Data Hiding in Digital Media and Secure Content Delivery*, 2003,51(4): 598-635.

[9] Hartung F, Kitter M. Multimedia watermarking techniques [J]. *Proceedings of the IEEE*, 1999,87(7):1079-1107.

[10] Wolfgang R B.Perceptual watermarking for digital Images and video[J]. *Proceedings of the IEEE*, 1999,87(7):1108-1126.

[11] Voyatzis G, Pitas I. The use of watermarks in the protection of digital multimedia products[J]. *Proceedings of the IEEE*, 1999, 87(7):1197-1207.

[12] Hsu C T,Wu J L.Hidden digital watermarks in images[J]. *IEEE Trans on Image Processing*, 1999,8(1):58-68.

[13] Chen B,Wornell G W.Quantization index modulation: A class of provably good methods for digital watermarking and information embedding [J]. *IEEE Trans on Information Theory*, 2001, (47): 1423-1443.