中华博士园地

这是本刊特为海内外正在就读和学成立业的博士、博士后青年学者们开辟的一片科普园地。深学浅著是一门德识、慧学、素质修养的学问。你们的新知识、新调研、新观察、新目光、新展望,能够用尽可能深入浅出、通俗流畅的语言,汇报给祖国人民、家乡父老子弟乡亲们吗?中华博士园地,乃耕耘忠孝之地,科教兴国、民族昌盛之地。要用慈母听得懂的语言,写出你们的心声!

数字水印——知识产权保护的新技术

陈 青 王延平

(武汉大学电子信息工程系,武汉 430072)

0 引 言

多媒体存储与传输技术的进步,尤其是因特网技术的盛行,带来了数字媒体应用的迅速增长。数字媒体有着一些模拟媒体不可比拟的优点,如数字信号很容易进行编辑和可以方便、便宜、无失真地被复制,数字声音、文本、图象和视频易于通过电子的(网络)或物理的(CD-ROM)系统低价高效地迅速传输和分配等,这些优点为电子图书馆、在线服务和电子商业等先进的多媒体服务提供了广阔的发展前景。但这些优点,也使与数字网络和多媒体信息相关的版权盗用问题显著增加。盗用者通过非法手段获取网络中的传输数据,修改数据内容。生产和再传输复制品等[1,2],这些都可能给被盗用者带来巨大的经济损失,并对安全权限造成强烈的冲击。因此怎样更好地保护图象、文本、声音和视频等数字媒体的知识产权就变得十分迫切了。

不过一种新的防盗版技术——"数字水印"技术,也因为数字媒体的上述优点而成为可能。数字水印的概念最初是由 Caronni 于 1993 年提出来的,并用于图象数字水印,此后,研究人员将数字水印的概念扩展到声音和视频等其它数字媒体,数字水印也日益成为一个非常活跃的研究领域。由于数字水印技术在版权保护、数据鉴别、数据监测等领域有着广泛的应用前景,因此引起工业界的浓厚兴趣。在版权保护方面,数字水印方法解决的是数字媒体版权保护三个层次(包括进入控制、使用权控制和设置识别标记)的技术中最后一个层次即设置识别标记的问题,其工作原理就是通过内嵌不可感知的信息到声音和视频等信号中,来确认版权所有者,并用检测和跟踪侵权行为。与传统发票上的水印不同的是,数字水印只能通过适当的软件检测。

另一种比较常用的防止非法复制的技术是密码学。通过设置密码,使数据在传输时变得不可读,可以给处于从发送到接收过程中的数据提供有效的保护。不过密码技术所能提供的保护其实是有限的或

陈 青 武汉大学电子信息工程学院博士生。主要从事图象处理,数学水印,图象编码和小波变换等方面的研究。

者说不完全的，因为一旦在接收端被解码后，这种保护就不存在了。新近的数字水印技术正好弥补了密码技术的这一不足，它通过将一信号直接内嵌到数据中，可以为解码的数据提供进一步的保护。数字水印的目的不在于限制或控制数据的获取，而是确保水印能总是不受侵犯并可恢复地留在数据中，从而确认所有权和跟踪侵权行为。

其实在数字水印技术之前，人们已经在关注数据隐藏和标记之类的技术，但早期的研究重点在数据隐藏上，因为当时预想的应用还没有涉及通过信号失真或有意的破坏来删除隐藏的数据等问题，那些方法在技术设计上都没有考虑版权标记的鲁棒性。然而随着水印技术在版权保护方面应用的不断增加，水印算法的设计应该特别着重考虑其鲁棒性及如何反篡改的问题。

1　数学水印的主要特性和可能的袭击

1.1　数学水印的主要特性

数学水印是一种鲁棒的数字标记，它被秘密地内嵌到数学信号中以识别发源、所有者、内容、使用权、权利、完整性或终点等。数字水印是叠加到数据中并引起原始数据改变的数字信号。要使版权标记成为可靠的产权识别工具，水印系统一般应该包含版权所有者的标记或代码以及能证实用户合法拥有数据的用户代码等基本信息，而且这些信息要以允许跟踪分配的讣式嵌入。

为了满足应用的要求，水印必须具有以下一些基本特性：

(1) 统计和视觉不可见(即不显著性)。数字水印的嵌入不会引起原始数据质量的明显下降，并且袭击者难于用统计的方法发现和删除水印。

(2) 容易提取。数据所有者应该能很容易地提取水印。

(3) 鲁棒性　袭击者难于用信号处理技术、失真和多次加水印等来破坏、删除水印或伪造数据的版权标记。

(4) 确定性。一般水印应能充分可靠地证明所有者对特定产品的所有权。

(5) 安全性。算法应该能产生大量不同的水印，以避免袭击者通过反复试验或其它不正当的方法恢复水印。只有被授权者能够检测、恢复和修改水印。

但到目前为止，还没有哪一种水印算法能完全满足上述所有要求。

1.2　对于印可能的袭击

水印对数字媒体版权的保护作用有可能由于受到有意或无意的袭击而削弱。对水印的袭击一般有两种基本形式：(1) 改变数据使内嵌于其中的版权标记无法辩认，即降低检测水印的可能性；(2) 降低水印作为指示合法所有权的能力，使内嵌标记不能作为可靠的识别工具。因此，要使水印算法在多媒体环境下有效和切实可行，版权标记必须具有鲁棒性。对水印技术的鲁棒性要求意味着水印应该能抵抗常见的信号处理变换、几何失真及在数据中重复加水印的混淆、伪造等袭击。

(1) 常见的信号处理变换包括：

① JPEG 压缩：JPEG 是近期最广泛地用于图象压缩的算法之一，任何水印系统都应对一定程度的压缩具有弹性。压缩算法将去掉视觉上的不显著信息，而通常正是在这些地方存在水印。为了使算法对 JPEG 压缩具有鲁棒性，有些学者提出将水印置于图象的视觉显著处或设计具有低通性的水印。

② 锐化、平滑、线性及非线性滤波：这些运算虽然会破坏水印，但也使图象质量严重退化。基于低通(均值、中值)滤波的变换可影响具有低通特性的水印信号。锐化函数属于照片编辑软件的标准函数，此类滤波器在检测某些由数字水印引入的高频噪声时非常有效，因而可用于对这些水印算法进行有效的袭击。

③ 亮度、对比度增强技术：这些运算通常并不能阻止水印的检测，相反地，人们常在检测前使用此类变换，以获得较好的效果。

(2) 几何变换的目的只是改变图象的外观，并不降低图象的质量。但却可能使水印变得不可检测，故水印对几何运算具有鲁棒性也就非常重要。常见的几何运算是：

① 剪切：剪切图象的一部分，将使水印不能分布和复制到整幅图象，从而使检测失败。

② 旋转：旋转是在对图象进行扫描后的一种基本变换，它使图象的水平特征的重新排列。小角度的旋转常与剪切相结合，它通常不会改变图象的商业价值，但可能降低水印的可检测性。

③ 尺度变换：在对打印图象进行扫描，或将高清晰度图象作为网络出版等用途时会遇到尺度变换的情况。在当今网络出版越来越流行的趋势下，水印系统的设计中不能忽略尺度变换的影响。尺度变换

通常分为均匀的和非均匀的两种。在均匀情况下水平和垂直方向尺度的变换因子是相同的,而非均匀情况水平和垂直方向用不同的尺度因子。通常的水印算法仅对均匀尺度变换具有鲁棒性。

④ 删除几行或几列:删除几行或几列是一种基本袭击,它对某些版权标记系统和任何在空域中直接使用扩频技术的水印算法是一种非常有效的袭击。

还有与 JPEG 相混合的几何变换。由于大多数艺术家通常首先用几何变换,然后将图象以压缩格式存储,故单独考虑旋转和尺度变换的袭击是不够的,应考虑它们与 JPEG 混合的情况。另外相反的情况,即在 JPEG 压缩后进行几何变换的混合方式也不能忽略,因为它有可能被故意的伪造者所采用。

尽管到目前为止提出的水印算法能处理上述的某些图象运算,但还没有哪一种水印算法能成功地对付上述所有可能的袭击。随机非线性不可感知的几何变换仍然是最具挑战性的,而目前还没有对这个问题进行讨论的文献。

2 数字水印框架、参数、方法及其性能评价

2.1 数字水印框架

一般来说,对数据加水印的处理可看成是由两部分组成的通讯任务:

(1) 水印的嵌入。此过程将水印信号在原始信号上进行调制。为了能成功地提水印信号,算法必须对故意或非故意的袭击和失真(相当于信道噪声)具有鲁棒性。

(2) 水印的检取。此步骤从接收信号或修改的信号中提取水印。

图 1 表示一般的内嵌过程。已知图象 I、水印 W、和密钥 K(通常是随机数发生器的种子),内嵌过程可定义为一种映射:$I\times K\times W\rightarrow I'$。

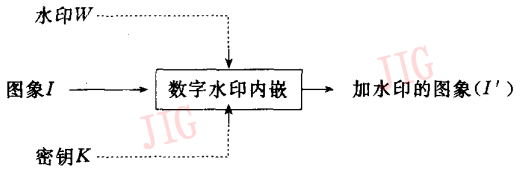

图1 一般的数字水印内嵌框图

一种检测过程如图 2 所示。它的输出为恢复的水印 W 或者是某种置信度测量,表示已知水印在所观察的图象中出现的可能性有多大。

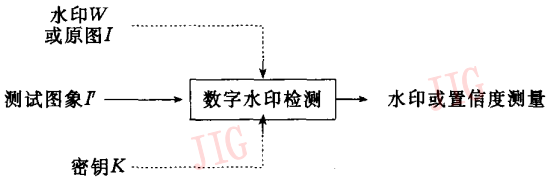

图2 一般的数字水印恢复框图

有几种典型的用输入和输出定义的水印系统:

(1) 私有水印:其检测至少要求提供原始图象。一种类型是从可能已被修改的图象 $\tilde{I}'$ 中提取水印 W,并用原图作为提示寻找在 $\tilde{I}'$ 中何处可能有水印:$(\tilde{I}'\times I\times K\rightarrow W)$;另一种类型的检测过程还要求使用内嵌水印的副本,并对问题"$\tilde{I}'$ 是否包含有水印 W?"作出"是"或"否"的回答:$\tilde{I}'\times I\times K\times W\rightarrow\{0,1\}$。由于其提供的信息少,并要求检测者能得到保密的材料,故此方法可望比其它方法具有更强的鲁棒性[4]。

(2) 半私有水印:其检测不用原图($\tilde{I}'\times K\times W\rightarrow\{0,1\}$),但须回答同样的问题。私有和半私有水印的唯一用途似乎是在法庭上提供证据来证明产品的所有者及其对应用(如 DVD,用户需要知道是否能播放某段内容)的控制权。近期文献中的许多算法[5—9]都属此范畴。

(3) 公有的水印(盲水印):因其检测既不要求保密的原图,也不要求内嵌的水印而成为最具挑战性的问题。此系统从可能已被修改的图象中提取 n 比特水印信息:$\tilde{I}'\times K\rightarrow W$[11,12]。公有水印的应用范围比其它算法要广泛得多,实际上用于公有系统的内嵌算法常可用于私有系统,同时鲁棒性得到改进。

(4) 不对称的水印(公钥水印):任何用户能看到但去不掉的水印。

2.2 数字水印的重要参数和变量

数字水印系统中的参数和变量影响和限制系统的性能。某些参数互为正比或反比的关系,相互制约。下面列出了数字水印系统的一些重要参数及对系统性能影响的一般分析:

(1) 内嵌信息量。这是一个重要的参数,它直接影响水印的鲁棒性。欲内嵌的信息越多,水印的鲁棒性越低,即内嵌信息量的增加会引起鲁棒性的下降。需内嵌的信息量取决于应用。

(2) 内嵌强度(即水印的能量)。通常须在水印

内嵌和图象质量之间进行折衷。鲁棒性的增加要求增大内嵌强度，而这将使图象的视觉质量严重下降。

(3) 数据尺寸和特性。数据尺寸正比于鲁棒性。尽管很小的图象没有很大的商业价值，但却要求水印软件能从中恢复出水印。图象的特性对水印的鲁棒性也是一个冲击，通常对自然具有较高鲁棒性的方法，当应用于合成图象时，其鲁棒性会惊人地减少。一个好的水印系统应适用于广泛的图象尺寸范围，以及不同类型的图象。

(4) 秘密信息(如密钥)。尽管秘密信息并不对图象的视觉精度或水印的鲁棒性构成冲击，但它在系统安全性方面起着重要的作用。密钥空间，即可能的秘密信息取值范围必须足够大，以使袭击耗时而不可能。

2.3　水印算法分类

尽管数字水印是用于知识产权保护的新的研究领域，但与其相关的理论和技术却是一些早已存在的理论和技术的结合，如数据隐藏、扩频通讯技术、知觉概念和噪声理论等。

根据代码嵌入图象的方式，数字水印算法可以分为两大类：一类是直接改变图象数据的空域技术；另一类是变换域技术，此技术图象变换域改变数据，再进行反变换得到加水印的图象。

空域技术的内嵌方法，通常是在图象的亮度或彩色光带、或者这两者之上加一调制信号来内嵌数据。具体说来，这又有好几种方式，一种是叠加一伪随机序列到图象的最低位(LSB)，使其携带水印信息[8,12]，伪随机序列有一相关的密钥可保证水印的安全性；第二种则是从扩频通讯技术发展起来的[13]，通常其水印的检测是通过相关运算实现的；再有一种是，有些学者提出，可以通过改变随机选择的象素值来内嵌数据[14]；此外还有以图象块为基础的内嵌方法[15]等。空域技术的优点是能够较有效地利用人类视觉系统特性，但它的缺陷是：(1) 为了使其对剪切变换具有鲁棒性，空域技术不得不重复地将同样的信息内嵌到图象的不同区域；(2)此技术从本质上来说对图象平多很敏感；(3) 空域技术对图象尺寸变换不具有鲁棒性。

变换域技术在内数据前先对图象进行某种可逆的数学变换，然后用某种规则按水印的指示对变换域的系数进行修改，再进行逆变换得到加水印的图象。两种最常用的变换是 DCT 和 DFT。通常将扩频信号加到 DCT 和 DFT 变换数据的中频段子集[7]，以获得鲁棒性和非显著性的折衷。用整幅图象进行变换的优点是水印将散布在整幅图象中，因而对剪切较鲁棒。又若将水印内嵌到 DFT 的幅度中，则此技术对平移变换具有鲁棒性。频域技术的主要缺点是计算代价较大，而且较难利用人类视觉系统的特性。

更好地选择是将上述两种技术结合起来，也就是设法使变换域技术也具有良好的空间局部化特性。这有两类不同的方法，一类是基于 JPEG 类的分块 DCT 方法，另一类是以小波为基础的方法。以 JPEG 为基础的水印技术能够较好地减少水印的显著性，并增强对 JPEG 压缩袭击的鲁棒性[11]。小波变换将图象在独立的频带和不同空间方向上进行分解，能更好地与人类视觉系统特性相结合[5]，是一种很有潜力的方法。混合技术能非常有效地使水印与图象的局部内容相适应，可在保持良好的图象质量的同时获得较大的鲁棒性，但此类技术对图象平移和尺度变换袭击较敏感。

2.4　数字水印系统的性能评价

数字水印算法性能评价的两个重要的准则是鲁棒性和显著性。鲁棒性直接依赖于内强度，而内嵌强度与图象退化(即水印的显著性)相关。鲁棒性反映水印经受各种图象变换的能力；显著性是数据损失量或水印引入图象的可见失真量。为了定量描述已知水印系统对特定袭击的鲁棒性，可将袭击程度连续地增加，直到水印不再能可靠地提取。这个准则可用于估计特定水印经受某种变换(如 JPEG 压缩)的能力。显著性有大量的度量来定量描述图象的质量，最常用的参数是峰值信噪比 PSNR。然而，图象信息的最终接受者是人，这个度量没有与人类视觉系统的感知特性相结合，不能真实地反映图象的视觉质量。近年来，越来越多的研究人员把注意力集中于研究适合考虑人类视觉系统特性的度量，其中一个重要的参数是考虑到对比敏感性，HVS 掩膜现象和人类空间视觉的多通道模型的掩峰值信噪比 MP-SNR[16]。

3　结束语

近年来，由于可能由内嵌入到文件中的标记来识别数字产品的起源、作者、创作者、所有权者、销售者(分配发行者)或授权消费者等，数字水印技术作为一种在开放的网络环境中多媒体版权保护的有效

方法而提出。为了避免和威摄侵犯版权的行为，需要法律、经济和技术的共同努力。科学家所面临的挑战是设计出更不可感知、易解码、永久的水印方法，并可满足更特殊的应用要求。目前趋向于研究利用人类视觉系统特性来开发人眼有限的动态范围，以产生更为鲁棒、更不显著的水印的方法。水印是一种具有巨大潜力的技术，但并非绝对安全，我们相信它是一种能补偿密码技术的不足，又能应用于模似和数字领域的一种实用技术。

参 考 文 献

1 Macq B ,Quisqauter J J. Cryptology for digital TV broadcast. In: Proceeding of the IEEE 1995,83(6):944～957.

2 Delaigle J F, Boucqueau J M, Quisqauter J J, Macq B. Digital images protecting techniques in a broadcast framework: An ouerview. In: Proceeding of ECMAST '96,1996,2:711～727.

3 Tanaka K, Nakamura Y, Matsui K. Embedding secure information into a dithered multilevel image. In: Proceedings of the 1990 IEEE Military Communications Conference, Sept 1990,216～220.

4 Cox I J, Miller M L. A review of watewrmarking and the importance of perceptual modeling. In:Rogowitz and Pappas, ISSBN 0-8194-2427-7,ISSN 0277-786X.

5 Kundurand D, Hatzinkos D. Digital watermarding using multiresolution wavelet decomposition. In: Int Conference on Acoustic, Speech and Signal Processing (ICASP), IEEE, Oct 1997,5:2969～2972.

6 Nicchiotti G, Ottaviano E. Non-invertible statistical wavewlet watermarking. In: 9th European Signal Processing Conference (EUSIPO'98), Island of Rhodes, Greece, 8～11 Sept 1998, ISBN 960-7620-05-4,pp. 2289～2292.

7 Tzovaras D, Karagiannis N, Strintzis M G. Robust image watermarking in the subband or discrete cosine transform domain. In: 9th European Signal Processing Canference (EUSIPO'98) IsIand of Rhodes, Greeece, 8～11 Sept 1998, ISBN 960-7620-05-4,pp. 2285～2288.

8 Van Schyndel R G, Tirkel A Z, Osborne C F. A digital watermark. In:Int Conference on Image processing, Austin, Texas, USA, 1994 IEEE,2:86～90.

9 Wolfgang R B, Delp E J. A watermarking technique for digital imaging. Further studies. In:Int Conference on Imaging, System and Technolony, Las Vegas, Nevada, USA, 1997, IEEE, pp. 279～287.

10 Swanson M D, Zu B, Tewfik A H. Robust data hiding for images. In:7th Digatal Signal Processing Wordshop (DSP'96), Loen Norway, Sept 1996, IEEE, pp. 37～40.

11 Zhao J, Koch E. Embedding robust labels into images for copyright protection. In: Int Congress on Intellectual Property Rights for Specialised Information, Knowledge and New Tech, Vienna, Austria, Aug 1995.

12 Wolfgang P, Delp E. A watermark for digital images. In: Proc IEEE Internat Conf Image Processing'96, Sept 16～19 1996, pp. 219～222.

13 Cox J, Kilian J, Leighton T, Shammoon T. Secure spread spectrum watermarking for multimedia. Tech Report, NEC Research Institute, No. 95-10,1995.

14 Pitas I. A method for signature casting on digital images. In: Proceedings of ICIP'96, 1996, Ⅲ,215～218.

15 Langelaar H, Van Der Lubbe J, Biemond J. Copy protection for multimedia based on labeling techniques. http://WWW. it. et. tudelft. nl/pda/smash/public/benelux-cr. html

16 Christian J Van den Branden Lambrecht, Joyce E Farrell. Percetual quality metric for digitally coded color images. In: Proceeding of EUSIPCO, Trieste, Italy, Sept 1996,pp. 1175～1178.