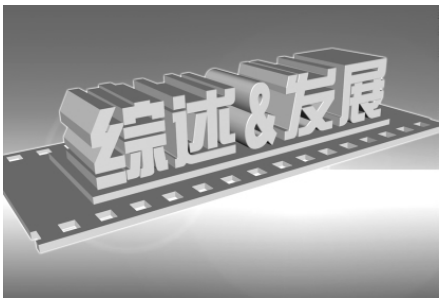

数字水印技术研究综述

赵学军，薛懋楠，杨勤璞，于凯敏，张乐

（中国矿业大学，北京 100083）

摘要：近年来，随着数字与网络技术的发展，作为一种新兴的信息安全技术，数字水印已成为国内外的研究热点同时拥有广阔的应用前景。本文简要介绍了数字水印的概念、特点以及应用，同时列举了几种典型算法，最后对数字水印的发展趋势进行了展望。

关键词：数字水印；空域算法；变换域算法；发展前景

中图分类号：TP311 **文献标识码**：A DOI:10.3969/j.issn.1001-0270.2012.06.01

A Sketch on Digital Watermarking

ZHAO Xue-jun, XUE Mao-nan, YANG Qin-pu, YU Kai-min, ZHANG Le

(China University of Mining and Technology Beijing, Beijing 100083, China)

Abstract: In recent years,with the development of digital technology and network technology,as a new information security technology,digital watermarking has become a research hot topic at home and abroad and has a broad application prospect.This paper briefly introduces the concept、characteristic and application of digital watermarking,at the same time enumerates several typical algorithm,at last, a prospect of digital watermarking is given.

Key Words: Digital Watermarking; Spatial Algorithm; Transform Domain Algorithm; Development Prospect

1 引言

随着计算机通信技术的发展，多媒体技术的进步使存储和传输数字化信息成为可能，然而多媒体内容的安全问题随之而来。对多媒体内容的保护分为两块：一是版权保护，二是内容完整性验证。传统的数字产品保护方法是加密，但其存在很大缺陷，其对内容的保护只局限在加密通信的信道中或其他加密状态下，一旦解密，就毫无保护可言；密码学中的认证方法对多媒体内容的保护也无能为力：一方面由于多媒体内容的真实性认证往往需要容忍一定程度的失真，而密码学中的认证方法不容许一个比特的改变；另一方面，用于多媒体认证的认证信息往往需要直接嵌入多媒体内容中，不另外保存认证信息，但密码学中的认证方法则需要另外保存信息认证码（MAC）。数字水印技术就是在这种背景下应运而生的。数字水印（Digital Watermark）技术是将与多媒体内容相关或不相关的一些标示信息直接嵌入多媒体内容当中，既不影响原内容的使用价值，也不容易被人的知觉系统觉察。通过这些隐藏在多媒体内容中的信息，可以达到确认内容的创建者、购买者，或者用来鉴别多媒体内容的真实完整性的目的。因此，数字水印是信息隐藏技术的一个重要研究方向。

2 数字水印的定义及特点

目前虽然有许多文献讨论有关数字水印技术的问题，但数字水印始终没有一个明确的统一定义。综

收稿日期：2012-10-10

合一些学者提出的定义以及分析已有的数字水印方案，我们给出如下定义：数字水印是永久镶嵌在其他数据（宿主数据）中具有可鉴别性的数字信号或模式，同时不影响宿主数据的可用性。

基于不同的应用，对其要求不尽相同，一般数字水印具备如下特点：

(1)隐形性：数字水印的嵌入不能使原始数据发生可感知的改变，也不能使被保护的数据在质量上发生可感觉到的失真。

(2)鲁棒性：数字水印必须难以去除，在仅仅知道部分数字水印信息的的情况下，试图除去或破坏数字水印应导致严重降质而不可用。数字水印应能抵御一般的信号处理，主要包括重采样、重量化、滤波、平滑、有失真压缩、A/D、D/A转换等等；同时对抗一般的几何变换，主要包括平移、旋转、缩放及分割等。

(3)安全性：数字水印中的信息应是安全的，难以被伪造或篡改，同时具备较低误检概率。

(4)可证明性：在实际的应用过程中，可能多次加入水印，数字水印技术必须能够允许多重水印嵌入被保护的数据同时各个水印均能被独立证明。

(5)易恢复性：这主要针对一些实时性要求较强的用途(如视频水印的验证)提出。只要拥有正确的水印算法和密钥就能很容易的从隐藏载体中提取出水印信息，而不必耗费大量时间做水印鉴定。

(6)嵌入容量：一般来讲，水印系统的嵌入容量要求相对较小，而信息隐藏则要求载体具有较大的嵌入容量。对于水印算法而言，嵌入的信息量越大，越有可能降低水印的鲁棒性。在实际应用系统中，需考虑嵌入容量与鲁棒性二者之间的折中关系。

通常我们认为具有上述特点的水印是严格意义上的水印，但由于对数字水印的定义尚未统一许多文献中讨论的数字水印并不完全具备以上特点，我们讨论的范围一般是更广义上的数字水印。

3　典型的数字水印系统模型

图1　水印信号嵌入模型

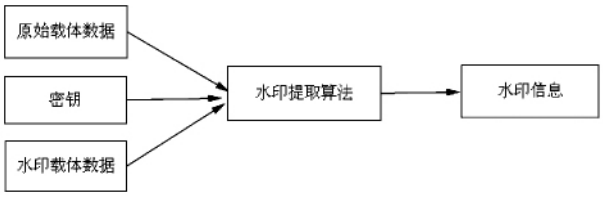

图2　水印信号恢复模型

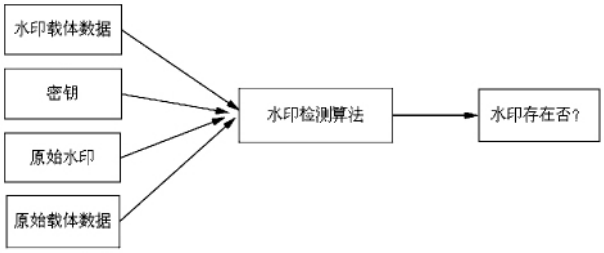

图3　水印信号检测模型

4　数字水印的应用

随着数字水印技术的发展，数字水印的应用领域也得到了扩展，主要有以下几个方面：

(1)版权保护：数字作品的所有者可用密钥产生水印，并将其嵌入原始数据，当该作品被盗版或产生产权纠纷时，所有者即可从被盗版作品中获取水印信号作为依据，以此保护所有者的权益。

(2)数字指纹：为避免未经授权的拷贝制作和发行，版权所有人可以向分发给不同用户的作品中嵌入不同的水印以标识用户信息。该水印可根据用户的序号和相关的信息生成，一旦发现未经授权的拷贝，即可根据此拷贝所恢复出的指纹来确定其来源。

(3)标题与注释：将作品的标题、注释等内容以水印形式嵌入该作品中。例如，一幅画的作者和创作时间等。

(4)访问控制：利用数字水印技术可以将访问控制信息嵌入到媒体中，在使用媒体前通过检测嵌入到其中的访问控制信息达到访问控制目的，这种水印应具有很强的鲁棒性。一个典型例子就是DVD防拷贝系统，即将水印信息加入DVD数据中，这样DVD播放机即可通过检测该水印信息而判断其合法性和可拷贝性。

(5)认证和完整性校验：通常采用脆弱水印。对插入了水印的数字内容进行检验时，须用唯一的与数据内容相关的密钥提取水印，再通过检验提取出的水印的完整性来验证数字内容的完整性。其优点在于认证内容密不可分，处理过程得到了简化。

5 数字水印的典型算法

近几年数字水印技术研究发展很快，新算法层出不穷，最基本的就是空域算法和频域算法（变换域算法），很多新的算法都是基于变换域的。下面介绍一些典型的算法：

（1）空域算法：空域算法是相对于变换域算法而言的。其中比较典型的水印算法有LSB和MSB。LSB是将信息嵌入图像点中最不重要的像素位，以此保证嵌入水印的不可见性；MSB是将信息嵌入到图像点中最重要位，即最高位。但他们都有其共同缺点，这也是时空域算法普遍存在的缺点：算法鲁棒性差。另外一个常用方法是利用像素的统计特征将信息嵌入到像素的亮度值中，该算法与前面算法的区别是，它利用的是像素的统计特征。典型的有Patch-work算法。它是随机选择N对像素点（a，b），每对像素点的差值是以0为中心的高斯分布。然后将点a的亮度值加1，点b的亮度值减1，以此改变分布的中心，并且使整个图像的平均亮度保持不变。最后采用统计的方法检测水印。为了抵抗有损压缩等处理，它将像素点对扩展成小块像素区域（patch），增加一个patch中所有像素点的亮度值，同时减少对应的另外一个patch中所有像素点的亮度值。此算法对抵御有损压缩编码（JPEG）、剪裁攻击和灰阶校正很有效，但由于其嵌入的水印信息少，对多拷贝联合攻击抵抗能力脆弱。还有Schyndel算法。该算法提出了相关检测方法。该算法首先把一个密钥输入一个m-序列发生器来产生水印信号，m-序列的自相关函数和频谱分布的特点类似于随机高斯噪声，此后这个序列被重新排列成二维水印信号，并按像素点依次插入到原始图像像素值的最低位。但该算法嵌入码低，且对串谋攻击抵抗力弱。

（2）变换域算法：基于时空域算法存在的固有缺点，当前对数字水印算法的研究主要集中在变换域，它的基本思想是通过离散傅里叶变换（DFT）、离散余弦变换（DCT）或离散小波变换（DWT）等把数字图像的数据转化为相应频域的系数，以此来实现水印嵌入。在此算法中，首先要对载体进行某种特定的正交变换，嵌入空间是载体的某个或某些频带，这些频带所对应的变换系数要遵循一定的规则进行修改。载体的低频系数反映载体的主要轮廓，集中载体的绝大部分能量，是载体的主要信息；载体的高频系数则反映载体的细节，不易被人眼察觉。其特点是数据改变幅度小，水印的稳健性强且物理意义清晰，与压缩标准兼容可直接在压缩域中进行处理，且透明性好。缺点就是其抵抗几何变换等攻击的能力比较弱。

（3）压缩域算法：基于JPEG、MPEG标准的压缩域数字水印系统，由于其水印检测与提取可直接在压缩域数据中进行，这样就简化了完全解码与重新编码的过程，因此在数字电视广播及VOD中有很高的实用价值。输入的MPEG-2数据流可分为数据头信息、DCT编码信号块和运动向量3部分，一般的方法都是主要改变DCT编码信号块。相应的，水印的检测与提取也可以直接进行于压缩域数据中。

（4）NEC算法：它的工作原理是，首先由作者的标识码和图像的hash值等组成密钥，该密钥就做为种子产生伪随机序列，此序列满足高斯N（0，1）分布。再对图像做DCT变换，同时用这个伪随机序列调制图像除直流（DC）分量外的1000个最大的DCT系数。此算法可以防止IBM攻击，同时提出了一个重要原则，即水印信号应嵌入原数据中对人感觉最重要的部分，这大大增强了水印的鲁棒性和抗攻击能力。随后Pod ilchuk利用人类视觉模型改进了此算法，进一步提高了算法的鲁棒性与透明性等特性。该算法在数字水印算法中占有重要地位。

（5）基于分形图像的编码方法：数学家M. F. Barnsley在论文中提出分形图像编码的概念，并且将迭代函数系统理论应用于图像编码，效果明显。此方法新颖有效，伴随着分形压缩技术的逐步完善，它的应用前景也会愈加广阔。

（6）生理模型算法：人的生理模型包括人类视觉系统（HVS）和人类听觉系统（HAS）。其思想均是利用从模型导出的JND（just noticeable difference）描述来确定在图像或声音的各部分所能容忍的数字水印信号的最大强度，以此避免破坏视觉或听觉的质量。实质就是，利用此模型确定与数据相关的调制掩模，再利用其嵌入水印。此方法同时具备好的透明性与鲁棒性。

6 数字水印的研究现状及发展方向

数字水印技术是当前数字信号处理、图像处理、密码学应用、通信理论、算法设计等学科的交叉领

域,是目前国际学术界的研究热点之一。国外的许多研究小组及公司都有有关数字水印及信息隐藏方面的商业软件,而国内似乎尚无此类软件,部分单位或许有实验软件或演示软件。就理论与实际成果而言,国内在数字水印方面的研究工作尚处于起步阶段。

我们认为今后数字水印技术的研究将倾向于完善数字水印理论,提高其算法的安全性、稳健性,强化它在实际网络中的应用以及建立相关标准等方向。

数字水印在理论方面的工作包括建立更好的模型、分析不同媒体中水印信息所能嵌入的容量(带宽)、比较各类算法的抗攻击性能等。

许多实际的应用对数字水印的鲁棒性要求很高,这就需要有鲁棒性更好的数字水印算法,因此,研究此类算法仍是数字水印的重点发展方向,但应注意与此同时应结合HVS或HAS的特点,保持良好的不可见性以及嵌入更大的水印信息容量,同时,要重视自适应思想以及一些新的信号处理算法在数字水印算法中的应用,比如分形编码、混沌编码、小波分析等等。

数字水印应用安全性很重要,基于其算法的安全性不能靠保密算法得到,数字水印算法必须能抵抗各类攻击,因此,研制安全性更高的水印算法也是重点之一。

对于实际网络环境下的数字水印应用,应重点研究其网络快速自动验证技术,这就需要紧密结合计算机网络技术和认证技术。

要提高不同的数字水印算法的兼容性、扩大数字水印的应用范围,就必须建立水印处理算法的标准,比如嵌入数字水印的标准、提取或检测数字水印的标准、数字水印的认证标准。目前国际上的水印处理尚未形成统一标准,形成公认的标准已成为水印研究者的共同目标。然而,标准算法必须具有其优越性、有效性和通用性,同时需要得到各方认同。所以标准的形成仍是一个艰苦的过程。标准一旦建立,将会大大促进数字水印技术的应用和发展。

将水印处理技术应用于其他领域也是今后的一个研究热点。比如军事和国防方面,即把其用于传递军事机密,或用其验证军事命令、信息的真实可靠性,并探索该领域的新技术新理论,这对于国防现代化建设和未来的信息化、网络化战争具有重大的意义。

同时,我们也应认识到,数字水印技术并非是万能的,须配合密码学技术及认证技术、数字签名或数字信封等技术一并使用。因此,不能把其与这些技术相孤立,只有配合这些技术才能构成完整的数字产品版权保护体系。

参考文献:

[1]孙圣和,陆哲明,牛夏牧.数字水印技术及应用.北京:科学出版社,2004.

[2]陈明奇,钮心忻,杨义先.数字水印的研究进展和应用.北京:通信学报,2001.

[3]Patchwork K. How to Secretly Embed a Signature in a Picture. Journal of the Interactive Multimedia Association Intellectual Property Project, 1996, 1.

[4]Wolfgang R B, Podilchuk C I, Delp E J.Perceptual Watermarks for Digital Image and Video [J].IEEE,1999 (7): 1108–1126.

[5]Bender W. Gruhl D.Morimoto N.Techniques for Data Hiding [J].IBM Syst.J,1996.35(3,4):313–336.

[6]汪国有,杨永祥.数字水印技术研究进展[J].网络安全技术与应用,2004.11:45–48.

[7]A. Z. Tirkel, C. F. Osborne, T.E.Hall.Image and watermark registration. Signal Processing, 1998,66(3):373–383.

[8]尹浩,林闯,邱锋,丁嵘.数字水印技术综述.计算机研究与发展,2005,42(7):1093–1099.

[9]Hartung F, Girod B. Watermarking of Uncompressed and Compressed Video[J].Signal Processing,1998.66(3):283–301.

[10]Lu Z, Pan J, Sun S. VQ–Based Digital Image Watermarking Method[J]. Elec.Letters ,2000.36(14):1201–1202.

[11]孙锐,孙洪,姚天任.多媒体水印技术的研究进展与应用[J].系统工程与电子技术,2003.25(06):271–276.

[12]Swanson M, Zhu B, Tewfik A H. Multiresolut in Scene–Based Video Watermarking UsingPerceptual Models [J]. IEEE, 1998:525–539.