数字水印技术研究进展

易开祥[1] 石教英[1] 孙 鑫[2]
[1](浙江大学 CAD&CG 国家重点实验室,杭州 310027)
[2](浙江大学工业控制技术研究所,杭州 310027)

摘 要 随着因特网的日益普及,多媒体信息交流达到了前所未有的深度和广度,但作品侵权也随之更加容易,篡改也更加方便,因此,如何保护作品版权已受到人们的高度重视,而如今信息隐藏技术,特别是数字水印技术作为版权保护的重要手段,已得到广泛的研究和应用.为了使人们对该技术有一个较全面的了解,因而对数字水印技术的研究与进展情况进行了较系统的论述,即首先对信息隐藏技术进行了介绍,并对该技术进行了分类,然后重点分析了数字水印技术的模型、典型算法及其攻击方法,最后对数字水印技术的研究发展及其应用前景指出了一些可能的方向.

关键词 信息隐藏 数字水印 版权保护
中图法分类号:TP391.41 **文献标识码**:A **文章编号**:1006-8961(2001)02-0111-07

Digital Watermarking Techniques: An Introductory Review

YI Kai-xiang[1], SHI Jiao-ying[1], SUN Xin[2]
[1](*State Key Laboratory of CAD&CG, Zhejiang University, Hangzhou* 310027)
[2](*Institute of Industry Process Control, Zhejiang University, Hangzhou* 310027)

Abstract The digital media, including text, image, graphics, audio and video etc., has become a main way for information communication along with the popularization of Internet and the development of multimedia techniques. People can get almost information through the Internet. But this gives rise to serious problems including wide spread copyright violation, illegal copying, easy forging etc. How to provide copyright protection and implement covert communication has drawn extensive attention in recent years. As a main method for covert communication and copyright protection(watermarking), information hiding has been widely studied and applied. In this paper, we make an introductory review on the information hiding techniques including the last achievement in this field. First, we give the general concepts and fundamental principles of information hiding such as the definition, characteristics, classification and general framework. Then, we analyze the processing model, the typical methods, the main application and the attack analysis of watermarking. Finally, we make a discussion on some open problems and point out possible directions for further research.

Keywords Information hiding, Digital watermarking, Copyright protection

0 前 言

多媒体数据的数字化为多媒体信息的存取提供了极大的便利,同时也极大地提高了信息表达的效率和准确性.随着因特网的日益普及,多媒体信息的交流已达到了前所未有的深度和广度,其发布形式也愈加丰富了.人们如今也可以通过因特网发布自己的作品、重要信息和进行网络贸易等,但是随之而出现的问题也十分严重 如作品侵权更加容易,篡改也更加方便.因此如何既充分利用因特网的便利,又能有效地保护知识产权,已受到人们的高度重视.

基金项目:国家自然科学基金资助项目(69773020,69823003)
收稿日期:2000-01-04 改回日期:2000-07-04

Van Schyndel 在 ICIP '94 会议上发表了题为“A digital watermark”的文章,这是第一篇在主要会议上发表的关于数字水印的文章,其中阐明了一些关于水印的重要概念,它被认为是一篇具有历史价值的文献.1996-05-30—1996-06-01,在英国剑桥牛顿研究所召开了第一届国际信息隐藏学术研讨会,这标志着一门新兴的交叉学科——信息隐藏学的正式诞生.如今信息隐藏学作为隐蔽通信和知识产权保护等的主要手段,正得到广泛的研究与应用[1~7].

1 信息隐藏

1.1 信息隐藏模型

信息隐藏(Information Hiding)不同于传统的密码学技术.密码技术主要是研究如何将机密信息进行特殊的编码,以形成不可识别的密码形式(密文)进行传递;而信息隐藏则主要研究如何将某一机密信息秘密隐藏于另一公开的信息中,然后通过公开信息的传输来传递机密信息.对加密通信而言,可能的监测者或非法拦截者可通过截取密文,并对其进行破译,或将密文进行破坏后再发送,从而影响机密信息的安全;但对信息隐藏而言,可能的监测者或非法拦截者则难以从公开信息中判断机密信息是否存在,难以截获机密信息,从而能保证机密信息的安全.

信息隐藏的例子层出不穷,从中国古代的藏头诗,到中世纪欧洲的栅格系统;从古希腊的蜡板藏书到德国间谍的密写术等这些都是典型的例子.多媒体技术的广泛应用,为信息隐藏技术的发展提供了更加广阔的领域.图 1 即是一个信息隐藏的通用模型[5].

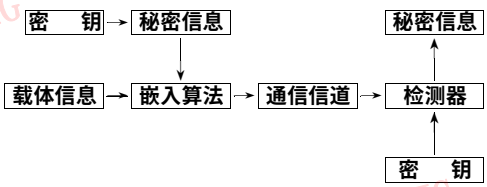

图 1 信息隐藏模型

人们称待隐藏的信息为秘密信息(secret message),它可以是版权信息或秘密数据,也可以是一个序列号;而公开信息则称为载体信息(cover message),如视频、音频片段.这种信息隐藏过程一般由密钥(Key)来控制,即通过嵌入算法(Embedding algorithm)将秘密信息隐藏于公开信息中,而隐蔽载体(隐藏有秘密信息的公开信息)则通过信道(Communication channel)传递,然后检测器(Detector)利用密钥从隐蔽载体中恢复/检测出秘密信息.

信息隐藏技术主要由下述两部分组成:(1)信息嵌入算法,它利用密钥来实现秘密信息的隐藏.(2)隐蔽信息检测/提取算法(检测器),它利用密钥从隐蔽载体中检测/恢复出秘密信息.在密钥未知的前提下,第三者很难从隐秘载体中得到或删除,甚至发现秘密信息.

1.2 信息隐藏特点

信息隐藏不同于传统的加密,因为其目的不在于限制正常的资料存取,而在于保证隐藏数据不被侵犯和发现.另外,由于信息隐藏必须考虑隐藏的信息在经历各种环境、操作之后,仍需具有免遭破坏的能力,因此,信息隐藏技术必须考虑正常的信息操作所造成的威胁,即要使机密资料对正常的数据操作技术具有免疫能力.这种免疫力的关键是要使隐藏信息部分不易被正常的数据操作(如通常的信号变换操作或数据压缩)所破坏.

根据信息隐藏的目的和技术要求,该技术存在以下特性[1~8]:

(1)鲁棒性(robustness) 指不因图象文件的某种改动而导致隐藏信息丢失的能力.这里所谓“改动”包括传输过程中的信道噪音、滤波操作、重采样、有损编码压缩、D/A 或 A/D 转换等.

(2)不可检测性(undetectability) 指隐蔽载体与原始载体具有一致的特性.如具有一致的统计噪声分布等,以便使非法拦截者无法判断是否有隐蔽信息.

(3)透明性(invisibility) 利用人类视觉系统或人类听觉系统属性,经过一系列隐藏处理,使目标数据没有明显的降质现象,而隐藏的数据却无法人为地看见或听见.

(4)安全性(security) 指隐藏算法有较强的抗攻击能力,即它必须能够承受一定程度的人为攻击,而使隐藏信息不会被破坏.

(5)自恢复性 由于经过一些操作或变换后,可

能会使原图产生较大的破坏，如果只从留下的片段数据，仍能恢复隐藏信号，而且恢复过程不需要宿主信号，这就是所谓的自恢复性.

信息隐藏学是一门新兴的交叉学科，在计算机、通讯、保密学等领域有着广阔的应用前景.数字水印技术作为其在多媒体领域的重要应用，已受到人们越来越多的重视.

2　数字水印

2.1　背景

随着数字技术和因特网的发展，各种形式的多媒体数字作品(图象、视频、音频等)纷纷以网络形式发表，其版权保护成为一个迫切需要解决的问题.由于数字水印(digital watermarking)是实现版权保护的有效办法，因此如今已成为多媒体信息安全研究领域的一个热点，也是信息隐藏技术研究领域的重要分支.该技术即是通过在原始数据中嵌入秘密信息——水印(watermark)来证实该数据的所有权.这种被嵌入的水印可以是一段文字、标识、序列号等，而且这种水印通常是不可见或不可察的，它与原始数据(如图象、音频、视频数据)紧密结合，并隐藏其中，成为源数据不可分离的一部分，并可以经历一些不破坏源数据使用价值或商用价值的操作而保存下来.

数字水印技术除了应具备信息隐藏技术的一般特点外，还有着其固有的特点和研究方法.例如，从信息安全的保密角度而言，隐藏的信息虽然被破坏掉，而系统可以视为是安全的，因为秘密信息并未泄露;但是，在数字水印系统中，隐藏信息的丢失，即意味着版权信息的丢失，从而也就失去了版权保护的功能，也就是说，这一系统就是失败的.由此可见，数字水印技术必须具有较强的鲁棒性、安全性和透明性.

2.2　典型数字水印系统模型[8]

图 2 为水印信号嵌入模型，其功能是完成将水印信号加入原始数据中;图 3 为水印信号恢复模型，其负责从水印数据中提取出水印信号;图 4 为水印信号检测模型，用以判断某一数据中是否含有指定的水印信号.

图 3、图 4 中的虚框部分表示在提取或判断水印信号时，原始载体数据不是必要的.

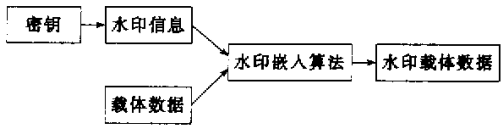

图 2　水印信号嵌入

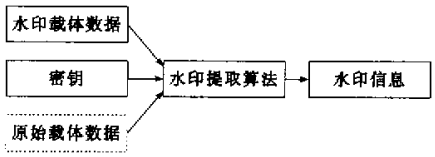

图 3　水印信号恢复

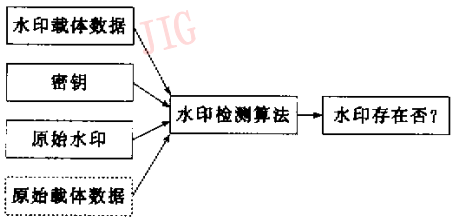

图 4　水印信号检测

2.3　数字水印主要应用领域[1~6,8,9]

(1)版权保护　即数字作品的所有者可用密钥产生一个水印，并将其嵌入原始数据，然后公开发布他的水印版本作品.当该作品被盗版或出现版权纠纷时，所有者即可利用图 3 或图 4 的方法从盗版作品或水印版作品中获取水印信号作为依据，从而保护所有者的权益.对这种应用领域来说，水印技术必须有较好的鲁棒性、安全性、透明性和水印嵌入的不可逆性.

(2)加指纹　为避免未经授权的拷贝制作和发行，出品人可以将不同用户的 ID 或序列号作为不同的水印(指纹)嵌入作品的合法拷贝中.一旦发现未经授权的拷贝，就可以根据此拷贝所恢复出的指纹来确定它的来源.对这种应用领域来说，水印技术除具有版权保护应用中的特性外，还必须具有防止串谋攻击(多拷贝攻击)等功能.

(3)标题与注释　即将作品的标题、注释等内容(如，一幅照片的拍摄时间和地点等)以水印形式嵌入该作品中，这种隐式注释不需要额外的带宽，且不易丢失.

(4)篡改提示　当数字作品被用于法庭、医学、新闻及商业时，常需确定它们的内容是否被修改、伪

造或特殊处理过.为实现该目的,通常可将原始图象分成多个独立块,再将每个块加入不同的水印.同时可通过检测每个数据块中的水印信号,来确定作品的完整性.与其他水印不同的是,这类水印必须是脆弱的,并且检测水印信号时,不需要原始数据.

(5)使用控制 这种应用的一个典型的例子是 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 DVD 数据中的水印信息而判断其合法性和可拷贝性.从而保护制造商的商业利益.

2.4 典型算法

近几年来,数字水印技术研究取得了很大的进步[2,7,10~25],本文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象数据(某些算法也适合视频和音频数据).

(1)空域算法[2,10~12] 该类算法包括文本水印算法、Schyndel 算法[10]和 Patchwork 算法等.其中文献[10]被认为是一篇具有历史价值的文献,它是第一篇在主要会议上发表的关于数字水印的文章,文中阐明了一些关于水印的重要概念和鲁棒水印检测的通用方法(相关性检测方法),该文提出的 Schyndel 算法首先把一个密钥输入到一个 m-序列(maximum-length random sequence)发生器来产生水印信号,然后此 m-序列被重新排列成 2 维水印信号,并按象素点逐一插入到原始图象象素值的最低位.由于水印信号被安排在了最低位上,因此它是不可见的,基于同样的原因,它可以轻易地被移去,因此也是不强壮的;Patchwork[2,12]提出了一种基于改变图象数据统计特性的水印算法,该算法首先随机选取 N 对象素点,然后通过增加象素对中一个点的亮度值,而相应降低另一个点亮度值的方法来隐藏信息.为增加其水印的鲁棒性,文中还把象素对扩展为小块的象素区域(如 8×8),再通过增加一个区域中的所有象素点的亮度值,而相应减少对应区域中所有象素点亮度值的方法来隐藏信息.但该算法嵌入码低,且对串谋攻击抵抗力弱.

(2)变换域算法[7,15~25] 文献[16]提出了一种 DCT 域数字水印算法,其方法是首先把图象分成 8×8的不重叠象素块,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.在水印信号提取时,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.其思想类似于扩展频谱通讯中的跳频(frequency hopping)技术,其特点是数据改变幅度较小,且透明性好,但是其抵抗几何变换等攻击的能力较弱.另外,基于 DFT 和 DWT 算法与上述算法具有相似的原理.

这种以变换域算法为代表的通用算法普遍采用变换技术,以便在频率域实现水印信号叠加,并借鉴扩展频谱通讯等技术对水印信号进行有效的编码,从而提高了透明性和鲁棒性,同时还适当利用滤波技术对水印信号引入的高频噪声进行了消除,从而增加了对低频滤波攻击的抵抗力.

(3)压缩域算法[13,14] 基于 JPEG、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 VOD(Video on Demand)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.

文献[13]提出了一种针对 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 Hartung 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 n_1 与原来的无水印系数的码字 n_0 进行比较,只在 n_1 不大于 n_0 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[7,17,19,20] 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象的哈希值组成,其次对图象做 DCT 变换,最后用伪随机高斯序列来调制(叠加)该图象除直流(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、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.随后 Podilchuk 等[5,21]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.

(5)生理模型算法[8,21~25]　人的生理模型包括人类视觉系统 HVS(Human Visual System)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,文献[23]、[24]实现了一个基于分块 DCT 框架的数字水印系统;文献[22]实现了一个基于小波分解框架的数字水印系统;文献[25]实现了一个空域数字水印系统.它们的基本思想均是利用从视觉模型导出的 JND(Just Noticeable Difference)描述来确定在图象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象相关的调制掩模,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.

3　水印攻击分析

所谓水印攻击分析,就是对现有的数字水印系统进行攻击,以检验其鲁棒性,通过分析其弱点所在及其易受攻击的原因,以便在以后数字水印系统的设计中加以改进.攻击的目的在于使相应的数字水印系统的检测工具无法正确地恢复水印信号,或不能检测到水印信号的存在.这和传统密码学中的加密算法设计和密码分析是相对应的.

3.1　IBM 攻击

这是针对可逆、非盲(non-oblivious)水印算法而进行的攻击.其原理为,设原始图象为 I,加入水印 W_A 的图象为 $I_A = I + W_A$.攻击时,攻击者首先生成自己的水印 W_F;然后创建一个伪造的原图 $I_F = I_A - W_F$,也即 $I_A = I_F + W_F$;此后,攻击者可声称他拥有 I_A 的版权,因为攻击者可利用其伪造原图 I_F 从原图 I 中检测出其水印 W_F,但原作者也能利用原图从伪造原图 I_F 中检测出其水印 W_A.这就产生无法分辨与解释的情况.而防止这一攻击的有效办法就是研究不可逆水印嵌入算法,如哈希过程.

3.2　StirMark 攻击

Stirmark 是英国剑桥大学开发的水印攻击软件,由于它是采用软件方法来实现对水印载体图象进行的各种攻击,从而在水印载体图象中引入了一定的误差,但人们可以以水印检测器能否从遭受攻击的水印载体中提取或检测出水印信息来评定水印算法抗攻击的能力.如 StirMark 可对水印载体进行重采样攻击,它首先模拟图象用高质量打印机输出,然后再利用高质量扫描仪扫描,重新得到其图象在这一过程中引入的误差.

另外,StirMark 还可对水印载体图象进行几何失真攻击,即它可以以几乎注意不到的轻微程度对图象进行拉伸、剪切、旋转等几何操作.StirMark 还通过应用一个传递函数,来模拟非线性的 A/D 转换器的缺陷所带来的误差,这通常见于扫描仪或显示设备.

3.3　马赛克攻击

其攻击方法是首先把图象分割成为许多个小图象,然后将每个小图象放在 HTML 页面上拼凑成一个完整的图象.一般的 Web 浏览器在组织这些图象时,都可以在图象中间不留任何缝隙,并且使这些图象看起来整体效果和原图一模一样,从而使得探测器无法从中检测到侵权行为.这种攻击方法主要用于对付在 Internet 网上开发的自动侵权探测器,该探测器包括一个数字水印系统和一个所谓的 Web 爬行者.但这一攻击方法的弱点在于,一旦当数字水印系统要求的图象最小尺寸较小时,则需要分割成非常多的小图象,这样将使生成页面的工作会非常繁琐.

3.4　串谋攻击

所谓串谋攻击就是利用同一原始多媒体数据集合的不同水印信号版本,来生成一个近似的多媒体数据集合,以此来逼近和恢复原始数据,其目的是使检测系统无法在这一近似的数据集合中,检测出水印信号的存在,其最简单的一种实现就是平均法.

3.5　跳跃攻击

跳跃攻击主要用于对音频信号数字水印系统的攻击,其一般实现方法是,在音频信号上加入一个跳

跃信号(jitter),即首先将信号数据分成 500 个采样点为一个单位的数据块,然后在每一数据块中随机复制或删除一个采样点,来得到 499 或 501 个采样点的数据块,接着再将数据块按原来顺序重新组合起来.实验表明,这种改变即使对古典音乐信号数据也几乎感觉不到,但是却可以非常有效地阻止水印信号的检测定位,以达到难以提取水印信号的目的.类似的方法也可以用来攻击图象数据的数字水印系统,其实现方法也非常简单,即只要随机地删除一定数量的象素列,然后用另外的象素列补齐即可,该方法虽然简单,但是仍然能有效破坏水印信号存在的检验.

4 研究展望

数字水印技术是一个新兴的研究领域,如今还有许多未触及的研究课题,现有技术也需要改进和提高.通过对现有技术的分析,数字水印技术今后可能的研究方向为[1~8,15~25,28]:

(1)算法分析 通过对现有数字水印算法的鲁棒性、安全性、抗攻击性等特性的研究,并结合数字信号处理技术,寻找出它们之间的关系,从而发现更加好的数字水印技术.

(2)基于特征的数字水印技术 因基于统计特征的数字水印技术容易受到非线性等变换方法的攻击,而基于特征的数字水印技术如基于边界信息的数字水印技术等则具有较好鲁棒性,因此可能成为今后的研究重点.

(3)公钥数字水印系统 即使用一个专有的密钥来叠加水印信号,而任何人均可通过一个公开的密钥来检测出水印信号,但是用公开的密钥来推导专有密钥和用公开的密钥来去除水印信号这两个过程都非常困难.目前,该领域还未取得突破性进展.

(4)数字水印代理(Agent) 其核心思想是将数字水印技术与 TSA(Trusted spotting agent)相结合.这种数字水印代理在网络上的服务器之间漫游,扮演着基于数字水印检测、验证和追踪非法拷贝的侦探角色.

(5)目前其它的数字水印技术,如对基于图形、矢量图和动画等媒体的数字水印技术研究得还比较少,仅见有文献[28]阐述的基于三角面片几何图形的水印嵌入算法.这也是今后数字水印技术的一个研究方向.

参 考 文 献

1 Q Ruanaidh J J, Dowling W J, Boland F M. Watermarking digital images for copyright protection. In: IEEE proceeding on Vision, Signal and Image Processing, 1996.8, 143(4): 250256.

2 Bender W, Gruhl D, Morimoto N *et al*. Techniques for data hiding. IBM System Journal, 1996, 35(3&4): 313336.

3 Kobayashi. Digital watermarking: Historical roots. IBM Research Reports, Tokyo Research Laboratories, 1997.

4 Voyatzis G, Nikolaidis N, Pitas I. Digital watermarking: An overview. In: 9th European Signal Processing Conference, Island of Rhodes, Greece, 1998: 912.

5 Jiri Fridrich. Applications of data hiding in digital images. In: the ISPAC '98 Conference in Melbourne, Australia, 1998.11.

6 Mahalingam Ramkumar. Data hiding in multimedia-theory and applications. [Ph.D. Degree], New Jersey: Department of Electrical and Computer Engineering, New Jersey Institute of Technology, 1999.

7 Cox I J, Matt L Miller. A review of watermarking and the importance of perceptual modeling. SPIE Proceeding on Human Vision and Electronic Imaging, 1997, 3016: 9299.

8 向辉. 基于信息重组思想的多媒体数据压缩与多媒体数据安全技术研究[博士学位论文]. 杭州: 浙江大学 CAD&CG 国家重点实验室, 1999.

9 Ramkumar M, Akansu A N. Image watermarks and counterfeit attacks: some problems and solutions. In: Proceeding on Content Security and Data Hiding in Digital Media Conference Newark, NJ, 1999, 102112.

10 Van Schyndel R, Tirkel A, Osborne C. A digital watermark. In: IEEE Proceeding on International Conference on Image Processing, Austin, Tex., IEEE Press, 1994: 8690.

11 Maxemchuk N F. Electronic document distribution. AT&T Technical Journal, 1994.9, 73(5): 7380.

12 Nikolaidis N, Pitas I. Copyright protection of images using robust digital signatures. In: IEEE Proceeding on International Conference on Acoustics, Speech, and Signal Processing, Atlanta, IEEE Press, 1996: 2168-2171.

13 Hartung F, Girod B. Watermarking of MPEG-2 encoded video without decoding and re-encoding. SPIE Proceeding on Multimedia Computing and Networking, San Jose, 1997, 3020: 264273.

14 Lintian Qiao, Klara Nahrsted. Non-invertible watermarking methods for MPEG encoded audio. SPIE Proceedings on Security and Watermarking of Multimedia Contents, San Jose, 1999, 3657: 194202.

15 Hui Xiang *et al*. Digital watermarking systems with chaotic sequences. SPIE Proceeding on Security and Watermarking of Multimedia Contents, San Jose, 1999, 3657: 449457.

16 Zhao J, Koch E. Embedding robust labels into images for copyright protection. In: Proceedings of the KnowRight '95 Conference on Intellectual Property Rights and New Technologies, Vienna, Austria, 1995: 241251.

17 Cox I J, Kilian J, Leighton T *et al*. A secure, robust watermark for multimedia. In: Proceedings of Info Hiding '96, Cambridge University, London, England, 1996: 185206.

18 Barni M, Bartolini F, Cappellini V *et al*. A DWT-based technique for

spatial-frequency masking of digital signatures. SPIE Proceeding on Security and Watermarking of Multimedia Contents, 1999, 3657: 3139.

19 Cox I J, Kilian J, Leighton T *et al*. Secure spread spectrum watermarking for images, audio and video. IEEE Proceeding on International Conference on Image Processing, 1996, 3: 243246.

20 Cox I J, Kilian J, Leighton T *et al*. Secure spread spectrum watermarking for multimedia. IEEE Trans. on Image Processing, 1997, 6(12): 1673-1687.

21 Christine I Podilchuk, Zeng Wenjun. Digital image watermarking using visual models. SPIE Proceeding on Human Vision and Electronic Imaging, 1997, 3016: 100111.

22 韦志辉等. 基于小波域中视觉门限模型的数字水印技术. 东南大学学报, 1998, 28(5): 4448.

23 黄继武, SHI YunQ. 一种自适应图象水印算法. 自动化学报, 1999, 25(4): 477482.

24 黄继武, SHI YunQ, 姚若河. 基于块分类的自适应图象水印算法. 中国图象图形学报, 1999, 4(8): 640643.

25 易开祥, 石教英. 一种自适应二维数字水印算法. 见: 全国第二届信息隐藏学术研讨会论文集, 北京. 2000: 108112.

26 Petitcolas Fabien A P, Anderson Ross J, Kuhn Markus G. Attacks on copyright marking systems. In: Information Hiding '98 Conference, Second International Workshop, Volume Springer Lecture Notes in Computer Science, , Portland, Oregon, USA, 1998, 1525: 218238.

27 Scott Craver, Nasir Memon, Boon-Lock Yeo. Resolving rightful ownerships with invisible watermarking techniques: limitations, attack, and implications. IEEE journal on selected areas in communication, 1998, 16(4): 573586.

28 Emil Praun *et al*. Robust mesh watermarking. http://www.cs.princeton.edu/gfx/proj/meshwm, 1999.

易开祥　1971 年生, 1995 年毕业于阜新矿业学院计算机系, 1998 年在辽宁工程技术大学获电力传动及其自动化硕士学位, 现在浙江大学计算机系攻读博士学位. 主要研究方向为数字图象处理、多媒体技术和数字水印技术等.

石教英　1937 年生, 毕业于前苏联列宁格勒大学. 现为浙江大学计算机系教授, 博士生导师, 浙江大学 CAD&CG 国家重点实验室学术委员会主任. 主要研究领域为分布式计算、科学计算可视化、虚拟现实及多媒体技术等.

孙　鑫　1973 年生, 1995 年毕业于阜新矿业学院电气工程系, 1998 年在辽宁工程技术大学获电力传动及其自动化硕士学位, 现在浙江大学控制系攻读博士学位. 主要研究方向为非线性系统、离散事件动态系统、计算机控制和图象处理等.