第 19 卷 第 6 期　　控 制 与 决 策　　2004 年 6 月
Vol. 19 No. 6　　Control and Decision　　June 2004

文章编号: 1001-0920(2004)06-0601-06

常用数字图像水印攻击方法及基本对策

刘春庆[1,2], 王执铨[1], 戴跃伟[1]
(1. 南京理工大学 自动化系, 江苏 南京 210094; 2. 空军第六飞行学院, 河北 涿州 072757)

摘　要: 数字水印是近年来出现的数字产品版权保护技术,目的是保护数字产品的合法拷贝和传播. 数字水印研究主要分为算法设计和攻击分析两个方面. 较为系统地论述了当前关于数字图像水印的常用攻击方法以及主要的对抗策略,分析了它们的优缺点,讨论了数字水印技术未来可能出现的研究热点.

关键词: 数字水印; 攻击方法; 抵抗策略
中图分类号: TP391　　**文献标识码**: A

Current attacking methods to digital image watermarking and basic countermeasures

LIU Chun-qing[1,2], *WANG Zhi-quan*[1], *DAI Yue-wei*[1]
(1. Department of Automation, Nanjing University of Science and Technology, Nanjing 210094, China; 2. The Sixth Flight Academy of the Air Force, Zhuozhou 072757, China. Correspondent: LIU Chun-qing, E-mail: liu-chunqing@sohu.com)

Abstract: Watermarking is a potential method for protection of ownership rights on digital audio, image and video data presenting itself in the recent years. The research for digital watermarking is mainly divided into two branches, i.e. embedding techniques and attacking methods. A systemic overview of the current attacking methods to digital image watermarking and the basic countermeasures against these attacks, as well as the analysis of the advantage and disadvantage of these attacks is given. The future directions in watermark techniques are also discussed.

Key words: digital watermarking; attacking methods; countermeasures

1 引　　言

数字水印是将信息 b 不可见地嵌入到数字数据 x 中(如图像、视频或音频信号),形成嵌入了水印的数据 y[1]. 经过处理、拷贝或重新分发,嵌入的信息应能从水印的数据中解码出来. 数字水印的潜在应用包括版权保护、分发跟踪、认证和条件使用控制等. 信息 b 可以是用户 ID,也可以是文件拷贝的序列码或认证信息.

在由掩模 M 给出的感知失真的限制下,水印可作为包含已编码和调制的水印信息 b 的外加信号 w,即 $y = x + w(M)$,其中 w 不必与原始信号 x 独立. 要使嵌入了水印的数据与原始数据在感知上相似,最简单的方法是保持水印信号的能量很低. 使用复杂的听觉或视觉模型,可获得更好的掩模 M,以加强水印方案的健壮性. 通常使用的嵌入方法可分为加性[2]、乘性[2]和量化[3]3 种. 在加性方案中, w 与 x 之间通常有微弱的依赖性;在乘性方案中, w 与 x 是相互依赖的;在量化方案中, w 与 x 具有很强的局部依赖性,但几乎是统计独立的.

水印方案的一个重要指标是对攻击的健壮性

收稿日期: 2003-05-12; **修回日期**: 2003-07-28.
基金项目: 高等学校博士点基金资助项目(20020288025); 江苏省自然科学基金资助项目(BK2001054).
作者简介: 刘春庆(1965—),男,山东昌邑人,博士生,从事信息隐藏理论与技术的研究; 王执铨(1939—),男,湖北武汉人,教授,博士生导师,从事信息安全、动态大系统等研究.

与安全性. 所谓水印攻击[4],就是对现有的数字水印系统进行攻击. 通过检验其健壮性与安全性,分析其弱点所在及其易受攻击的原因而改进设计. 这同传统密码学中的加密算法设计和密码分析是相似的. 在对水印嵌入技术进行广泛研究的同时,部分学者致力于水印攻击技术的研究. 与水印嵌入技术的发展类似,水印攻击技术也经历了一个快速发展的过程. 可以说这两种技术是在互相斗争中同步发展起来的.

1997 年,Peticolas 等人[5]发布了数字图像水印攻击软件 StirMark 的第 1 个版本 1.0 版,成功地攻击了当时的各种水印算法. 水印技术研究者随后对受到的攻击采取了相应的对策,对水印嵌入技术进行改进,研究出更安全的水印系统. 与此同时,也促进了更复杂的攻击技术的发展. StirMark 等陆续发布了 2.2,2.2b,2.3,3.0,3.1,4.1 版,现已成为应用最为广泛的数字图像水印基准测试工具. 此外,其他学者也在开发实用的水印攻击软件,如 Unzign[6], Checkmark[7]和 Opitimark[8]等. 现在,这些软件几乎整合了目前流行的主要攻击方式.

除了阻止水印正确检测和正确读取等攻击之外,在协议层上的攻击技术也得到了发展. Craver 等人[9]提出第 1 个协议攻击方法——可逆攻击,指出用于版权保护的水印必须是不可逆的. Kutter 等人[10]发现了另一种协议攻击方法——拷贝攻击,这类攻击无需任何关于水印技术或密钥的特定信息,能从一幅水印图像中将水印拷贝到另一幅目标图像. 目前,拷贝攻击已应用于 Checkmark 等水印攻击软件.

要研究新的更健壮更安全的水印系统,必须了解对数字水印的攻击技术. 本文将系统地论述目前对数字图像水印技术的常见攻击方法与基本对策,所介绍的内容也可借鉴到其他水印应用领域.

2 常见水印攻击方法与基本对策

根据文献[11]的描述,水印攻击方法可以分为 4 类:健壮性攻击、表达攻击、解释攻击和合法攻击. 其中前 3 类可归类为技术攻击,而合法攻击则完全不同,它是在水印方案所提供的技术特点或科学证据的范围之外进行的. 在此,仅论述常见的前 3 类技术攻击方法和一些基本对策.

2.1 健壮性攻击

健壮性攻击以减少或消除数字水印的存在为目的,包括像素值失真攻击、敏感性分析攻击和梯度下降攻击等. 这些方法并不能将水印完全除去,但可能充分损坏水印信息. 为抵抗这类攻击,总体要求水印算法是公开的,算法的安全性应依赖于与图像内容有关或无关的密钥及算法本身的特性.

2.1.1 像素值失真攻击

像素值失真攻击是指对图像像素值的修改,可分为信号处理攻击和分析攻击两种方法[11].

信号处理攻击是通过对水印图像进行某种操作,以削弱或删除嵌入的水印,而不是试图识别或分离水印. 这种攻击包括线性或非线性滤波、图像压缩、添加噪声、图像量化、模数或数模转换等. 造成像素值失真的 4 种基本攻击操作是:外加噪声、幅值变化、线性滤波和量化;其他的攻击操作可看作这 4 种基本方式的有机组合[12]. 在这 4 种基本攻击操作中,线性相关检测对外加噪声以及归一化相关检测对幅值变化都是健壮的,而变阈值的优化检测方法[13],对线性滤波和量化处理比相关检测具有更好的健壮性.

对于不同的攻击操作,可采用相应比较健壮的水印模型,如线性滤波对水印检测的影响依赖于加到每个载体频率上的水印信号能量的大小,因此可将水印模型设计成在滤波影响最小的频率上加入最大的水印能量[12]. 线性滤波实际上是信号与对称滤波器的卷积,并不影响 Fourier 系数的相位,所以将水印信号加到 Fourier 系数的相位上,不会受到这类线性滤波的影响[14]. 另外,使用扩频技术或在视觉显著的频率分量上嵌入水印,也能有效地抵抗多种像素值失真攻击[2].

对于使用优化的消除噪声的水印攻击方法,可采用满足功率谱条件的水印模式[15],使水印的功率谱与原图像的功率谱成比例;或将水印嵌入到感知重要的频率分量上,如嵌入到 DCT 变换的中低频系数上. 攻击者为除去水印必须对水印图像施加很强的攻击,这时攻击过的图像一般不能使用.

分析攻击是通过分析水印图像来估计图像中的水印,然后将水印从图像中分离出来并使水印检测失败. 常见的例子是合谋攻击,它有两种基本类型:其一是攻击者拥有同一个原图像嵌入了不同水印的拷贝,通过取所有拷贝的均值或仅从每个拷贝中取一小部分,可得到一个检测不到水印的原图像的近似值[2]. 其二是攻击者拥有嵌入了同一个水印的不同水印图像,对这些图像取均值并以这个均值作为嵌入水印的估计值,然后从水印图像中将这个估计值减去[16]. 它的一种变形是同一个水印重复嵌入一个数据的几个位置,再将这几个位置看作独立的而

实施上述合谋攻击,从而估计出嵌入的水印[17]. 一个攻击者拥有大约 10 个不同的拷贝就能成功地将水印除去[1].

合谋攻击依赖于获得很好的嵌入水印的估计值,借助于水印功率谱条件[15] 可削弱这类攻击. 另外,文献[18]提出针对第 2 种合谋攻击的安全对策,利用特殊的水印编码设计出 c^* 安全的水印方案.

2.1.2　敏感性分析攻击

水印敏感性分析攻击的基本思想是[19]:使用相关水印检测器寻找从水印检测区域到区域边缘的捷径,而该捷径可由检测区域表面的法线近似表示,并且该法线在检测区域的绝大部分是相对恒定的. 敏感性分析攻击一般可分为 3 步实施:

第 1 步,对欲攻击的水印图像 I_w,寻找一个非常接近相关检测区域边界的图像 I_{out}. 可通过多种方法改变图像 I_w 而获得图像 I_{out},如减少图像 I_w 的对比度或亮度的幅值,使用无水印图像与水印图像 I_w 的线性组合,使用水印图像 I_w 的平均值代替采样值. 运用上述 3 种方法逐步改变水印图像 I_w 的失真程度,直到不能检测到水印为止,所得图像作为图像 I_{out}.

第 2 步,找出图像 I_{out} 检测区域表面法线方向的近似值,这是进行水印敏感性分析攻击的核心. 文献[8]采用迭代技术估计检测区域表面法线,每步迭代给图像 I_{out} 加上一个 N 维随机向量并记下相关检测结果,如果检测到水印存在,则将该随机向量加到法线的估计值上;如果检测不到水印,则从法线估计值中减去该向量. 该法线方向估计值与图像 I_w 中水印的相关性是迭代次数的单调递增函数,当相关性达到预定要求时则停止迭代.

第 3 步,对该法线进行缩放调整作为水印的近似值,并将其从图像 I_w 中减去,得到质量良好的检测不到水印的近似图像.

水印敏感性分析攻击的成功,依赖于检测区域边界的法线可用于寻找越出检测区域的捷径. 如果检测区域边界的曲率使在每一点的法线仅提供关于该捷径方向的极少信息,则敏感性分析攻击在计算上是不可行的. 因此构造具有这种性质的水印检测区域是一个需要关注的问题.

2.1.3　梯度下降攻击

梯度下降攻击[12] 要求使用的水印检测器输出具体的检测值,而不仅是最终的二值判决结果(即是否检测到水印). 随着嵌入水印图像的缓慢改变,攻击者根据检测值的变化来估计水印图像检测统计量的梯度. 这种攻击的基本思想在于:检测统计量下降最快的方向是越出检测区域的捷径. 给定一个水印图像,可采用搜索策略确定检测统计量下降最快的局部梯度,图像沿该梯度方向可被某个量所改变. 这种处理过程可以逐步迭代下去,直到在改变的图像中检测不到水印为止.

梯度下降攻击的成功依赖于如下假设:局部梯度指出了通向检测区域边界的捷径方向. 这对许多检测统计量(包括线性相关和归一化相关) 是必然的. 为抵抗这种攻击,在检测区域内的检测统计量不应向边界方向单调下降,而应包含许多局部最小值,使得局部梯度方向不能提供确定越出检测区域边界的捷径的任何信息.

水印敏感性分析攻击和梯度下降攻击都是通过寻求从"水印存在"到"水印不存在"的边界所在,从而构造出不含水印的近似图像. 它们虽然效果良好,但都需要具备水印检测器才能实施.

2.2　表达攻击

表达攻击是让图像水印变形而使水印存在性检测失败. 与健壮性攻击相反,表达攻击实际上并不除去嵌入的水印,而试图使水印检测器与嵌入的信息不同步. 当二者完全同步时,检测器能恢复嵌入的水印信息,但对同步处理的复杂性要求太高而不便于实用. 为了战胜表达攻击,水印的检测算法应有与人交互的功能,或设计更复杂更智能的包含所有表达攻击模式的检测器.

2.2.1　置乱攻击

置乱攻击[12] 是指在将水印图像提交水印检测器之前,先对图像的像素值进行置乱,通过水印检测器之后再进行逆置乱. 这种置乱可以是像素值简单的行(或列) 的置换,也可以是比较复杂的随机置乱. 置乱程度与使用的检测策略有关. 最著名的置乱攻击是马赛克攻击[20],该攻击方法目的是挫败 Webcrawler. 它将嵌入了水印的图像分割成许多检测不到水印的小方块,这些小方块在 Web 页上按相应的 HTML 标记重新组装起来. Webcrawler 只能查看每个图像小块,但由于这些小块太小而无法容纳水印数据,所以 Webcrawler 无法发现水印. 对付这类攻击的一种策略是检测算法与人相结合.

2.2.2　同步攻击

许多水印技术对同步性非常敏感,要求在检测水印之前,嵌入了水印的图像必须正确对齐. 攻击者可在保真度的约束下,通过对图像的几何变形来干扰这种同步性,使得水印虽然存在但却检测不出来.

引起失同步的这些几何变形可以是简单的平移、旋转、缩放,或较复杂的图像剪切、水平翻转、行(或列)删除,以及随机几何变形(如直方图拉伸、均衡、非线性扭曲等),甚至是某些几何变形的组合. 攻击者可利用水印攻击软件 Unzign, Stirmark 等实施攻击. Unzign 引入了局部像素飘移,在对空域水印方案攻击时很有效; Stirmark 引入了全局和局部两种几何失真; Checkmark 可以进行扭曲、模板移除等攻击. 此外,还可利用水印同步方案的知识设计专用的攻击方法.

水印系统设计者所能采取的对策通常是预见可能的攻击方式,提高水印系统对同步攻击的健壮性. 常用的方法包括同步模板登记技术[21]、自相关函数方法[22,23]、不变水印技术[24,25]、内在同步技术[26~29]等. 自相关函数方法和同步模板登记技术要求确认几何变形和逆转变形后的水印检测必须是成功的,缺一不可;内在同步技术要求显著特征点在检测时能可靠地提取出来,但有些几何变形会影响显著特征点与图像的相对位置,从而使水印无法检测,这在设计水印系统时必须加以注意.

对于一个成功的表达攻击而言,并不需要削弱或除去水印,因此它几乎不影响图像质量,这是健壮性攻击和解释攻击所无法比拟的. 正由于表达攻击没有削弱或除去水印,当使用更复杂、更智能化的水印检测器时,很可能检测到图像中的水印,这是表达攻击的一个致命的弱点.

2.3 解释攻击

在一些水印方案中可能存在对检测出的水印具有多种解释. 解释攻击包括拷贝攻击、可逆攻击等,它使数字水印的版权保护受到了挑战. 潜在的解决方法是构建与图像内容相关的数字水印.

2.3.1 拷贝攻击

拷贝攻击[10]是从嵌入水印的图像中估计出水印并拷贝到目标图像的其他图像中. 拷贝的水印要自适应于目标图像,以保证其不可察觉性. 使用拷贝攻击在目标图像中生成一个有效的水印,这既不需要算法知识又不需要水印密钥知识. 拷贝攻击分为3步进行:第1步,找出图像中水印的估计值;第2步,处理该估计值,使得水印能量最大化并满足不可感知性要求;第3步,将处理后的水印估计值嵌入目标图像得到伪造的水印图像.

文献[10]的方法依赖于获得满意的原图像的估计值,使获得的估计值是不可行的来阻止拷贝攻击,如使用满足功率谱条件的水印模式[15]. 但是对最低位水印方案可直接进行拷贝攻击,只要将嵌入水印图像的最低位全部拷贝到目标图像的最低位上即可. 一种潜在的解决方法是运用密码签字技术,将水印与图像联系在一起. 如果在水印图像中将水印成功地拷贝到无水印的图像中,检测器便能确定该水印不属于后一个图像. 另外,基于量化的水印方案对拷贝攻击具有免疫力.

2.3.2 可逆攻击

可逆攻击[9]基于大多数水印方案的嵌入算法是可逆的和多数水印嵌入是健壮的这一事实,攻击者将水印嵌入过程逆过来使用即可. 可逆攻击对盲水印系统同样适用[9],可通过建立一个类似噪声但与发布的图像具有很高相关性的伪造水印实施攻击,这样的水印可通过提取和改变发布图像的某些特征来构造. 攻击者从发布的图像中减去伪造的水印便可建立一个伪造的原图像,从而使水印检测陷入死锁,造成图像所有权的模糊性.

水印嵌入算法必须设计成不可逆的. 方法是使水印依赖于图像的内容,如使用原图像的单向杂凑值作为伪噪声发生器的种子生成水印,这时攻击者要伪造一个原图像在计算复杂性上是不可能的;也可利用数字签名技术[30],将嵌入的水印及签名连同原图像的签名一起嵌入,这种方法可证明是安全的.

拷贝攻击和可逆攻击都属于在协议层上的攻击,会对水印的许多应用造成严重损害. 在版权保护方面,可逆攻击的威胁要大得多,因为任何人都可声称他对访问过的任何水印图像拥有所有权;拷贝攻击在这方面的应用是作者盗用某名人的名义,出售自己的作品以牟利. 在有关身份认证的应用中,拷贝攻击所造成的威胁是重大的,使得用户无法根据水印的检测结果确定作品来源的真实性.

从以上分析可以看出,健壮性攻击将对水印造成实质性的损害,遭受这类攻击的水印是难以检测或恢复的;表达攻击是水印方案面临的公开问题,目前仍然缺乏有效的对抗策略,只能通过预见可能遇到的具体攻击方法进行预防,由于它不影响水印的存在性,使用更先进的检测器可能检测到攻击过的水印;解释攻击破坏了水印应用的基础,攻击的是水印必须具有的唯一性解释,但在采取相应的措施后这种攻击是难以实施的.

3 对未来研究趋势的展望

数字水印技术是一个新兴的具有相当难度的研究领域,但目前还没有一种算法能够经得起所有的攻击. 该领域还有许多未涉及的研究课题,作者认

为以下几方面问题尤为值得关注:

1) 亟需建立完善的水印理论体系. 水印技术及其攻击分析的研究依赖于水印技术整体理论框架的建立,虽然它借鉴了通信理论、信息论、对策论等,但仍未建立起完善的水印理论体系. 由于缺乏系统的理论体系,水印技术的研究和应用必将受到极大的制约.

2) 建立更加完善的水印评估标准. 该标准应包括水印隐藏分析和攻击测试两个方面,而目前广泛使用的水印测试软件都没有涉及隐藏分析,也没有考虑水印嵌入过程可能暴露水印的存在性,仅仅注重了移除水印和阻止水印正确检测等问题.

3) 研究更加安全的专用水印算法. 目前开发安全通用的水印系统是不现实的,必须根据具体的应用环境预见可能遭受的攻击方式. 对各类攻击组成的综合攻击展开研究并寻求对策是一个重要的课题.

此外,还应在理论上证明水印嵌入算法本身所具有的抗攻击性能;在技术上对遭受攻击的水印信息进行修复,使其恢复嵌入的信息;并且分析现有水印技术的缺陷,研究新的水印攻击方法.

4　结　　语

本文较为系统地介绍了数字图像水印的常用攻击技术,分析了各类攻击方法的攻击目的、适用环境及其优缺点,并给出了挫败这些攻击的一些基本对策. 应当清楚地认识到,数字水印研究的两个方面(即水印算法设计和水印算法攻击)是互相依存、互相促进的,好的攻击方案能促使人们设计出更好的水印算法;而好的水印算法的出现也促使人们考虑对它的有效攻击. 对数字水印攻击方法和水印算法设计的研究,必将导致更好的水印方案的出现和更成功的数字水印的应用.

参考文献(References):

[1] Voloshynovskiy S, Pereira S, Pun T, et al. Attacks on digital watermarks: Classification, estimation-based attacks and benchmarks[J]. *IEEE Communications Magazine*, 2001,39(8):118-125.

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

[3] Chen B, Wornell G W. Dither modulation: A new approach to digital watermarking and information embedding [A]. *Proc of SPIE*[C]. Bellingham: Society of Photo-optical Instrumentation Engineers,1999. 342-353.

[4] 易开祥,石教英,孙鑫. 数字水印技术研究进展[J]. 中国图像图形学报,2001,6(2):111-117.
(Yi K X, Shi J Y, Sun X. Digital watermarking techniques: An introductory review[J]. *J of Images and Graphics*,2001,6(2):111-117.)

[5] Petitcolas F A P, Kuhn M G. Attacks on copyright marking systems[A]. *Proc of the Second Int Workshop on Information Hiding*[C]. Berlin: Springer,1999. 218-238.

[6] Petitcolas F A P. Watermarking schemes evaluation[J]. *IEEE Signal Processing*,2000,17(5):58-64.

[7] Pereira S, Voloshynovkiy S, Madueno M, et al. Second generation benchmarking and application oriented evaluation[A]. *Proc of the Fourth Int Workshop on Information Hiding*[C]. Berlin: Springer,2001. 340-353.

[8] Solachidis V, Tefas A, Tsekeridou S, et al. A benchmarking protocol for watermarking methods[A]. *Proc of IEEE Int Conf on Image Processing*[C]. Thessaloniki: Institute of Electrical and Electronics Engineers Commputer Society, 2001. 1023-1026.

[9] Craver S, Memon N, Yeo B L, et al. Resolving rightful ownerships with invisible watermarking techniques: Limitations, attacks and implications[J]. *IEEE J on Selected Areas in Communications*,1998,16(4):573-586.

[10] Kutter M, Voloshynovskiy S, Herrigel A. The watermark copy attack[A]. *Proc of the SPIE*[C]. San Jose, 2000. 371-380.

[11] 杨义先,钮心忻,任金强. 信息安全新技术[M]. 北京: 北京邮电大学出版社,2002. 56-59.

[12] Cox I J, Mill M L, Bloom J A. *Digital Watermarking* [M]. San Francisco: Morgan Kaufmann Publishers, 2001. 241-316.

[13] 赵春晖. 基于优化检测原理的鲁棒非加性水印算法[J]. 哈尔滨工程大学学报,2002,23(4):14-20.
(Zhao C H. Robust non-additive watermark algorithm based on optimum detection theory[J]. *J of Harbin Engineering University*,2002,23(4):14-20.)

[14] Kalker T, Janssen A J. Analysis of watermark detection using SPOMF[A]. *Proc of the Int Conf on Image Processing*[C]. San Jose,1999. 319-319.

[15] Su K, Girod B. Power-spectrum condition for energy-efficient watermarking[A]. *IEEE Int Conf on Image Processing*[C]. Los Alamitos,1999. 301-305.

[16] Cox I J, Linnartz J M G. Some general methods for tampering with watermarks[J]. *IEEE J on Selected Areas in Communications*,1998,16(4):587-593.

[17] Boeuf J, Stern J P. An analysis of one of the SDMI candidates[A]. *Proc of the Fourth Int Workshop on Information Hiding*[C]. Berlin: Springer,2001. 368-374.

[18] Boneh D, Shaw J. Collusion-secure fingerprinting for digital data[A]. *Proc of Advances in Cryptology, Lecture Notes in Computer Science*[C]. Berlin: Springer, 1995. 452-465.

[19] Kalker T, Linnartz J P, Dijk M V. Watermark estimation through detector analysis[A]. *IEEE Int Conf on Image Processing*[C]. Los Alamitos, 1998. 425-429.

[20] Petitcolas F A P, Anderson R, Kuhn M G. Information hiding: A survey[J]. *Proc of the IEEE*, 1999, 87(7): 1062-1078.

[21] Tirkel A Z, Osbourne C F, Hall T E. Image and watermark registration[J]. *Signal Processing*, 1998, 66(3): 373-383.

[22] Kutter M. Watermarking resisting to translation, rotation and scaling[A]. *Proc of SPIE*[C]. Boston, 1998. 423-431.

[23] Honsinger C. Data embedding using phase dispersion[A]. *IEE Seminar on Secure Image and Authentication*[C]. London, 2000. 5: 1-7.

[24] Lin F, Brandt R D. Towards absolute invariants of images under translation, rotation and dilation[J]. *Pattern Recognition Letters*, 1993, 14(5): 369-379.

[25] Kim H S, Baek Y, Lee H K. Rotation-scale-and translation-invariant image watermark using higher order spectra[J]. *Optical Engineering*, 2003, 42(2): 340-349.

[26] Bas P, Chassery J M, Davoine F. Geometrical and frequential watermarking scheme using similarities[A]. *Proc of SPIE*[C]. Bellingham: Society of Photo-optical Instrumentation Engineers, 1999. 264-272.

[27] Bas P, Chassery J M, Macq B. Robust watermarking based on the warping of pre-defined triangular patterns[A]. *Proc of SPIE*[C]. Bellingham: Society of Photo-optical Instrumentation Engineers, 2000. 99-109.

[28] Bas P, Chassery J M, Macq B. Geometrically invariant watermarking using feature points[J]. *IEEE Trans on Image Processing*, 2002, 11(9): 1014-1028.

[29] Izquierdo E. Using invariant image features for synchronization in spread spectrum image watermarking[J]. *Applied Signal Processing*, 2002, (4): 410-417.

[30] Katzenbeisser S, Veith H. Securing symmetric watermarking schemes against protocol attacks[A]. *Proc of SPIE*[C]. San Jose: The Int Society for Optical Engineering, 2002. 260-268.

下 期 要 目