文章编号:1005－0523(2004)01－098－05

# 图像数字水印的应用及基准测试软件

吴志强

(华东交通大学 机电工程学院,江西 南昌 330013)

**摘要**:近年来,随着各种图像数字水印算法的提出,研制针对不同水印应用系统的基准测试软件将对数字水印的发展起到很好的促进作用.本文在讨论图像数字水印的各种应用及影响图像数字水印系统的重要参数的基础上,对数字水印的各种典型的攻击方式进行了较完整的分析,最后对现有的典型基准测试程序进行了探讨,指出了它们的局限性.

**关 键 词**:图像数字水印; 鲁棒性; 基准测试

**中图分类号**:TP391 **文献标识码**:A

## 1 引 言

随着计算机技术、通信技术、信息处理技术和智能化网络技术的日新月异,WWW 上数字媒体的运作和服务方式也在不断翻新,如电子印刷出版、数字仓库和数字图书馆、网络视频和音频、电子商务等.这些以网络电子版方式传播的知识产品在给人们带来信息共享和商业利润的同时,也面临着盗版、非法复制以及存取失控等日益严重的威胁.因此对数字媒体的提供商和原创作者而言,如何进行切实有效的知识产权(intellectual property rights)保护是一个值得关注的课题.依靠密码学的加密技术虽然能保证数字产品内容的安全传送,但是加密的内容一旦被破解,传统的密码技术就无有效的手段来保证其不被非法拷贝、再次传播和盗用[2].为了防止这种情况的发生,数字水印技术应运而生.从 1993 年 Caronni[2] 提出第一个数字水印方法到现在近十年的时间,全世界范围内在这一领域的研究活动蓬勃发展.在大量的研究文献中,人们一般对数字水印的设计方法比较注重,而往往忽略了一个重要的问题,这就是如何对水印系统的合理测试和评估.目前,对水印的测试可以使用现有的一些图像处理软件,如 Photoshop,利用这些软件可以对图像进行一 些常规的操作如:滤波、锐化、模糊、压缩甚至一些简单的几何变形.但如果要对水印的鲁棒性作系统的测试,则必须使用基准测试软件.至今为止,在全世界研究的能够被大家接受的基准软件并不多,最权威的要数英国剑桥大学近年推出的软件 Stirmark 和瑞士日内瓦大学开发的 Checkmark.

本文的第 2 部分对图像数字水印的应用及影响其性能的参数进行了讨论;第 3 部分对图像数字水印的攻击方式作了较完整的分析;第 4 部分对现有典型的基准测试程序进行了探讨,指出了它们的局限性;第 5 部分为结论部分.

## 2 影响图像数字水印的应用及性能参数

综合国内外学者提出的各种定义并分析已有的数字水印方案,数字水印可以定义为: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,而且并不影响宿主数据的可用性.虽然对水印性能的期望值需要放低一些,但其在许多大规模的商业应用中无疑具有十分旺盛

**收稿日期**:2003－09－06

**作者简介**:吴志强(1960－),男,江西南昌人,华东交通大学高级工程师.

的生命力[1].

目前,图像数字水印主要包括以下四种应用:所有者识别(owner identification)、所有权证明(proof of ownership)、认证(authentication)、违反者跟踪(Traitor Tracking).

1) 所有者识别:虽然版权标记对保证版权不再是必需的,但它仍然被广泛使用.版权标记的形式通常是"? 日期,所有者".在书或照片的显眼位置、影片演员表的末尾、都可以看到版权标记.这样的明文版权标记有一个缺点,即它经常被从受保护对象上除去,因为包装可被扔掉,电影的演员表可被删掉,图像也可被剪切.Digimarc 公司为此项应用专门设计了一套水印系统,并投入市场[2].该系统将嵌入和检测模块加到 Adobe 的通用图像处理程序 Photoshop 上,检测器一旦发现水印即向中央数据库查询,以便识别水印的所有者.

2) 所有权证明:通常,多媒体产品的所有者希望水印不仅能够识别版权信息,而且可以证明所有权.举例说明之:假设 Alice 将她创作的一幅带有版权标记"? Alice 2000"的图像在网上发布,Bob 盗窃了这幅图像并用图像处理技术将版权标记改为"? Bob 2000",如果 Bob 宣称该图像的版权属于他,那么这样的版权纠纷如何解决? 按照传统的方法,首先 Alice 将图像的拷贝发送给版权机构进行注册,然后版权机构将图像和版权所有者信息存档.当 Alice 和 Bob 发生版权纠纷时,Alices 可以从版权机构获得她是合法所有者的证明.如果 Alice 没有将图像注册,那么她至少应该能够出示图像的底片,但由于数字图片接收的迅捷性,出示底片是不现实的.从理论上来说,Alice 把水印嵌入到图像中以证明自己的所有权是可行的.但是,正如 Craver 等人所说的那样,这并不是一个简单的问题.

3) 认证:随着照像机和视频摄录机越来越多地运用到数字技术,对图像进行窜改的能力也越来越强.数字照片可以轻易地被改动而又让人难以察觉,这就造成甚至无法利用原始的底片进行检验.在很多的应用中,图像的真实性是至关重要的,例如法律案例和医学图片.关于认证问题,密码学中已进行了深入地研究.Friedman 通过计算图像的密码签名创设了一种"可信赖像机",在其中他首次讨论了验证技术的应用.在他的方法中只要像素的一个比特被修改,图像和签名就不再匹配,因此任何窜改都可以被检测出来.但是这种签名是一种变形数据,它必须和图像一起传送,通常被置于某种特殊图像格式的文件头中,如果图像被拷贝成另一种不包含同样文件头的格式,则签名将会丢失,图像也就不再能进行验证.一个完美的解决方法是利用水印将签名直接嵌入到图像中.那样就不必担心签名和图像会分离,而且由于水印和图像遭到的窜改是相同的,我们可以对此种窜改进行更多的了解.因此,有些水印系统可以指出图像发生改变的大致位置,还有一些系统允许对图像作特定改变,如 JPEG 压缩,但不允许图像发生更大的实质性的改变,如从罪证照片中移去重要目标.

4) 违反者跟踪:数字水印还可用于监视或追踪数字产品的非法复制,这种应用通常称作"指纹"(Fingerprinting).它类似于软件产品的序列号,即在每个发行拷贝中嵌入不同的水印.因为单个加入水印的拷贝会受到共谋攻击(Collusion Attacks),嵌入的水印必须被设计成共谋安全的.在一些应用场合,如:在 WWW 上用特定的网络搜索器搜索盗版图像,指纹的提取必须要简单、快捷.

各种不同的水印系统最重要的性能是鲁棒性(抵御各种无意或有意去除图像中所嵌入的水印的能力),而其鲁棒性又主要依赖以下几个重要参数:

1) 嵌入信息的数量:这是一个重要的参数,因为它直接影响水印的鲁棒性.对同一种水印方法而言,要嵌入的信息越多,水印的鲁棒性越差.

2) 水印嵌入强度:水印嵌入强度(对应于水印的鲁棒性)和水印的可见性之间存在着一个折衷,增加鲁棒性就要增加水印嵌入强度,相应地会增加水印的可见性.

3) 图像的尺寸和特性:虽然尺寸小的含有水印的图像没有多少商业价值.但一个水印软件应该能够从小图片中恢复出水印,这样可以有效地防止水印的马赛克攻击.除了图像尺寸之外,图像的特性也对水印的鲁棒性产生重要影响.如:对扫描的自然图像具有高鲁棒性的水印方案在应用于合成图像(如计算机生成图像)时,鲁棒性会大大削弱.一个合理的基准测试所能适应的图像尺寸应该很大,并且应能使用不同类型的测试图像.

4) 秘密信息(如密钥):尽管秘密信息的数量不直接影响水印的可见性和鲁棒性,但它对系统的安全性起了重要的作用.和其它的安全系统一样,水印系统密钥空间(秘密信息允许取值的范围)必须足够大,以使穷举攻击法失效.

## 3 图像数字水印的攻击方法

水印是用来保护所有者信息所有权的声明或是所有者用来控制信息内容的手段.攻击者的目的是想要消除信息所有者拥有的水印内容的有效性.正如象计算机安全问题那样,保密算法的安全并不代表整个计算机系统的安全,水印系统的安全并不只是水印算法本身的鲁棒性高,还存在着其他方面的问题,因为水印生命周期中的任何一个阶段若被攻击者破坏了,就可以打破水印对信息的保护.因此,信息内容所有者和水印软件开发者必须认识和分析水印每一个阶段可能受到的攻击,以确保有足够的安全方法对抗攻击.我们把水印的攻击分为以下五大类:

1) 鲁棒性攻击:在不损害图像使用价值的前提下减弱、移去或破坏水印.它包括常见的各种信号处理操作,如图像压缩、线性或非线性滤波、叠加噪声、图像量化与增强、图像裁剪、几何失真、模拟数字转换以及图像的校正等.还有一种可能性是面向算法分析的,这种方法针对具体的水印插入和检测算法的弱点来实现攻击.如 StirMark[6]攻击方案中,它以几乎注意不到的轻微程度对图像进行拉伸、剪切、旋转等几何操作进行几何攻击,也可以对图像进行重采样攻击,即通过模拟打印—扫描过程引入一定的误差.

2) IBM 攻击:这是由美国 IBM 公司的水印技术研究小组针对可逆水印算法而提出来的一种水印攻击方案,因而也称之为 IBM 水印攻击方案,它是针对可逆、非盲(non-oblivious)水印算法而进行的攻击.其原理为设原始图像为 I,加入水印 $W_A$ 的图像为 $I_A=I+W_A$.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 $I_A=I_F+W_F$.这就产生无法分辨与解释的情况.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) 马赛克攻击:马赛克攻击(Mosaic attack)并不一定要移去水印,它的目标是对数据作一定的操作和处理,使得检测器不能检测到水印的存在.一个典型的例子是用这种方法愚弄 Internet 上的自动侵权探测器 Webcrawler.这个探测器自动在网上下载图片,然后根据水印检测有无侵权行为,它的一个弱点是当图像尺寸较小时,会认为图像太小,不可能包含水印,这样我们可以先把水印图像分割,使每一小块图像的尺寸小于 Webcrawler 要求的尺寸下限,再和合适的 HTML 标记把小图像重组在 Web 页中.这种攻击方法一点也不改变图像的质量,但由于 Webcrawler 看到的只是单个的小图像,所以它失败了.对付马赛克攻击的一种方法是研制的水印软件能够从小图片中恢复出水印

4) 共谋攻击:所谓共谋攻击(Collusion attack)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.对付共谋攻击的一种方法就是限制可用的水印拷贝个数,也可采用共谋安全码来设计水印方案,但采用共谋安全码方案的不足是:随着编码数目的增加,编码长度按指数增加.

5) 法学攻击:这种攻击方法与前三种方法极为不同,它主要是利用法律上和一些条款的漏洞以达到攻击的目的,这种攻击大多数已超出了技术讨论的范围.

## 4 典型基准测试软件及其局限性

### 4.1 典型基准测试软件

目前有许多水印攻击测试软件如 Stimark,Unzign,RichardBarret's attack software,Checkmark 和 Optimark 等,其中比较有代表性的是 Stimark, Checkmark 和 Optimark.它们已经成为水印攻击软件的典范,对它们进行功能上的分析,对水印嵌入系统的研究,具有重要的实际意义.

StirMark 是剑桥大学计算机实验室编写的一个用于测试图像水印技术鲁棒性的免费工具软件.它从 1997 年 11 月开始推出,先后有 1.0、2.2 、2.3、3.0、3.1、4.0 等多个版本的软件,此软件多个平台有 Linux、Winddows9x/WindowsNT、Macintosh 等各种版本.StirMark 提供了对图像进行高斯滤波、中值滤波、锐化、拉普拉斯攻击、JPEG 压缩、比例伸缩、挤压、旋转、去除行或列、水印翻转等各种图像处理操作,同时还采用模拟重采用仿真扫描/打印过程.对水印图像只要使用 StirMark 一次,就能引入不可见的图像降质.StirMark 还提供了一个水印系统测试方案,根据这个测试基准,可以对水印图像进行一系列的攻击.对各种水印方案进行测试,可得到各种方法的对比结果.体现 StirMark 公正性的另一重要方面是图像水印算法的测试对象可以是取材各

异的标准图片.从信号处理的角度来看,这些图片分别具有各种各样的特征,如:具有纹理/平滑区域;边缘整齐;可进行尖锐化处理、模糊处理及亮度/对比度的调整等,也包含各种内容、尺寸和类型的图像.我们可以在 StirMark 软件网站上免费下载这些图片.

Checkmark[3]是由瑞士日内瓦大学开发的一种基准测试工具,它是在 UNIX 或 Windows 平台下运行于 Matlab 上的用于数字水印技术的一组基准套件. Checkmark 最初的 1.0 版是在 2001 年 6 月 10 发布的,后来又发布了 102, 104, 105 版,最新的 Checkmark 是在 2001 年发布的 1.2 版,已支持彩色图像,在线 FAQ(常见问题解答),并更新了在线结果. Checkmark 根据 Stirmark 改写了全部的攻击类,还包含了一些未在 Stirmark 中提出的攻击,而它还考虑了水印应用.与 Stirmark 相比,添加了新的质量测量方法—加权 PSNR 和 Watson 测量方法,以灵活的 XML 格式输出和生成 HTML 结果表格;应用驱动评估,特别是用于算法的快速测试的非几何应用,其算法不包括同步机制;容易将 Matlab 的单个攻击用于测试.

Optimark[3]是用于静止图像水印算法的一个基准测试工具,它由希腊 Thessalonikir 的 Aristotle 大学信息学系的人工智能和信息分析实验室开发.目前 Optimark 最新的版本是 2002 年更新的 1.0 版.与 Stirmark 和 Checkmark 不同的是, Optimark 具有图形界面,它能利用不同的水印密钥和信息,使用多重测试进行检测/解码性能评估. Optimark 针对水印检测器给出的不同结果(浮点结果或二值结果),相应给出不同的性能测量方法的评估.此外, Optimark 还提供了对解码性能的测量方法、平均嵌入和检测时间、算法有效载荷以及某一攻击和某一性能标准的算法崩溃极限的评估.使用用户在选定的攻击和图像上定义的权后, Optimark 能给出多重等级的结果,并且用户还可以选择自定义和事先设置基准部分.

### 4.2　现有基准测试软件的局限性

现有水印基准测试软件是对鲁棒水印技术的检测,用它们来评价现今的水印技术还存在以下局限性:

1) 水印按稳健性划分,可分为鲁棒性水印和易损性水印,现有的测试没有考虑易损性水印.

2) 现有的测试没有考虑隐藏分析,即对水印嵌入系统可能带来暴露隐藏信息存在性的问题没有考虑,它们仅仅注重移除水印和阻止水印正确读取的问题.

3) 面向不同需求的水印系统,应该有不同的评价标准;因此,仅仅采用一种测试评价是不合理的.

4) 水印系统应该有一个基本必要安全条件,它必须满足这个基本条件,然后才能进行更深层次的测试,而目前的基准测试软件没有涉及到这个基本问题.

## 5　结束语

数字水印技术的发展不能仅局限在新算法的提出,在图像中嵌入水印,随即进行提取,尚不足以说明算法性能的优劣,还要保证图像在经过形变之后仍能正确分离.为了能够全面地评估水印算法的性能,进而客观、公正地比较算法的有效性,研制针对不同水印应用系统的基准测试软件,是非常有意义的工作.

**参考文献:**

[1] I.J.Cox, Matt L.Miller and Jeffrey A.Bloom, Watermarking applications and their properties. int. conf. On Information Technology2000. Las Vegas.

[2] G.Caronni Ermitteln unauthorisierter verteriler maschinenlesbaren daten. Technical report , ETH Ziirich, Switzerland, August, 1993.

[3] V.Solachidisv, TefasA, NikolaidisN, TsekeridouS, KikolaiddisA, PitasI. A benchmarking protocol for watermarkin methods. In: Proceeding of 2001 IEEE International conference Image Processing(ICIP '01), Thessaloniki, Greece, 2001. 1023～1026.

[4] M.G.Kuhn, and F.A.P.Petitcolas. a Fair Benchmark for Image Watermarking Systems. Electronic Imaging '99, Security and Watermarking of Mulitimedia Contents, 1999(3657).

[5] 王道顺,等. 图像水印系统有效性的评价框架[J].计算机学报,2003,(7):779—788.

[6] 刘　彤,裘正定.图像数字水印的评估[J].计算机工程与应用,2001,(23):91—92.

(下转第 120 页)

# Developing New Algorithm of Finding Prime Factorization in a Positive Integer by New Method

**WANG Sen[1], WANG Bo[2]**

(1. East China Jiaotong University Nanchang 330013, China; 2. No. 15 Middle School of Qi-Qi Har City 161005, China)

**Abstract**: In this paper a the algorithm of finding frime factorization in a positive Integer is developed by a new method and the analysis of this algorithm is given.

**Key word**: PAR method; prime factrization; algorithm

---

(上接第 101 页)

# Application and Benchmark Test Sotfware of Image Digital Watermarking

**WU Zhi-qiang**

(School of Mechanical Engineering, East China Jiaotong University, Nanchang, Jiangxi, 330013 China)

**Abstract**: In recent years, with many arithmetics of image digital watermarking having been proposed, the digital watermarking will be brought advance to, when benchmark testing softwares are developed to aim at the different applications of digital watermarking. To address this issues, the applications and important parameters of digital watermarking system are discussed at frist, and then the typical attacks for it are analysed integratly, At last the existing benchmark stirmarks is probed into, and it's localizations are pointed out.

**Key words**: image digital watermarking; Robustness; benchmark testing software