基于图像的数字水印技术

吕建勋，贾世杰
（大连交通大学 电气信息学院，辽宁 大连 116028）

摘 要：随着信息技术和Internet的飞速发展，数字水印技术已成为信息安全领域的一个重要内容。目前数字水印技术正处于一个快速发展和持续深入的阶段，应用领域也在快速扩展。在简要介绍了数字水印技术的基础上，着重分析了基于图像的数字水印及分析技术，对图像数字水印技术的产生、发展及主要算法进行了分析。随着人们对数字水印技术的认识和研究的不断深入，它必定会在Internet网络图像、数字图书馆、医学应用等方面发挥巨大作用。

关键词：信息隐藏；数字水印；数字图像
中图分类号：TP391.41 **文献标识码**：A **文章编号**：1673-629X(2009)02-0173-03

Digital Watermark Technologies Based on Images

LÜ Jian-xun, JIA Shi-jie
(College of Electrical & Information, Dalian Jiaotong University, Dalian 116028, China)

Abstract: With the rapid development of the information technology and Internet, the digital watermark technology has become an important aspect of information security. Currently the digital watermark technology is on the process of increasing fast and continuous development, and the application fields are also expanding rapidly. Briefly introduces the technologies of digital watermark, especially analyzes the digital watermark technologies based on images. Besides, the generation, development and main algorithms are also being discussed. With the constant deepening of research on the digital watermarking technology, it will playe a great role in many fields, such as Internet network images, digital libraries, medical applications, etc.

Key words: information hiding; digital watermark; digital image

0 引 言

随着Internet与数字媒体信息服务的飞速发展，信息安全问题日益突出。多媒体信息在网络上的传递、发布和扩散带来了一系列的问题和应用需求，从总体上来说可以分为两大部分：伪装式保密信息传递（即信息隐藏）和多媒体信息的版权保护问题（即数字水印）。信息隐藏主要应用在需要安全保密通信的部门，利用多媒体信息中的冗余空间携带隐蔽信息，达到秘密信息伪装传递的目的；数字水印从实质上说也是一类信息隐藏，但是其目的不是为了保密通信，而是为了标明载体本身的一些信息，如多媒体信息的创作者、版权信息、使用权限等一系列需要标明的信息，利用数字水印，还可以跟踪多媒体产品的非法传播和扩散，打击盗版。数字水印技术目前正处于一个快速发展和持续深入的阶段，应用领域也在快速扩展。从最初的图像水印、音频水印，发展到软件水印、视频水印、文字水印；从最初的算法研究，扩展到行业领域的应用，如数字地图的版权保护、数字图书的版权保护、证件防伪、多媒体数据的检索、电子公文防篡改等。

收稿日期：2008-06-13
基金项目：辽宁省教育科学研究项目（2006B024）
作者简介：吕建勋（1985-），男，辽宁大连人，研究方向为通信与信息工程。

1 数字水印技术的产生与发展

Van Schyndel等人在ICIP'4 94会议上发表了题为"A digital watermarking"有关数字水印的论文，提出了数字水印的概念及其可能的应用，并针对灰度图像提出了两种向图像最低位中有效位嵌入水印的算法，标志着这一领域的开始[1]。1996年在英国剑桥召开了信息隐藏领域的第一次学术研讨会，这标志着信息隐藏作为一个新的科学学科的诞生。1999年12月，Stefan Katzenbeisser和Fabien A. P. Petitcolas等人出版了信息隐藏领域的第一本专业论著"Information hiding and techniques for steganorgraphy and digital watermarking"，该书概述了数字水印和隐写术领域近年来的发展，是信息隐藏领域里比较权威的著作[2]。

十多年来，数字水印技术得到了长足的发展。在

水印嵌入及解码方面，经历了从最初简单的基于 LSB 的位平面的调整算法，到 Cox 等人提出的基于扩频技术的数字水印算法和 Bami 等人提出的 DCT(Discrete Cosine Transformation，离散余弦变换)域盲水印算法，以及 Phil 提出的基于模型的数字水印算法等等[3]。在水印检测方面，Jessica Fridrich 等人提出了在彩色图像中检测隐藏信息的方法，也称为 RQP(Raw Quick Pairs)方法[4]。Jessica Fridrich 等人还提出了一种基于无损嵌入容量的 LSB 信息隐藏检测方法[5]。该方法适用于灰度或彩色图像。Yeuan－Kuen Lee 和 Ling－Hwei Chen 提出了一种转换密度函数的方法来检测基于位平面的 LSB 嵌入[6]。Guo－Shiang Lin 和 Wen－Nung Lie 提出了基于特征分析方法的信息隐藏信息检测方法[7]，可以适用于时空域和频率域。Hary Farid 提出了一种基于高阶统计量的检测模型[8]。Honeyman 等人开发了基于 JPEG 的隐藏信息检测的系统[9]。在水印攻击方面，简单的方法有线性滤波，几何变换，JPEG 压缩等，还有 Martin Kutter 等提出的基于拷贝的攻击方法，Cox 等人提出的联合攻击方法[10]，以及 Craver 等人利用水印算法提取水印时需要原始图像的弱点而提出的虚假水印攻击方法等一些特殊攻击方法。该系统是基于网络的检测系统，可以自动收集 JPEG 图像文件，并检测多种 JPEG 的隐藏工具。

目前，国际上剑桥大学、IBM 研究中心、NEC 美国研究所、麻省理工学院等都对数字水印进行了深入的研究。国内在信息隐藏与数字水印方面的研究起步稍晚，可喜的是，随着国际间的信息与技术交流，国内关于信息隐藏的研究也迅速升温。1999 年 12 月召开了第一届信息隐藏学术研讨会，会议决定研讨会每年召开一次，以促进国内信息隐藏技术的研究工作。2000 年 1 月，由国家 863 计划智能计算机专家组织展开了“数字水印技术学术研讨会”，充分反映了我国对这一领域研究的高度重视和大量投入。2004 年国家颁布了《中华人民共和国电子签名法》，给数字水印技术的应用提供了必要的法律依据。目前，国内清华大学、北京大学、北京邮电大学、中科院自动化所、北方工业大学、浙江大学、国防科技大学等也都在对该技术进行深入研究。

在实用化方面，20 世纪 90 年代末期国际上开始出现一些数字水印产品。美国的 Digimarc 公司率先推出了第一个用于静止图像版权保护的数字水印软件，而后又以插件形式将该软件集成到 Adobe 公司的 Photoshop 和 Corel Draw 图像处理软件中。AlpVision 公司推出的 LaveIIt 软件，能够在任何扫描的图片中隐藏若干字符，用于文档的保护与跟踪。IBM 公司将数字水印用于数字图书馆的版权保护系统。日本电气公司、日立制作所、先锋、索尼等正联合开发同一标准的基于数字水印技术的 DVD 的版权保护技术，使得消费者可以在自用的范围内复制和欣赏高质量的动画图像节目，而以盈利为目的大批量非法复制则无法进行。德国最近在利用数字水印来保护和防止伪造电子照片的技术方面取得很大进展，该技术可以用于个人身份证的防伪[11]。一些国际标准中已结合了数字水印或者为其预留了空间。SDMI 规范中联合加密和数字水印技术来实现版权保护。已经颁布的 JPEG2000 国际标准中，为数字水印预留了空间。已颁布的数字视频压缩标准 MPEG－4(ISO/IEC 14496)，提供了一个知识产权管理和保护的接口，允许结合包括数字水印在内的版权保护技术。

2 基于图像数字水印技术的主要算法

由于通信技术与信息隐藏的相似性，人们借鉴通信理论来描述信息隐藏模型[12]。目前通常将数字水印看作是一个通信过程，这里以一个数字图像水印系统来分析数字水印，而其它的媒体形式应该是大同小异的。一个完整的数字图像水印的通信系统模型如图 1 所示。

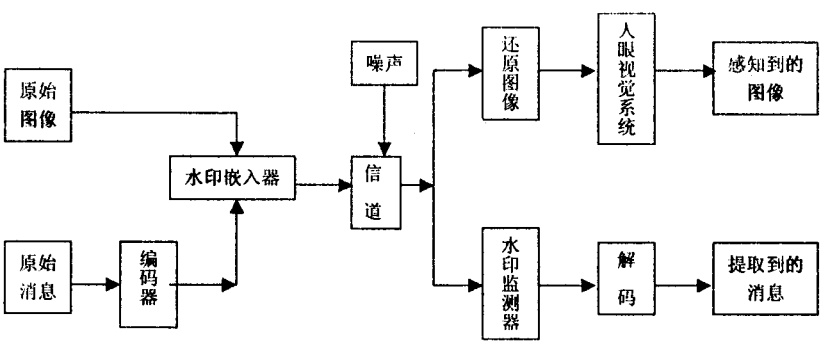

图 1 一个完整的数字图像水印的通信系统模型

目前研究最多和最深入的是在静止图像中的隐藏，一方面是由于静止图像具有较大的冗余空间来隐藏信息(如 BMP 图像)，另一方面图像处理工具较多且隐藏效果直观。在静止图像中的水印技术主要有如下四种[13]。

2.1 基于空间域的水印技术

空间域技术直接更改图像的数据，通常是在图像的亮度或彩色光带或者两者之上加一个调制信号嵌入数字水印。该技术属于早期研究，目前的水印技术大都基于最不显著位 LSB(least significant bit)方法。这

种水印具有一定的鲁棒性,但由于它位于图像的 LSB 上,所以很容易被去除,且容易受到有损压缩、量比、有噪信道传输的影响而丢失无法满足数字水印的鲁棒性要求。时空域信息隐藏技术的特点是易于实现和隐藏容量大,但其稳健性较差,适用于隐蔽通信。

2.2 基于变换域的数字水印技术

变换域水印技术是先将图像变换到频率域,改变图像的频率域系数,然后进行反变换得到加入水印的图像如扩频隐藏、DCT 隐藏、小波隐藏技术等,若以彩色图像为宿主,则此类技术主要利用人眼对高空间频率分量上噪声不敏感的特点,将待隐藏信息编码到图像的高频分量,以实现信息隐藏的目的 。此类技术的优点是,在变换域中嵌入的隐藏信号能量可分布到空域的所有像素上,有利于保证水印的不可见性;其次,在变换域,视觉系统的某些特性可更易结合到水印的编码过程,且与国际数据压缩标准兼容,实现在压缩域内的水印编码;最后,由于 JPEG,MPEG 等压缩算法的核心是在 DCT 变换域进行数据量化,所以通过巧妙的融合水印过程和量化过程,就可以使水印抵御有损压缩,因而安全性比较强。但是隐藏的数据容量有限,较难实现大数据量隐藏。变换域数字水印技术稳健性较好,但隐藏容量较小。

2.3 基于融合的数字水印技术

图像融合主要有两种方式。一种是将两幅图像按照某种方式叠加生成一个新的图像,使新图像中包含两个图像的信息。采用较好的融合算法能保证恢复时无须原始公开图像。另一种是利用数字图像的自相关性,通过放大原始公开图像来隐藏 3 幅与公开图像同样大小的数字图像。此方法对于彩色图像的隐藏比较实用,尤其适用于 BMP 彩色图像的加密隐藏,而且对所要隐藏的图像进行置乱处理后,安全性更高。

2.4 量化噪声伪装

通常数字信号中的量化噪声很难被观察者发现,通过控制预测量化器的量化等级的选择来嵌入图像数据流,而嵌入其中的特定数据对于公开图像而言近似一种量化噪声,因而不容易被发现。

另外一些其他算法也是值得关注的:

(1) 分形水印。基于图像分形压缩的分形水印是由 Puate 和 Jordan 首先提出的[14]。实验表明,这种水印可以有效抵抗 JPEG 压缩,缺点是计算量大、速度慢,这主要是由分形压缩产生的。

(2)基于特征的水印算法。1999 年 Kutter[15]等人最先提出第二代水印的概念,建议水印的嵌入在感知有意义的特征区域中进行。对于图像来说,可能是边缘、拐角和纹理区域,或者是突出点所在的区域。这样,当只有部分图像时,仍能够通过这些特征点来定位并提取水印。

3 结束语

数字水印技术是一门多学科、多领域的新兴交叉学科,它涉及到密码学、通信理论、编码理论、信号压缩和视觉理论,以及信号处理和图像处理等相关理论[16]。在网络的信息技术及电子商务迅速发展的今天,水印技术的研究更具有重要意义。随着人们对数字水印技术的认识和研究的不断深入,它必定会在 Internet 网络图像、数字图书馆、医学应用等方面发挥它的巨大作用。

参考文献:

[1] 王丽娜. 信息隐藏技术与应用[M]. 武汉:武汉大学出版社,2004.

[2] Katzenbeisser S, Petitcolas P. Information Hiding Techniques for Steganography and Digital Watermarking[M]. London: Artech House,2000.

[3] 孙水发. 数字水印的应用及需求分析[J]. 信息技术,2007(9):8-11.

[4] Fridrich J, Du R, Meng L. Steganalysis of LSB Encoding in Color Images[C]//. Proc. IEEE Int'l Conf. Multimedia and Expo, CD-ROM. Piscataway, NJ:IEEE Press, 2000.

[5] Fridrich J, Goljan M, Du R. Detecting LSB Steganography in Color and Gray-scale Images[J]. Magazine of IEEE Multimedia Special Issue on Security,2001,9(4):22-28.

[6] Lee Y K,Chen L H. An Adaptive Image Steganographic Model Based on Minimum-error LSB Replacement[C]//Proceedings of the 9th National Conference on Information Security. Taiwan:[s.n.], 1999:8-15.

[7] Lin G S, Lie W N. Study on Detecting Image Hiding By Feature Analysis[C]//Proc. of IEEE International Symposium on Circuits and Systems, ISCAS-2001. Sydney, Australia: [s.n.],2001:149-152.

[8] Farid H. Detecting Hidden Messages Using Higher-order Statistical Models[C]//In: Proc.of the IEEE Int'l. Conf. on Image Processing 02[R]. New York: IEEE, 2002:905-908.

[9] Provos N, Honeyman P. Detecting Steganographic Content on the Internet[R]. Michigan: University of Michigan, 2001.

[10] 韩　枭,姜良华. 数字水印技术综述[J]. 科技广场,2007(7):105-107.

[11] 刘振华. 信息隐藏技术及其应用[M]. 北京:科学出版社,2002.

[12] Smith J R, Comiskey B O. Modulation and Information Hiding in Images[C]//workshop on information hiding. UK: Uni-

(下转第 182 页)

```
end if
}}
end;
```

在算法的实现中，不是先生成所有的候选项目集再确定频繁项目集，而是生成一个候选项目集后就计算其频繁度，减少内存占用，提高算法的效率。

3.3 结果描述

数据挖掘将获取的信息以便于用户理解和观察的方式反映给用户，这时可以利用可视化工具。对于DM系统的挖掘结果，可以用自然语言、图形、表格等多种方式进行表示。在本系统中采用自然语言的方式表示。规则 A=>B 解释的形式为：加强对课程 A 的学习，有助于课程 B 的学习。其中前件 A 和后件 B 均可以包含任意多个属性。并且系统向用户推荐一个课程先后学习的序列。

由频繁项集 L_4 输出的一些关联规则：

加强对《计算机数学基础》《电子技术》《计算机组成原理》的学习，有助于课程《计算机体系结构》的学习。

加强对《计算机数学基础》《电子技术》的学习，有助于课程《计算机组成原理》《计算机体系结构》的学习。

加强对《计算机数学基础》的学习，有助于课程《电子技术》《计算机组成原理》《计算机体系结构》的学习。

课程推荐序列：《计算机数学基础》=>《电子技术》=>《计算机组成原理》=>《计算机体系结构》可由系统给出几种挖掘所得的规则形式及推荐课程设置的序列，给用户提供参考，由决策者决定所采用的规则及序列，做出相应的决策，指导学员选课，以帮助学员更好地完成各门课程的学习。

4 结束语

该系统实现了一个完整的数据挖掘过程，用户只要提供必要的数据，系统就可以自动地对选定的数据库进行分析，并且返回用户需要的信息，帮助用户做出决策，从而帮助学员选课及进一步学习，起到了很好的促进作用，具有一定的实用价值。同时数据挖掘技术已经在许多领域取得好的应用，随着数据的不断增长，把数据挖掘技术应用到远程教育教学中，能够较客观实时地反映问题，这一研究也对远程教育教学管理提出了很好的建议。

参考文献：

[1] Agrawal R, Imielinski T, Swami A. Mining Association Rules between Sets of Items in Large Database[C]//In SIGMOD' 93. Washington, DC: [s. n.], 1993: 207 - 216.

[2] Han Jiawei, Kamber M. 数据挖掘概念与技术[M]. 范 明，孟小峰等译. 北京：机械工业出版社，2003: 150 - 221.

[3] 朱 明. 数据挖掘[M]. 合肥：中国科学技术大学出版社，2002: 129 - 140.

[4] 程涛远. 基于园区网络的数据仓库相关技术的研究[D]. 济南：济南大学，2002: 36 - 40.

[5] 贾彩燕，倪现君. 关联规则挖掘研究述评[J]. 计算机科学，2003, 30(4): 145 - 148.

(上接第 175 页)

versity of Cambridge, 1996.

[13] 林 榕. 基于图像的信息隐藏技术综述[J]. 装备制造技术，2007(7): 91 - 93.

[14] 罗建禄. 图像数字水印技术综述[J]. 重庆工商大学学报：自然科学版，2007, 24(1): 10 - 11.

[15] Kutter M, Bhattacharjee S K, Ebrahimi T. Towards second generation watermarking schemes[C]// in Proc. IEEE Int. Conf. Images Processing: vol. 1. Kobe, Japan: [s. n.], 1999: 320 - 323.

[16] Moulin P, O'Sullivan J A. Information - Theoretic Analysis of Information Hiding[J]. IEEE Transaction on Information Theory, 2003, 49(3): 563 - 593.

(上接第 178 页)

Using Key Graphs[J]. IEEE/ACM Transaction on Networking, 2000(8): 16 - 30.

[2] Moyer M, Rao J, Rohatgi P. A survery of security issues in multicast communicastions[J]. IEEE Network, 1999, 13: 12 - 23.

[3] Wallner D, Harder E, Agee R. Key management for multicast: Issues and architecture[S]. IETF RFC 2627, 1999.

[4] Kwak D W, Lee Seung Joo, Kim Jong Won, et al. An Efficient, LKH Tree, Balancing Algorithm for Group Key Management[J]. IEEE Communication, 2006, 10(3): 222 - 224.

[5] Son Ju - Hyung, Lee Jun - Sik, Seo Seung - Woo. Energy Efficient Group Key Management Scheme for Wireless Sensor Networks[M]//IEEE, Invited Paper. [s. l.]: [s. n.], 2007.

[6] 康巧燕，孟相如，王建峰，等. 基于逻辑层次树的动态组播密钥管理改进方案[J]. 计算机工程，2007(8): 123 - 125.

[7] 徐明伟，董晓虎，徐 恪. 组播密钥管理的研究进展[J]. 软件学报，2004, 15(1): 141 - 149.

[8] 周 杰，张金焕，王全迪，基于 RSA 的组播加密方法及其密钥管理方案[J]. 大连理工学报，2005, 45(10): 122 - 125.

[9] 李新国. 数字内容保护系统中的认证和密钥管理技术研究[D]. 西安：西安电子科技大学，2006.