苏庆堂 著

彩色图像
数字盲水印技术

清华大学出版社

彩色图像
数字盲水印技术

苏庆堂 著

清华大学出版社
北京

内 容 简 介

本书结合矩阵分解、整型小波变换和离散余弦变换等理论，从水印不可见性、鲁棒性、水印容量和算法实时性等角度出发，提出多种彩色图像盲水印算法，较好地解决了彩色数字图像的版权保护问题。

全书共分10章：第1章介绍彩色图像盲水印技术的研究背景、意义及国内外研究现状；第2章介绍数字水印常用的数学知识，为后续算法的研究奠定理论基础；第3章介绍彩色数字图像的基本知识，为研究彩色图像盲水印技术的研究打下专业知识基础；第4～9章分别介绍不同的盲提取水印算法，每一种算法包含详细的步骤过程和实验结果；第10章对彩色图像盲水印算法进行了总结和展望。同时，附录部分给出了数字水印常用名词的中英文对照表。

本书可供信息隐藏、信息安全、数字取证等领域的研究开发人员参考，也可作为高等学校计算机应用、信息安全、电子与通信等专业研究生与本科生的参考资料。

图书在版编目(CIP)数据

彩色图像数字盲水印技术/苏庆堂著. —北京：清华大学出版社，2015
ISBN 978-7-302-42162-7

Ⅰ. ①彩… Ⅱ. ①苏… Ⅲ. ①电子计算机－密码术 Ⅳ. ①TP309.7

中国版本图书馆CIP数据核字(2015)第269063号

责任编辑：白立军
封面设计：傅瑞学
责任校对：李建庄
责任印制：李红英

出版发行：清华大学出版社
网　　址：http://www.tup.com.cn，http://www.wqbook.com
地　　址：北京清华大学学研大厦A座　　**邮　　编**：100084
社 总 机：010-62770175　　**邮　　购**：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质量反馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
课件下载：http://www.tup.com.cn,010-62795954
印 装 者：三河市中晟雅豪印务有限公司
经　　销：全国新华书店
开　　本：185mm×230mm　　**印　　张**：13.75　　**字　　数**：275千字
版　　次：2015年11月第1版　　**印　　次**：2015年11月第1次印刷
印　　数：1～500
定　　价：39.00元

产品编号：066689-01

前　言

随着计算机技术和网络技术的快速发展，数字产品尤其是彩色数字图像得以在Internet上大量传播，但是因其自身易篡改、易复制的特点使得其版权保护越来越困难，盗版和侵权等问题也越来越严重，因此，无论是利用彩色数字图像作为宿主图像还是用之作为水印的彩色图像数字水印技术越来越受到人们的重视，成为图像水印技术的热点之一。

本书从分析现有相关算法的特点及其局限性入手，以实现彩色图像数字水印盲提取为目的，分别从水印容量、鲁棒性、不可见性、算法执行效率等不同角度，利用空域、变换域、矩阵分解等技术，对彩色图像数字水印算法进行比较深入地研究，取得了一些有意义的成果，主要研究内容如下。

(1) 从分析空域算法和变换域算法的优点出发，提出了一种新的在空域中实现基于DCT变换的彩色图像盲水印算法。根据DCT变换的原理，分析并利用其DC系数的形成过程，无须进行DCT变换，在空域中就可计算出每一8×8分块的DC系数，同时利用系数量化技术将二值水印重复嵌入4次获得含水印的彩色图像。盲提取水印后，根据“先选择后组合”及“少数服从多数”的原则决定所提取的二值水印。该算法既具有空域算法效率高的优点，又具有变换域算法鲁棒性强的优点。

(2) 针对彩色图像水印所含信息量大且难以嵌入的特点，提出一种新的基于整数小波变换和状态编码的双彩色图像水印算法。该算法既利用整数小波变换不存在舍入误差的特点，又利用了所提出的状态编码技术能以非二进制信息形式来表示水印像素信息的特点。通过改变分组数据状态码的方法来嵌入水印，在提取水印时可以直接利用分组数据的状态码来提取所嵌入水印信息。仿真结果表明，该算法能够保证大容量彩色水印信息的嵌入。

(3) 针对如何有效地提高彩色图像水印的不可见性问题，提出基于SVD的双彩色图

像数字水印算法。通过分析SVD的特点，提出新的矩阵优化补偿的方案。嵌入水印时，将4×4像素块进行SVD分解，并修改其U分量第二行第一列元素与第三行第一列元素来嵌入水印；然后，通过改进的优化方法来补偿含水印的像素块，进一步提高水印的不可见性。提取水印时，直接根据含水印图像的U分量中被修改元素的关系来提取所嵌入的水印。实验结果表明，该水印算法不但克服了SVD虚警检测的错误，而且具有较好的水印不可见性。

(4) 针对彩色图像水印鲁棒性较差的问题，提出了基于Schur分解的彩色图像盲水印算法。首先，研究了矩阵的Schur分解理论及图像矩阵块Schur分解后的特点；然后，通过修改系数之间的关系来嵌入水印。实验结果表明，该算法不但具有较好的不可见性而且具有较强的鲁棒性。

(5) 针对彩色图像水印算法执行时间长的问题，提出一种高效的基于QR分解的彩色图像盲水印算法。首先，对图像矩阵经QR分解后的嵌入水印的条件进行了分析讨论；然后，对每个选定的4×4像素块进行QR分解，通过对矩阵R的第一行第四列元素的量化来嵌入水印信息。提取水印过程中，不需要原始宿主图像和原始水印图像。仿真结果表明，该算法不但满足了水印性能的不可见性和鲁棒性要求，而且具有很高的执行效率。

(6) 研究设计基于盲提取的双彩色图像水印算法始终是一种挑战性的工作，本书分析了Hessenberg矩阵的特点，提出了一种基于Hessenberg分解的彩色图像水印算法。通过系数量化技术将加密的彩色图像水印信息嵌入Hessenberg矩阵的最大系数中，提取水印时不需要原始宿主图像或原始水印图像的参与。实验结果表明，所提出的水印算法在水印不可见性、鲁棒性和时间复杂度方面具有较好的水印性能。

本书的出版得到山东省自然科学基金项目(No. ZR2014FM005，No. ZR2013FL008)、山东省重点研发项目(No. 2015GSF116001)、山东省教育厅项目(No. J14N20)、鲁东大学博士基金(No. LY2014034)、山东省科技厅项目(No. 2014GGB01944)的资助，并得到鲁东大学信息与电气工程学院的大力支持和帮助，在此深表感谢！烟台风能电力学校的王环英老师参与了本书的编写工作，鲁东大学的王金柯、林恩伟等同学在文字录入、书稿校对方面付出了辛勤劳动，在此向他们深表谢意！

特别感谢清华大学出版社，感谢责任编辑及其他参与此书出版工作的各位老师为本书顺利出版而付出的辛勤劳动！

限于作者学识水平，书中难免存在不妥之处，请同行和读者批评指正。

作者邮件地址：sdytsqt@163.com。

苏庆堂

2015年7月定稿于烟台

目　录

第1章　绪论

信息作为一种重要的战略资源，其获取、加工、存储、传输和安全保障能力成为一个国家综合国力的重要组成部分，信息安全已成为影响国家安全、社会稳定和经济发展的决定因素之一。信息隐藏是一门新兴的信息安全学科，其技术是将秘密信息隐藏在不易被人怀疑的普通载体文件中，使秘密信息不易被别有用心者发现、窃取、修改或破坏，从而保证了信息在网络上传输的安全性。信息隐藏与数字水印作为信息安全领域最新的研究领域，在近几年得到了很大的发展。本章从分析多媒体信息安全出发，首先介绍信息隐藏技术的基本术语、分类与发展，然后介绍信息隐藏技术领域的一个重要分支——数字水印技术的产生背景、基本概念与框架、常用的攻击方法与评价标准，最后介绍彩色图像数字水印的研究现状。

1.1　信息隐藏技术简介

1.1.1　信息隐藏技术的基本术语

近年来，计算机网络技术和多媒体处理技术的迅速发展使得世界各地的人们交流更加方便、更加快捷。多媒体数据的数字化为多媒体信息的存取提供了极大便利，同时也极大地提高了信息表达的效率和准确性。随着 Internet 的快速发展与日益普及，多媒体信息的交流已达到了前所未有的深度与广度，其发布形式也愈加丰富。如今，人们可以通过 Internet 发布自己的作品、重要信息和进行网络贸易等，但是随之出现的问题也日益突出，如作品侵权更加容易、作品篡改也更加方便。因此，如何既充分利用 Internet 的便利，又能有效地保护知识产权，已受到人们的高度重视。在这种背景下，一门新兴的交叉学科——信息隐藏学正式诞生。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，正得到广泛研究与应用。

信息隐藏有时也称为数据隐藏，其基本过程如图 1.1 所示。通常，人们把希望被秘密隐藏的对象称为嵌入对象，它是含有特定用途的秘密信息或重要信息。用于隐藏嵌入对象的非保密载体称为载体对象。这里“对象”含义广泛，它可以是消息、文本、图像、音频、视频、软件、数据库等。信息嵌入过程的输出对象，即已经藏有嵌入对象的输出对象称为隐藏对象，或称为伪装对象，因为它与载体对象之间没有视觉感知或听觉感知上的差别。将嵌入对象添加到载体对象中得到隐藏对象的过程称为信息嵌入，嵌入过程中所使用的算法称为嵌入算法。信息嵌入的逆过程，即从隐藏对象中重新获得嵌入对象的过程称为信息提取，或称为信息恢复。在提取过程中所使用的算法称为提取算法。执行嵌入过程和提取过程的组织或个人分别被称为嵌入者和提取者。

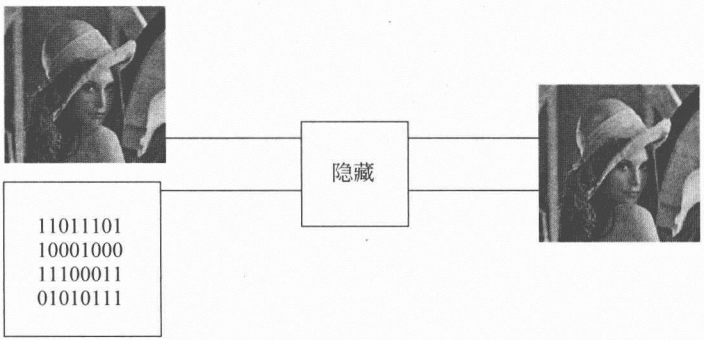

图 1.1　信息隐藏基本过程

在信息隐藏系统中，为了增加安全性，人们通常需要使用一些额外的秘密信息来控制嵌入与提取过程，只有它的持有者才能进行操作，这个秘密信息称为隐藏密钥。嵌入过程的隐藏密钥称为嵌入密钥，提取过程的隐藏密钥称为提取密钥。通常嵌入密钥和提取密钥是相同的，相应的信息隐藏技术称为对称信息隐藏技术，否则称为非对称信息隐藏技术。

可以把信息隐藏的研究分为信息隐秘书写技术和隐藏分析技术两部分。前者主要研究向载体对象中秘密添加嵌入对象的技术；后者主要研究如何从隐藏对象中破解出嵌入信息，或通过对隐藏对象的处理达到破坏嵌入信息或阻止信息检测目的的技术。类似地，可以称隐藏技术的实现方法或研究者称为隐藏者，而隐藏系统的攻击方法或隐藏分析技

术的研究者称为隐藏分析者或伪装分析者。注意，在信息隐藏的不同分支领域中，上述的相关术语可能不同。

1.1.2　信息隐藏技术的分类

1. 隐蔽通道

隐蔽通道可定义为系统中不受安全策略控制的、范围安全策略的信息泄露路径。按信息传递的方式区分，隐蔽通道分为隐蔽存储通道和隐蔽定时通道。如果一个进程直接或间接地写一个存储单元，另一个进程直接或间接地读该存储单元，则称这种通道为隐蔽存储通道。如果一个进程通过调节它对系统资源的使用，影响另一个进程观察到的真实响应时间，实现一个进程向另一个进程传递信息，则称这种通道为隐蔽定时通道。

2. 隐写术

信息隐藏中一个重要的子学科是隐写术(stegnaography)。不同于密码学中对信息内容的保护，隐写术着眼于隐藏信息的本身存在。它来自于希腊词根 steganos 和 graphie，字面的意义是“密写”，它通常被解释为把信息隐藏于其他信息当中，即不让计划的接收者之外的任何人知道信息的传递事件(而不只是信息的内容)。例如，通过在一份报纸上用隐形墨水标志特定的字母，达到给间谍发送消息的目的。现代的隐写术主要指在数字信息处理和计算机领域，利用计算机中普遍存在的冗余性向其中嵌入秘密数据。

3. 匿名技术

匿名技术是指不暴露身份和个人特征的一种技术，该技术主要应用于网络环境下。网络匿名可分为发送方匿名和接收方匿名，分别保护通信双方的身份，所使用的主要技术有匿名重发和网络代理等技术。

4. 版权标记

版权标记是向数字作品中嵌入可以鉴别的版权标记信息，该技术是进行数字作品版权保护的一种有效技术。根据标记内容和所用技术的不同，可以将版权标记技术分为数字水印技术和数字指纹技术。与钞票水印相类似，数字水印技术是将特制的标记，利用数字内嵌的方法嵌入数字图像、声音、视频等数字产品中，用以证明创作者对其作品的所有权，并作为鉴定、起诉非法侵权的证据，同时通过对水印的探测和分析，以保证数字信息的

完整可靠性，从而成为知识产权保护和数字多媒体的防伪的有效手段。数字指纹技术是为避免未经授权的复制和发行，出品人可以将不同用户的 ID 或序列号作为不同的指纹嵌入作品的合法副本。一旦发现未经授权的副本，可以从此副本中恢复指纹来确定它的来源[1]。

1.1.3 信息隐藏技术的发展

自从出现人类文化，人类就有保护信息的想法。密码术和隐写术这两个词正式出现在 17 世纪中叶，且都来源于希腊语。描述信息隐藏的最早文献是历史学家之父 Herodotus 于公元前 400 多年写的《历史》。这本书中介绍的一个例子是使用打蜡的木匾：波斯的 Demeratus 想要告知希腊的朋友 Xerxes，有人要来侵犯他们。在那个时候，书写用的木匾通常是用两片打上蜡的书片，连起来作为一本书。字是写在蜡上的，用蜡融化掉就可以重新使用。而 Demeratus 使用的方法是先将蜡去掉，把信息写在木片上，然后在木片上打上蜡。这样从外观上就看不出蜡里藏有信息了。起初这种方法很奏效，但后来就被人们识破了[2]。

“计算机网络是现代密码学之母，而 Internet 则是现代信息隐藏之母”。20 世纪 70 年代计算机网络的兴起掀起现代密码学研究的热潮，并使密码学发展成为一门相对成熟的学科。随着 20 世纪 90 年代 Internet 的迅速发展，多媒体技术的逐渐成熟和电子商务的兴起，网上多媒体信息急剧增加。如果没有网络，信息技术绝不会如此迅速发展，而网络的开放性与资源共享使得网络信息安全问题日益突出。这就需要有效的保护数字产品版权的手段与技术来解决这一现实问题，这种需要是数字水印技术研究的主要推动力。

在目前很多数字信息隐藏算法中都采用了扩频技术。扩频通信可看作是一种把信息隐藏在宽频伪随机噪声中的通信方式。扩频通信在军事中的应用已有半个多世纪的历史，近些年来被广泛用于民用通信。它使用比发送的信息数据速率高得多的伪随机编码，扩展作为基带信号的信息数据频谱，成为极低功率谱密度的宽带信号，从而在实际上难以和背景噪声相区别。此外，高频有利于嵌入信息的不可见性，但不利于鲁棒性，低频尽管有利于鲁棒性，但却会带来不可接受的可见性。扩频技术可通过将低频能量信号嵌入每一个频段来解决这种矛盾。

就目前而言，信息隐藏技术远未成熟，尚缺乏系统性的理论基础和公平统一的性能测试与评价体系，信息隐藏的广泛应用依赖于对其不断地探索与实践。

1.2　数字水印技术

1.2.1　数字水印技术的背景

随着计算机多媒体技术的迅猛发展，人们可以方便地利用数字设备制作、处理和存储文本、图像、语音和视频等媒体信息。与此同时，数字网络通信正在飞速发展，使得信息的发布和传输实现了“数字化”和“网络化”。在模拟时代，人们把磁带作为记录设备，盗版复制通常要比原始复制的质量低，即二次复制的质量更糟糕。在数字时代，歌曲或电影的数字复制过程完全不损失作品质量。自从 1993 年 11 月 Internet 上出现了 Mosaic 网页浏览器，Internet 对用户变得友好起来，很快人们便开始乐于从 Internet 上下载图片、音乐和视频。对数字媒体而言，Internet 成了最出色的分发系统，因为它不但便宜，而且不需要仓库存储，又能实时发送。因此，数字媒体很容易借助 Internet 或 CD-ROM 被复制、处理、传播和公开。这样就引发出数字信息传输的安全问题和数字产品的版权保护问题。如何在网络环境中实施有效的版权保护和信息安全手段，已经引起了国际学术界、企业界以及政府有关部门的广泛关注。其中，如何防止数字产品（如电子出版物、音频、视频、动画、图像产品等）被侵权、盗版和随意篡改，已经成为世界各国亟待解决的热门课题之一。

数字产品的实际发布机制是一个冗长的过程。它包括原始制作者、编辑、多媒体集成者、重销者和国家官方等。本书给出了一个简单的发布模型，如图 1.2 所示。图中的“信息发布者”是版权所有者、编辑和重销者的统称，他们试图通过网络发布数字产品 x。而图中的“用户”也可称为消费者（顾客），他们希望通过网络接收到数字产品。图中的“盗版者”是未授权的供应者，他们未经合法版权所有者的许可重新发送产品 x（如盗版者 A）或有意破坏原始产品（如盗版者 B）并重新发送其不可信的版本 x^*，从而消费者难免间接收到盗版的副本 x 或 x^*。

盗版者对数字多媒体产品的非法操作行为，通常包括以下三种情况。