新一代信息隐藏技术：鲁棒数字图像水印技术研究

邓铭辉 著

黑龙江人民出版社

新一代信息隐藏技术：
鲁棒数字图像水印技术研究

邓铭辉 著

黑龙江人民出版社

图书在版编目（CIP）数据
新一代信息隐藏技术：鲁棒数字图像水印技术研究/邓铭辉著.
—哈尔滨：黑龙江人民出版社，2010.5
ISBN 978-7-207-08656-3
Ⅰ.①新…. Ⅱ. ①邓…. 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（2010）第 082287 号

责任编辑：马少滨
特约编辑：甄静泊
装帧设计：李天语

新一代信息隐藏技术：鲁棒数字图像水印技术研究

Xinyidai xinxi yincangjishu lubangshuzituxiang shuiyinjishu yanjiu

邓铭辉 著

出版发行 黑龙江人民出版社
通讯地址 哈尔滨市南岗区宣庆小区 1 号楼
邮　　编 150008
网　　址 www.longpress.com
电子邮箱 hljrmcbs@yeah.net
印　　刷 哈尔滨市石桥印务有限公司
开　　本 787×1092 毫米 1/16
印　　张 13.625
字　　数 150 千字
版　　次 2010 年 5 月第 1 版　2010 年 5 月第 1 次印刷
书　　号 ISBN 978-7-207-08656-3 /TP・16
定　　价 26.00 元

（如发现本书有印制质量问题，印刷厂负责调换）
本社常年法律顾问：北京市大成律师事务所哈尔滨分所律师赵学利、赵景波

前　言

近年来，多媒体存储与传输技术的不断进步，尤其是 Internet 技术的盛行，带动了数字媒体应用的迅猛发展，各种形式的多媒体作品包括图像、视频、音频等得以网络的途径向外发布，这些技术给人们带来了极大的方便，但随之而来的副作用也十分明显，例如任何人都可以通过网络轻而易举地得到他人的原始作品，尤其是数字化的图像、音乐、电影等，甚至有些人不经作者的同意而对原作品任意加以复制、修改，严重地侵害了作者的著作权，因此如何在网络中实施有效的版权保护和解决信息安全的问题，也就成为了一个迫在眉睫的研究课题。

在这种情况下，一种专门解决互联网上多媒体信息安全的技术——数字水印技术诞生了，它将水印嵌入到数字化媒体中，然后通过对它的检测（提取）来对图像的使用情况进行跟踪，从而实现隐藏传输、存储、版权保护等功能。目前数字水印已经成为多媒体版权认证和完整性保护的有效手段。

本书以静止数字图像作为研究对象，根据图像处理理论和水印技术的自身特性出发，深入分析几何攻击对数字水印的鲁棒性影响以及对图像本身的影响，通过理论推导和实验证明寻找到适合于抗几何攻击的图像水印理论与技术，分别利用 3D 小波变换理论、时频分析理论、DCT 变换理论、单向 Hash 函数加密和 Haar 正交函数系理论对数字图像水印的抗几何攻击的鲁棒性进行了系统的重点研究，提出了一些新的理论思想和技术方案。从理论和实践上部分解决了数字水印所面临的几何攻击所导致的鲁棒性差和可检测性差问题，实现了抗几何攻击的鲁棒数字水印技术。主要研究内容如下：

1．对图像任意裁剪、旋转和缩放参数的估计算法的研究

针对几何变换(裁剪、旋转和缩放)对数据同步性的破坏提出几何参数估计算法，进行几何变换图像和原图像的配准，实现水印的可靠检测。利用边缘图像傅立叶变换的旋转不变性和差分相关技术准确估计裁剪图像的倾斜角度，通过二维相关函数计算相对位移，求得裁剪图像在原图像中的位置，从而将裁剪图像与原图像的配准。采用空域差分相关技术准确估计缩放图像的参数，实现与原图像的配准。

2．应用 DCT 变换和单向 Hash 函数加密理论的鲁棒水印技术研究

根据离散余弦变换理论和基本单向 Hash 函数加密提出了一种抗几何攻击的鲁棒数

字水印技术，利用单向 Hash 函数来决定数字水印的嵌入位置与嵌入强度，使水印的嵌入位是伪随机序列，对于未被授权的使用者，很难检测出水印的存在，只要图像的原始所有者保存一个相应的密钥，就能保证水印不被攻击者轻易破坏，算法采用了 8×8 离散余弦变换方法，并将水印嵌入到经仔细选择中频成分，很好的兼顾了数字水印不可见性与健壮性。本算法采用了 EIGFamal 水印加密方案，无疑这种算法是非常安全的。

3．基于 Haar 正交函数系的抗几何攻击鲁棒水印算法研究

通过深入研究桥函数理论，由理论分析和公式推导得到结论：实广义桥函数系包含实多值 Haar 函数系，Haar 函数系是一种完备的归一化正交函数系。由此提出基于 Haar 正交函数系的抗几何攻击的鲁棒水印算法，该算法根据 Haar 正交函数系的完备归一化正交性质，对图像进行分块 Haar 正交变换，根据图像视觉系统特性和 Haar 正交变换性质，提取重要的中频系数，并结合零水印嵌入技术，将水印自适应地嵌入 Haar 正交变换的中频矩阵，对几何攻击具有很强的抗攻击性，算法实现了良好的鲁棒性和有效性。

4．基于 3D 小波变换的鲁棒数字图像水印算法研究

根据离散小波变换理论和对视频序列进行 3D 小波变换的研究结果，提出了一种基于 3D 小波变换的数字水印算法，将原图像拆分为一个图像视频帧，将水印自适应地加入到每个图像帧二维小波变换的中频域的不同位置，利用图像二维小波变换中频域的特性和人类视觉系统特性，大大提高了水印算法的有效性，该水印算法对图像裁剪有非常强的的鲁棒性，在图像大部分被剪裁的极端情况下，仍能够非常清晰地检测出有效水印信号，通过大量的实验证实了该水印技术的可行性，这无疑是一种新的思想和解决方案。

5．应用时频分析理论，基于二维 Radon-Wigner 变换的鲁棒图像水印技术研究

根据时频分析理论基础，提出了一个在二维空间时-频分布域的抗几何攻击的图像鲁棒水印算法。利用线性频率变化来表示水印，通过二维 Radon-Wigner 变换来检测水印，二维线性调频信号作为水印，这种信号对各种静态滤波器都是不变的，而且还具有几何对称性。在二维 Radon-Wigner 变换域，作为水印的线性调频信号在遭受缩放、旋转和剪切等线性几何攻击的情况下，仅仅改变其在空间/时-频分布中位置，对于几何攻击是鲁棒的。对比其他的水印算法，该算法尤其对于几何破坏具有更好的鲁棒性，同时还具有优良的频率特性，将是一种非常新颖的、前景看好的数字水印技术。

本书由东北农业大学邓铭辉博士著，全书约 15 万字。

由于计算机技术的发展日新月异，新技术层出不穷，加之时间仓促，作者水平有限，错误和不当之处在所难免，敬请各位读者和专家批评指正。

此为试读，需要完整PDF请访问：www.ertongbook.com

目　录

第1章 绪 论

1.1 本书的背景、目的和意义

近年来，随着多媒体技术的不断进步和计算机网络的日益普及，数字媒体的应用取得了惊人的发展，多媒体信息的交流也达到了前所未有的深度和广度。人们可以通过Internet网发布自己的多媒体作品（包括音频、视频、动画、图像等）、传递重要信息、进行网络贸易等，但随之而来的副作用也十分明显。例如，任何人都可以通过网络轻而易举地得到他人的原始作品，尤其是数字化的图像、音乐、电影等。盗用者不但可以通过非法手段获取电子数据，而且可以未经作者的同意而对原作品任意加以复制、修改、生产和再传输等。这些不法行为严重地侵害了作者的著作权，给版权所有者带来巨大的经济损失，对信息安全造成强烈的冲击。总之，信息技术是一把双刃剑，一方面它为人们合法使用信息资源提供了极大的方便，另一方面它又助长了非法侵权、盗版和恶意篡改的盛行。因此如何既充分利用Internet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。如何在网络中实施有效的版权保护和解决信息安全也就成为了一个迫在眉睫的研究课题。

数字产品的网络发布、传输存在的安全性问题。“信息提供者”是数字作品的版权所有者，他们通过网络发布数字产品。“信息消费者”也可以称为顾客，他们希望通过网络接收到数字产品。“攻击者”是非法用户，未经授权的供应者和蓄意破坏者的统称。他们未经合法版权所有者的许可重新发送产品或有意破坏原始产品并重新发送其不可信的版本，从而使信息消费者难免间接收到盗版的副本。数字作品所受到的潜在攻击来自于两个方面：

（1）恶意篡改

修改数字产品的内容，使得合法用户接收到的数字产品不真实、不可靠，甚至失去原有的使用价值。

（2）侵犯版权

非法使用：未经版权所有者的允许非法复制或翻印数字产品。

非法转卖：未经版权所有者的允许将数字产品转卖。

破坏版权：将数字产品所携带的版权信息消除，使得该产品得不到正当的保护。

以前人们解决信息安全的问题是通过加密的手段来完成的，即首先将多媒体文件加密成密文以后发布，使得网络传输过程中的非法攻击者无法从密文获得机密信息，从而

达到信息安全的目的，但这并不能完全解决问题。一方面加密后的文件因其不可理解性而大大妨碍了多媒体信息的传播；另一方面文件经过解密后内容完全透明，所加密的文档就与普通文档一样将不再受到保护，也即没有了秘密而言，更无法幸免于侵权和盗版。因而，传统的加密方法已经受到了十分严峻的挑战。

在这种情况下，信息隐藏（information hiding）技术再次引起了人们的高度重视。所谓“信息隐藏”是将有用的或重要的信息隐藏于其他信息里面以掩饰其存在。事实上它从诞生起就一直受到人们的关注，而今天多媒体的版权保护和安全问题又给它注入了新的生机与活力，由其相应发展和演变而来的数字水印技术也就成为了当前国际学术界研究的一个前沿方向和热点。

在多媒体数据的网上交易和传输中，有两个关键的技术问题需要解决：一是多媒体数据的访问控制和安全传送；二是对多媒体内容的保护。访问控制需要解决用户的认证及管理、对多媒体产品数据库的访问控制以及数据的安全传送等问题，对于该问题传统的密码学方法可以胜任。第二个问题主要包括两部分：一是版权保护，二是内容完整性（真实性）保护，这时密码学的方法就无能为力了。因为密码学方法的思想是将多媒体文件加密成密文，然后进行发布，它主要是通过使非法攻击者无法从密文获得机密信息来达到信息安全的目的。因此采用加密的方法无法解决网络传输中版权保护的问题。因为一方面，如果将多媒体数据文件加密成密文后，实际上将其变成了不可理解的文件，大大地妨碍了多媒体信息的传播和交流；另一方面，加密的方式仅能在数据从发送者到接收者的传输过程中奏效，只能在信道中对数据进行加密保护，但是当信息被接收和被解密后，所加密的文档就与普通文档一样丧失了所有的保护。也就是说当数字作品一旦被用户接收继而被解密后就完全暴露于众，其对数字作品的保护作用也随即消失，无法防止数据的非法复制，更无法幸免于盗版。

数字水印，属于信息隐藏技术的一种，与钞票水印相类似，它是将具有确定性和保密性的信息（水印）直接嵌入到数字化媒体（静止图像、语音、文档、图书、视频等）中，使之作为原始数据的一部分而保留在其中，因而即使在解密之后仍可以对数据的复制和传输实施跟踪，从而实现隐藏传输、存储、标注、身份识别、版权保护等功能。可见，一方面它可以被用来证明原创作者对其作品的所有权作为鉴定、起诉非法侵权的证据；另一方面作者还可以通过对其数字产品中的水印进行探测和分析来实现对作品的动态跟踪，从而保证其作品的完整性。因而数字水印已经成为了知识产权保护和数字多媒体防伪的有效手段。

数字水印的基本手段是将产权、产品的标识码以及购买者的信息等（称为水印信号）嵌入到数字媒体中。嵌入的水印信号应当不降低原数据的质量，而且在感觉上不易被察

此为试读，需要完整PDF请访问：www.ertongbook.com

觉（即不可见水印，可见水印由于容易受到攻击，目前已不是研究的主流方向），并能够经受一定的攻击而不被清除，需要时可以通过检测（提取）嵌入的水印信息来鉴别数字媒体的版权、认证该数据的真伪或辨识该数据的原购买者、进行完整性鉴定等等。

从载体来看数字水印有图像数字水印、音频数字水印、视频数字水印等几种类型。其中图像数字水印是数字水印中比较重要的和常用的数字水印，它是以数字图像为载体，利用某种图像处理方法将水印嵌入到图像中，被嵌入的水印可以是一段文字、图标、序列号等。它又可以分为两大类：鲁棒水印和易损水印。鲁棒水印的特点是难以被去除，主要用于版权保护。易损水印的特点是可以随着原始图像的破坏而被破坏，主要用于图像完整性保护。本课题的主要研究对象是鲁棒图像数字水印。

作为一门新兴的多学科应用技术，数字水印涉及了不同领域的思想和理论，如信息论、信号处理、编码理论、密码学、图像处理、检测理论、多媒体技术、模式识别、计算机科学及网络等技术。数字水印技术的研究，对于其他众多科学的发展具有重要的推动作用。随着人们对数字水印技术的研究和对其作用认识的不断深入，数字水印技术必将在 Internet 网络图像和音视频、数字视频点播系统、卫星数字视频、数字图像和视频数据库、数字图书馆、医学图像、数码相机、数字知识产权保护、电子商务、数字新闻电视广播、DVD 版权保护、加密和安全通信、医学应用、文化遗产继承、现代文化艺术、军事命令的网络发布、军事机密的网络传输等领域得到广泛的应用。

总之，面对人类社会的数字化进程，在网络交流日益普及和电子商务逐渐启动的今天，多媒体数字水印技术的研究不但在防止侵权和打击盗版方面将发挥着重要的作用，而且对于规范世界各国数字化市场、促进人类信息产业健康持续的发展具有极为重要的意义。

1.2 国内外水印技术研究的动态

数字水印技术是近年来发展起来的一项重要的应用研究，其学术特点在于它横跨计算机科学、图像信息处理、多媒体技术、模式识别、密码学、数字通讯等众多学科和领域。作为数字化时代的一门新兴技术，它尚未形成一套独立完整的学科理论体系，但其重要的现实作用已经引起国内外众多知名学府、研究机构和公司的极大兴趣，成为了当前信息科学中的一个新颖且具有广阔应用前景的研究热点。

1.2.1 国外数字水印技术的研究动态

鉴于数字水印技术的应用前景和其在经济、技术上的重要性，全球支持或开展此项研究的政府机构和商业机构很多。主要有美国财政部、美国版权工作组、美国洛斯阿莫思国家实验室、美国海陆空军研究实验室、麻省理工学院、瑞士洛桑联邦工学院、Purdeu大学、英国的剑桥大学、德国的 Erlangen-Nuremberg 大学、NEC 研究所、IBM 研究所、微软公司、飞利浦、朗讯贝尔实验室等众多研究机构。其中美国的 Digimarc 公司于 1995 年就推出了有专利权的水印制作技术，是当时世界上唯一一家拥有这一技术的公司，并在 Photoshop 4.0 和 CoreDraw 7.0 中得到应用，但用其做出来的水印尚不够健壮。1997 年 1 月 7 日该公司又推出了独立的水印阅读软件 ReadMarc，利用它可以发现图像中是否含有水印及其内容。1998 年美国政府的报告中出现了第一份有关图像数据隐藏的 AD 报道。1999 年 2 月五大唱片公司联合宣布与 IBM 合作，联合开发一个在因特网上方便、快速、安全发布数字视听产品的实验系统。2001 年 1 月 Digimarc 公司又宣布与图形艺术的业界团体 PIA（Printing Industries of America）联手合作在打印机中使用 Digimarc 的“Media Bridge”电子水印技术。2001 年 7 月富士通公司开发出了“阶层型电子水印”为其在因特网上实现电子博物馆和电子美术馆系统“Musethque Light”提供安全保障。2007 年汤姆逊公司宣布，数字影院服务器的领导厂商选择汤姆逊功能完善的数字水印产品 NexGuard，并将其集成到 1200 部数字影院服务器中，影响降低到最低限度并且保持一定的位率。2007 年 Microsoft 提出了一种用于下载版软件的防盗版水印技术，购买者在下载时每个软件都会带上由购买者个人身份信息(例如购买者姓名、地址、信用卡号码等)生成的水印。数字水印中包含的信息使得软件的每一个实例都是唯一的，这样就能有效地防止盗版和非法复制。

IEEE 的 Transaction 及许多国际重要期刊都安排了数字水印的技术专刊，如《IEEE Transactions on Image Processing》、《IEEE Transactions on Consumer Electronics》、《Proceedings of IEEE》、《Signal Proceedings》、《IEEE Journal of Selected Areas on Communication》、《Communications of ACM》等相继出版了数字水印的专辑。 SPIE 和 IEEE 的一些重要的国际会议还开辟了相关的专题，如 1998 年的国际图像处理大会上就专门开辟了两个关于数字水印的专题讨论。此外国外水印技术专家和研究学者还积极进行学术交流与合作。国际的信息隐藏学术研讨会开始于 1996 年。1996 年 5 月第一届国际信息隐藏学术研讨会(International Information Hiding Workshop)在英国剑桥牛顿研究所召开，至今已经举行了九届。在这些会议上研究人员发表了许多有关数字水印方面的论文。国际光学工程学会（SPIE）从 1999 年起，每年召开一次多媒体信息安全与数字

水印大会，其会议的论文主要也都是关于数字水印技术方面的文章。这些会议的举行，大大增加了研究人员们彼此间的交流，促进了数字水印技术的不断发展。

1.2.2 国内数字水印技术的研究动态

随着国内 IT 产业的迅速崛起和互联网的迅猛发展，数字水印技术在我国数字领域中的地位和作用也日益上升，业内的许多有识之士纷纷加入到这方面研究的洪流中来，取得了许多高水平的研究成果。目前国内有许多高等学校和科研院所，如清华大学、北京大学、北京邮电大学、同济大学、北京信息学院、中科院自动化所、浙江大学、北方工业大学、大连理工大学、西安理工大学、国防科技大学等，都对这项技术进行了深入的研究。许多研究人员也都纷纷以各种不同的形式发表了自己的研究成果，对这项技术的研究提出了许多独到的见解，已经取得了许多可喜的成就。

此外，我国科研人员也十分注重学术交流，我国的信息隐藏学术研讨会（CIHW）是由我国信息科学领域的何德全、周仲义、蔡吉人三位院士与有关单位联合发起的。1999 年在北京电子技术应用研究所举行了第一次学术会议，参加会议的有何德全、周仲义、蔡吉人三位院士，还有来自全国许多高等院校和研究所的专家。参加研讨会的学者来自全国各地从事信息隐藏技术研究的二十四个高等院校或科研机构，至今全国信息隐藏学术研讨会已经举办了八届。国家“863 计划”、“973”项目等都对数字水印的研究有项目资金支持。2000 年 1 月由国家 863 计划智能计算机专家组织召开了“数字水印技术学术研讨会”，来自多家科研机构与高等院校的专家学者和研究人员参加这次会议，对数字水印技术的理论研究和实际应用具有深远的战略意义。随着中国加入世界贸易组织，有关知识产权的保护问题变得极为重要。国家对数字产品产权保护技术非常重视，在科技部编制的《2002 年度科技型中小企业技术创新基金若干重点项目指南》中明确指出了对于“数字产品产权保护(基于数字水印、信息隐藏、或者网络认证等先进技术)”、“数字产品内容防拷贝(基于条件读取、软件加密、或交互验证等先进技术)”和“个性化产品(证件)的防伪(基于水印、编码、或挑战应答等技术)”等多项防盗版与防伪技术予以重点支持。从目前的发展来看我国相关学术领域的研究与世界水平处在同一阶段，有独特的思路，而且部分已推出具有自主知识产权的产品。

1.3 数字图像水印的研究状况

数字水印技术是二十世纪九十年代伴随着信息技术、网络技术、多媒体技术的发展

而发展起来的，这其中对图像水印技术的研究起步最早，也是目前最成熟的一种数字水印技术。

1.3.1 易损水印的发展和现状

早期最简单的易损水印方案由 van Schyndel[1]等人提出，这是第一篇在主要会议上发表的关于数字水印的文章，阐明了关于水印的一些重要概念。此算法首先把一个密钥输入一个 m-序列发生器来产生水印信号，然后排列成二维水印信号，按像素点逐一把他们嵌入到像素位平面的最低位 LSB（Least Significant Bit）。由于水印信号被安排在最低位上，它是不可见的。这种方法极易受攻击，最简单的攻击方法是保留最低位平面的比特值，随意改变其他的比特值，整个图像完全改变，但是检测时仍然能够提取出水印。通过计算图像 Hash 值[2]也可以作为一种易损水印方法，它的主要缺点是只能作出图像是否篡改的结论，而不能给出篡改的报告，一个像素值的改变就能使图像得不到认证。一种改进的方法是行列 Hash 函数方法，对图像的每一行和每一列分别求 Hash 值，并将这些值保存起来以为今后的认证图像的 Hash 值进行比较。检测时对检测图像的行和列的 Hash 值如果检测到某行和某列的 Hash 值与保存的 Hash 值不同，则该行和列的交点被篡改，其缺点是极易误检。另一种改进的易损水印方法是分块式 Hash（block-based hash function）[3,4]的 BBHF 方法：计算图像像素块 $W_B \times H_B$ 的 Hash 值，其中 W_B 和 H_B 分别是图像块的宽度和高度，这些 Hash 值存储起来以作为今后的图像认证的参考值。如果认证图像的某块的 Hash 值与该块的参考 Hash 值不一致，说明该块被篡改。另一种易损水印方法是 VW2D(Variable-Watermark Two-Dimensional)，该方法也是分块式空域水印方法。其嵌入过程为 $Y(b)=X(b)+W(b)$，其中 $X(b)$为原始图像分块，$Y(b)$为水印图像分块，$W(b)$为水印分块。检测过程为：$\delta(b)=Y(b)W(b)-Z(b)W(b)$，其中 Z(b)为检测图像，如果 $\delta(b)$ 小于阈值 T，则表明 Z(b)通过认证，如果 Y(b)=X(b)，有 $\delta(b)=0$。由于这种方法抵抗几何图像处理操作，因而被称为半易损水印方法[4]。近年来出现了一种新的半易损水印方法[5-7]，这种方法是利用基于分块 DCT 的 JPEG 压缩的两个不变属性来生成并嵌入水印的，其方法主要是使图像的认证能够接受基于分块 DCT 变换的 JPEG 压缩，并拒绝其他操作，比如剪切。

目前的易损水印，还有后来提出并发展起来的半易损水印或多或少都存在一定的缺点：或者是嵌入方法简单，极易受到攻击；或者容易产生检测误差，从而使得检测结果不可靠；或者存在应用上的局限性，比如只能给出图像是否篡改，而不能给出篡改的程度，甚至不能对篡改定位。因而易损水印（半易损水印）仍然是一个值得进一步研究的

领域。

1.3.2 鲁棒水印的发展和现状

鲁棒水印和易损水印技术是同步发展的，其算法实现也可分为两类：一类是基于空域的方法，如 van Schyndel 等提出的 LSB 法，N.nikolaidis[8]等人在此基础上作了改进，应用互相关函数改进检测过程，从而大大改进了鲁棒性。二类是基于变换域的方法，主要的变换方法有离散余弦变换（DCT）、离散傅立叶变换（DFT）、离散小波变换（DWT）等，而以 DCT 变换最为流行。1997 年，I.J.Cox[9]在 DCT 域将扩频通信的思想应用到数字水印系统中引起巨大的反响，被认为是数字水印技术飞跃性的发展，大大提高了数字水印系统鲁棒性。针对静态图像压缩标准 JPEG[10]，在离散弦变换基础上嵌入数字水印的研究成为热点，Barni、Piva[11,12]、Huang 等[13]、HSU 等[14-16]、Tang 等[17]做了很多有意义的工作。针对目前流行的视频压缩标准 MPEG[18]、H.263[19]，Dittmann 等[20]提出了两种适用于空域的算法；Xia 等[21]、Zeng 等[22,23]做了基于离散小波的数字水印技术研究；Pitas 等在统计学的基础上，提出了一种新颖的算法[24-26]；Wolgang 等[27, 28]提出了可以有效抵抗线性和非线性滤波及 JPEG 有损压缩的数字水印嵌入算法；Kankanhalli 等研究了基于内容的数字水印技术[29]，这与计算机视觉的发展是密不可分的。在计算机图形学研究领域，1999 年的 SIGGRAPH 大会上，Praun 等提出了造型的三维网格上嵌入数字水印的方法[30], Ohbuchi 也做了类似的工作[31]；Maes 提出了基于几何变形的方法[32]；Paute 等[33]从分形压缩的角度提出了水印嵌入方法。此外，Petitcolas 等[34,35]、Barnett 等[36]、Scott 等[37]从另一个角度提出了一些对数字水印进行攻击的方法，有助于鲁棒性要求很高的数字水印技术的研究。国内也在这方面做了许多研究[38-46]。

以上提出的水印算法主要是从基本算法上来提高水印鲁棒性的。水印的鲁棒性总是与水印媒体的质量有关的，对于一个给定的算法水印鲁棒性越好，一般来说其水印媒体的质量越差。为了充分利用人类的生理特性，使得在提高水印鲁棒性的同时尽量保证水印媒体的质量，一些基于人类生理特性的水印方法被提出[47-50]。它的特点是根据人类的生理特性，比如图像水印的人眼视觉特性，考虑到人眼对不同频域的不同反应，给该频域位置加上不同的加权系数，使得在提高鲁棒性的同进保证了图像的视觉效果。

随着对水印系统攻击研究，虽然许多水印系统能够抵抗许多基本处理，如压缩、添加噪声、滤波、A/D 和 D/A 转换等，但是它们在几何变形攻击下却不能幸免。几何攻击是指水印图像经历诸如旋转、缩放、裁剪和平移等几何操作。几何攻击是最为严厉和最难解决的水印攻击方法，如水印系统测试的工具软件 unZign 和 StirMark 等,它们能成

功地攻击各种水印系统，对攻击后的系统经常不能正确的提取水印。如何恢复在几何变形下的水印，针对各种情况，出现了许多嵌入算法。Ruanaidh 提出了两个 DFT 域的水印算法[51]。他把水印嵌入图像 DFT 系数的相位信息中，其算法的依据是 RHayes 的结论:从图像的可理解角度，相位信息比振幅信息更重要，从而实现了水印的平移、旋转和尺度拉伸不变性。Hordan[52]利用 DFT 的性质嵌入了一个发散谱水印在一个图像中，对水印的平移、旋转和尺度拉伸具有鲁棒性。Barni[53]通过对 DFT 振幅信息修改,预先利用电子地图文字的大小和方向对图像几何形状进行标准化，然后嵌入水印,利用规范化的图像几何形状提取水印。同时 Caldeli[54]利用几何不变性理论在 DFT 域中采用一个同步模板检测水印。Lin[55]利用 Fourier 变换,讨论了水印抗平移、旋转和尺度拉伸的情况。Ni[56]在 Fractal 变换中实现了抗几何攻击的水印技术。Choi[57]在空间域上利用正弦曲线波在垂直方向来检测水印并对几何变换进行补偿。Agung[58]在 DCT 变换域中利用原始图像来识别被攻击后的水印，其结果表明对几何变换具有鲁棒性。Hel[59]利用几何 Hashing 技术在 DCT 变换域嵌入水印，对几何变换具有鲁棒性。Maes[60]利用预先确定密度像素模式(特征点)嵌入和提取水印，对几何变换具有鲁棒性，其缺点是不能抗有损压缩。与此相似，Ozer[61]利用一部分图像特征点恢复水印。Johnson[62]提出了一种抗水印几何变形的多项式变换技术。Ingemar[63]使用参考水印和错误纠错码技术讨论了水印多次嵌入方法。比较有影响的是 Kutter[64]所提出的具有一般几何不变性的数字水印算法，把一个 32 位的数字签名嵌入到彩色的图像中，此算法对一般的几何变换如移位、剪切、旋转、缩放等，鲁棒性较好。目前如何设计具有全面鲁棒性的数字水印系统依然是水印研究的关键问题之一。

1.3.3 空域水印技术的研究状况

数字水印的概念是 Caronni[65]于 1993 年提出来的，并应用于数字图像，此后研究人员将数字水印的概念逐步扩展到视频和音频等领域。

1994 年，van Schyndel[66]等在 ICIP’94 上发表了题为“A digital watermark”的文章，他是第一篇在重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和鲁棒水印检测的通用方法——相关性检测。他提出了 LSB 法（Last Significant Bit），该方法首先把一个密钥输入一个 m 序列（Maximum－length random sequence）发生器来产生水印信号，然后此 m 序列被重新排列成二维水印信号，按像素点逐一插入到原始图像像素值的最低位，以保证水印的不可见性，对这种水印的检测是通过计算一个互相关函数来进行的。该算法的优点是简单易行，有较大的信息隐藏量。但该算法实

此为试读,需要完整PDF请访问: www.ertongbook.com