摘　要

近年来，随着数字网络通讯的飞速发展以及数字多媒体的广泛应用，对数字产品版权保护的需求也日益迫切。数字水印技术就是在这样一个背景下作为一种多媒体数据的版权保护和内容认证的新技术，得到了广泛的研究和应用。数字水印技术通过在原始数据中嵌入特定的秘密信息——数字水印来证实数据的完整性或创作者对该数据的所有权，以此来抵制非法人员对数字作品进行盗版或恶意篡改等。数字图像水印算法是目前数字水印技术研究的一个重要方面，具有极大的理论研究价值和应用前景，是目前学术研究的一个热点。数字图像水印算法种类繁多，本文主要研究的是变换域的数字图像盲水印算法。

本文首先简要的介绍了数字水印的研究背景、发展现状及其主要应用领域，给出了数字水印技术的概念与分类、基本框架、技术特征、常见攻击方式及性能评估方案；其次，简单介绍了几种常用的数字水印预处理的图像置乱方法，并通过实验给予验证；接下来给出了两种变换域的数字图像盲水印算法：一种是基于混沌置乱的 DCT 域灰度级数字图像盲水印算法，另一种是基于超混沌和人类视觉系统的小波域数字图像盲水印算法，并通过实验验证了算法的有效性。同时，为了提高水印的保密性和提取出的水印的视觉效果，算法还利用了混沌、超混沌对原始水印信号进行了置乱处理。此外，为了在加强保密性的同时兼顾水印的不可觉察性和鲁棒性，在基于小波域的数字水印

算法中还充分考虑了人类视觉系统的特性，做到了自适应的选择水印的嵌入位置。最后，对全文的工作进行了全面的总结，并对下一步的研究工作提出了自己的看法。

关键词：数字水印；离散余弦变换；离散小波变换；图像置乱；盲提取；人类视觉系统

ABSTRACT

With the rapid growth of internet technologies and extensive use of multimedia data, the enforcement of multimedia copyright protection becomes an important issue. In the situation, digital watermarking is widely studied and used as a new technology for copyright protection and content authentication in recent years. It embeds some secret messages into the multimedia to protect the property or integrality so that digital produces can resist being copied, tampered and so on. Digital image watermarking algorithm is a important part of the investigation hotpots in the digital watermarking technology. Among the various classifications of watermarking, transform domain image watermarking technology is mainly studied in this paper.

First, a recapitulative introduction is made in this paper, which includes the basic theoretic knowledge of digital watermarking technology such as background, development situation, main application field, concept, sort, basic principle, characteristics, common attacking methods, assessment programme and so on. Second, several common algorithms about image watermarking encrypting is introduced and been proved through the experiment. Then two kinds of digital watermarking algorithm are proposed. One is a gray-scale blind watermarking algorithm

in DCT domain based on chaos permutation, the other is a blind watermarking algorithm in DWT domain based on hyper chaos and human visual system. To improve the security and visual effect, chaos and hyper chaos is used to scramble the watermarking signal. In the same time, to improve the invisibility and robustness, human visual system is used to select the appropriate position to embed the watermarking signal adaptively. Finally, conclusions about this paper are made and several opinions about the further research is proposed.

Key words: Digital watermarking, DCT, DWT, Image permutation, Blind extracting, HVS

湖南师范大学学位论文原创性声明

本人郑重声明：所呈交的学位论文，是本人在导师的指导下，独立进行研究工作所取得的成果。除文中已经注明引用的内容外，本论文不含任何其他个人或集体已经发表或撰写过的作品成果。对本文的研究做出重要贡献的个人和集体，均已在文中以明确方式标明。本人完全意识到本声明的法律结果由本人承担。

学位论文作者签名：赵永　　2008年 6月 3日

湖南师范大学学位论文版权使用授权书

本学位论文作者完全了解学校有关保留、使用学位论文的规定，研究生在校攻读学位期间论文工作的知识产权单位属湖南师范大学。同意学校保留并向国家有关部门或机构送交论文的复印件和电子版，允许论文被查阅和借阅。本人授权湖南师范大学可以将本学位论文的全部或部分内容编入有关数据库进行检索，可以采用影印、缩印或扫描等复制手段保存和汇编本学位论文。

本学位论文属于

1、保密□，在------年解密后适用本授权书。

2、不保密☑。

（请在以上相应方框内打“✓”）

作者签名：赵永　　日期：2008年 6月 3日

导师签名：[illegible]　　日期：2008年 6月 3日

第 1 章 绪论

1.1 数字水印的研究背景

随着数字技术和因特网的发展，各种形式的多媒体数字作品如图像、文本、视频、音频等纷纷以网络形式发表，这从很大程度上改变了人们的生活面貌，促进了社会的发展，并为多媒体信息的存储和传播提供了极大的便利。与传统的模拟作品相比，数字作品具有很大的优越性：人们可以方便地利用数字设备制作、处理和存储各种形式的多媒体数字作品。然而数字作品的便利性和不安全性是同时存在的，它可以低成本、高速度地被复制和传播，而且某些数字作品如歌曲、电影等的拷贝过程完全不损失作品的质量。数字媒体很容易借助 Internet 或 CD-ROM 被复制、处理、传播和公开。数字作品面临着易被非法侵权盗版和恶意篡改的严峻挑战，这必将严重阻碍信息产业的健康发展，在数字产品领域里迫切需要新的技术出现，以保证数字产品的知识版权问题。因此，如何既充分利用互联网的便利，又能实施有效的版权保护和信息安全手段，就成为一个迫在眉睫的现实问题，并引起了国际学术界、企业界以及政府部门的广泛关注[1-4]。其中，如何防止数字产品被侵权、盗版和随意篡改，已经成为世界各国待解决的热门话题[5]。

最初，人们首先想到的是采用密码技术来解决这一问题。密码技术是信息安全技术领域的主要传统技术之一，现有的数字内容的保护

多采用加密的方法来完成，即首先将多媒体数据文件进行的特殊的编码，形成旁人不可识别的密文后再发布，使得其在传递的过程中出现的非法攻击者无法从密文中获取机密信息，从而达到版权保护和信息安全的目的。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妨碍多媒体信息的传播；另一方面多媒体信息经过加密后容易引起攻击者的好奇和注意，随着电脑软硬件技术的迅速发展以及基于网络的具有并行计算能力的破解技术的日渐成熟，加密信息有被破解的可能性，而且当信息被接收并进行解密后，所有加密的信息就完全失去了保护，无法得到版权认证。另外，即使加密信息破解失败，非法攻击者仍然可能直接将密文破坏，使得即使是合法的接收者也无法获取有用的信息。换言之，密码学只能保护传输中的内容，而内容一旦解密就不再有保护作用了。因此，一种替代技术或是对密码学进行补充的技术就显得十分必要，它应该，甚至在内容被解密后也能够继续保护内容。

数字水印技术(Digital Watermarking)就是在这种应用要求下迅速发展起来的。数字水印是一种有效的数字产品版权保护和数据安全维护技术，是信息隐藏技术研究领域的一个重要分支。数字水印技术利用人类本身的视觉系统特性(HVS)或听觉系统特性(HAS)以及数字多媒体作品具有很大的冗余性的特点，在不引起人感知的情况下采用数字嵌入的方法将水印信息嵌入到多媒体载体中，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，同时无需占用额外带宽。水印的透明性保证了人们从表面上无法判断水印的存在或水

印嵌入的具体位置，只有通过专门的检测器才能从掩蔽载体中恢复或检测到数字水印信息，而水印的鲁棒性使得水印能抵抗各种常见的处理操作，具有较好的抗攻击能力，因而能起到版权认证的作用。

1.2 数字水印的发展历史及现状

数字水印的提出最早是在 20 世纪 90 年代，但是,通过向艺术作品中嵌入标识码以证明所有权的技术思想却可以追溯到 1954 年。1954 年，美国 Muzac 公司的埃米利•希姆布鲁克申请的一项关于将标识码透明地嵌入到音乐作品中以证明其所有权的专利(“Identification of sound and like signals”)[6]。这是迄今为止所知道的最早的的电子水印(Electronic watermarking)技术。然而，数字水印技术真正受到实质性的关注还是在 20 世纪 90 年代以后。早期的数字水印技术都是针对数字图像进行研究的，关于该技术的论述首见于 Tirkel 等人在 1993 年撰写的“Electronic water mark”一文[7]。该文首次使用了“water mark”这一术语，这标志着数字水印技术作为一门正式研究学科的诞生。后来二词合二为一就成为“watermark”，而现在一般都使用“digital watermarking”一词来表示“数字水印”。现在我们所说的“水印”一般都是指“数字水印”。在其随后发表的一篇题为“A Digital Watermark”[8]的文章中，针对灰度图像提出了两种向图像最低有效位（LSB，Least Significant Bit）中添加水印的方案，折中最低有效位的方法简单易行，但水印稳健性差，即使是常见的处理操作后，水印也无法正确提取。为了提高水印的稳健性，1995 年 Cox 等人[9]提出了一种基于扩频通信的水印算法，将水印嵌入到图像感知

上最重要的频域因子中，算法的鲁棒性得到了很大的提高，Cox 的方案已经成为数字水印中一个比较经典的方案，但其水印的提取必须要有原始图像的参与，即它不是盲水印方案。1996 年，Pitas 等人提出了另一种空域中的数字水印方案[10]，由于该方案提取水印时不需要原始作品的参与，因此成为了盲水印方案的典型。

1996 年 5 月，第一届信息隐藏国际学术研讨会在英国剑桥牛顿研究所召开，大大推动了数字水印的研究，许多大学、科研机构和公司企业纷纷开展了这方面的研究，越来越多的数字水印方案不断被提出，同时对数字水印的攻击方法也不断被发现。此后第二届、第三届信息隐藏国际研讨会又分别与 1998 年，1999 年在波兰和德国召开，其他一些重要国际会议如 IEEE 和 SPIE 等也都有了关于信息隐藏和数字水印技术的专题。我国也先后于 1999 年和 2000 年召开了我国第一届信息安全隐藏学术研究会(CIHW)以及第一届数字水印技术研讨会。CIHW 研讨活动至今已成功举行了五届全国会议。同时，国家多项科研发展计划以及自然科学基金都为数字水印的研究项目提供资金支持。国家 863 计划智能计算机专家组会同中科院自动化模式识别国家重点实验室和北京邮电大学信息安全实验室还召开了专门的“数字水印学术研讨会”[11,12]。

20 世纪 90 年代末期一些公司开始正式地销售水印产品。在图像水印方面，美国的 Digimarc 公司率先推出了第一个上用数字水印软件，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 LavelIt 软件可以

将若干字符隐藏到任何扫描的图片中，这些字符标记可以作为原始文件出处的证明，也就是说，任何用于 Word 文档、出版物、电子邮件或者网页的电子图片都可以借助于隐藏标记知道它的原始出处。AlpVision 公司同时还推出了专为打印文档设计的安全产品：SafePaper，它将水印信息隐藏到纸的背面，以此来证明该文档的真伪，它可以作为文件（如医疗处方、法律文书、契约等）是否为指定的公司或组织所打印的证明，同时，还可以将一些重要或秘密的信息，如商标、专利、名字、金额等隐藏到数字水印中。欧洲电子产业界和有关大学协作开发了采用数字水印技术来监视复制音像软件的监视系统，以防止数字广播业者的不正当复制的行为。现在，国内也已经出现了一些生产水印产品的公司，其中比较有代表性的是由中科院自动化研究所的刘瑞祯、谭铁牛等人于 2002 年在上海创办的一家专门从事数字水印、多媒体信息和网络安全、防伪技术等软、硬件开发的公司——上海阿须数码技术有限公司，该公司从事数字证件、数字印章、PDF 文本、分块离散图像、视频、网络安全等多方面数字水印技术的研究，现在这家公司已经申请了一项国家和三项国家数字水印技术专利。虽然数字水印在国内的应用还处于初级阶段，但水印公司的创办使得数字水印技术在国内不仅仅停留在理论研究的层面上，而是从此走向了实用化和商业化的道路，这必将推动国内水印技术的蓬勃发展，为国内的信息安全产业提供有效的、安全的保障。

1.3 数字水印技术的应用

数字水印技术从正式提出到现在虽然只有十几年，但由于其广阔

的应用前景及其在经济、技术等方面研究的重要性，得到了国内外学术界、政府和信息产业部门的高度重视。而数字水印相关的产品虽然是近几年才出现，但其应用前景和应用领域却是巨大的，总的来说，防止拷贝和数字作品的版权保护是推动数字水印发展的主要驱动力量，而且随着研究的深入，数字水印技术已开始广泛地渗透到信息安全的各个领域，有着广阔的应用前景。目前数字水印主要的应用领域有[13]：

(1) 广播监控 为了实现广播监控，可以使用数字水印技术对识别信息进行编码，通过识别嵌入到作品中的水印信息来鉴别作品是何时何地被广播的。它利用自身嵌入在内容之中的特点，无须利用广播信号的某些特殊片断，因而能够完全兼容于所安装的模拟或数字的广播基础设备。

(2) 所有者识别 文本版权声明用于作品所有者识别具有一定的局限，一方面在拷贝时这些声明很容易被去除，另一方面它可能占据一部分图像空间。由于水印既不可见，也与嵌入的作品不可分离，因此比文本声明更利于使用在所有者识别中。它通过嵌入代表作品版权所有者身份的水印来达到识别目的，如果作品的用户拥有水印检测器，他们就能够识别出含水印作品的所有者，即使遭到改动，水印也依然能够被检测到。

(3) 所有权验证 在发生所有权纠纷时，可以使用数字水印来提供证据，以保护数字作品的版权，而且为了使所有权验证达到一定的安全级别，可以限制检测器的发放。如果对手没有检测器，清除水印是相

当困难的。

(4) 交易跟踪 利用水印来记录作品的某个拷贝所经历的一个或多个交易。作品的所有者或创作者可在不同的拷贝中加入不同的水印，如果作品被滥用，所有者可以用水印来鉴别并找出那个合法获得内容但非法重新发生内容的人。

(5) 内容真伪鉴别 如今以难以察觉的方式对数字作品进行篡改已经变得越来越容易，可以使用水印技术将签名信息嵌入到作品中，这种被嵌入的签名称作真伪鉴别印记，如果对作品进行微小的改动就会造成真伪鉴别印记的失效。这类水印通常必须是脆弱的，且可以实现水印的盲检测。

(6) 拷贝控制 上述的绝大多数水印都只能在不合法行为发生之后起作用，为了防止受保护的内容进行非法拷贝，可以将水印嵌入内容之中并与内容同时播放，当具有拷贝控制机制的设备通过自带的水印检测器检测到“禁止拷贝”的水印标志时，将禁止播放或拷贝。

(7) 设备控制 设备控制是指设备能够在检测到内容中的水印时作出反应。例如，Digimarc 的“媒体桥”系统可将水印嵌入到经印刷、发售的图像中，如果这幅图像被数字摄影机重新拍照，那么 PC 机上的“媒体桥”软件和识别器便会设法打开一个指向相关网站的链接。

1.4 本文内容安排

本文主要研究的是变换域内的数字图像水印算法，其中重点研究 DCT 及 DWT 域两种。论文的主要工作和章节安排如下：

第一章 简要介绍了数字水印技术的研究背景、发展及研究现状，

概述了数字水印技术的应用，给出了本文的主要研究内容及章节安排。

第二章 详细阐述了数字水印技术的概念与分类、基本框架、技术特征、常见攻击方式以及数字水印系统的性能评估方案。

第三章 介绍了一些常用的水印图像预处理的置乱方法，包括基于混沌的图像置乱，经典的 Arnold 猫脸变换以及基于幻方变换的图像置乱方法等。

第四章 分析了二维离散余弦变换的物理意义，给出变换公式。简要介绍了灰度图像的位分解。结合混沌映射，提出了一种基于混沌置乱的 DCT 域灰度级盲水印算法，并给出仿真实验结果。

第五章 简要介绍了小波理论基础及人类视觉系统的基本特性，结合超混沌置乱的方法，提出了一种基于超混沌和人类视觉系统的小波域盲水印算法，并给出了仿真实验结果，验证了算法的有效性。

第六章 对全文进行总结，并对下一步的研究工作进行展望。

第 2 章 数字水印技术

2.1 数字水印技术概念与分类

2.1.1 数字水印概念

数字水印技术(digital watermarking)是一种信息隐藏技术，它的基本思想是在数字图像、音频、视频和文档等数字作品中嵌入秘密信息，以便保护数字产品的版权、证明产品的真实可靠性、跟踪盗版行为或者提供产品的附加信息[14-17]。其中的秘密信息可以是版权标志、用户序列号或者是其他产品相关的信息。含有水印的数字产品在经历信道传输后，可以通过对水印的检测与分析来保证数字信息的完整可靠性，或证明作者对其作品的所有权、授权单位或个人的使用权，并作为鉴定、起诉非法侵权的证据，从而成为知识产权保护和数字多媒体防伪的有效手段。

2.1.2 数字水印的分类

数字水印的分类方式有很多种，分类的出发点不同导致了分类的不同。最常见的分类方法有以下几种[18,19]：

(1) 有意义水印和无意义水印

按水印信号的意义划分，可分为无意义水印和有意义水印。无意义水印指嵌入的水印信号没有实际的含义，可以为伪随机实数序列、伪随机二值序列和混沌序列等。有意义水印是指嵌入的水印信号具有一定的意义，能比较直观的表示数字作品的信息，可以为数字图像或

数字音频和文字等。对于有意义水印，如果由于受到攻击或其他原因致使提取的水印破损，人们仍然可以通过观察确认数字作品中是否存在水印。而对于无意义水印，如果解码后的水印序列有若干码元错误，则只能通过统计决策来确定信号中是否含有水印。目前有意义水印在实际应用中更加广泛，它能更有效的保护数字作品的版权。

(2) 可见水印和不可见水印

从人类视觉系统来看，按照数字水印在数字作品中是否可见可以分为可见水印(Visible watermark)和不可见水印(Invisible watermark)。可见水印是指水印在数字作品中是可以看见的。不可见水印将水印嵌入到图像、音频或视频中，从表面上是不可察觉的，但是当发生版权纠纷时，所有者可以从中提取出标记来证明数字作品的版权，它是目前应用更为广泛的水印。

(3) 鲁棒水印和脆弱水印

从水印对抗各种攻击的稳健程度可以划分为鲁棒水印(Robust watermark)和脆弱水印(Fragile watermark)。鲁棒水印主要应用于数字产品的版权保护，它不仅要具有较强的抵抗常见图像处理的能力，而且还要能抵抗一定失真内的恶意攻击。脆弱水印主要应用于多媒体数据的完整性认证，当嵌入水印的载体数据被修改后，通过水印检测，可以对载体是否进行了修改或进行了何种修改进行判定，此类水印的鲁棒性要求应该是最低的。

(4) 依水印所依附的载体形式划分

按水印所附载的媒体可以划分为图像水印、音频水印、视频水印、

文本水印以及用于三维网格模型的网格水印等等。随着数字技术的不断发展，将会有更多不同类型的数字媒体出现，同时将会产生更多与之相对应的载体的数字水印技术。以图像为载体的数字水印技术是当前水印技术研究的重点之一，它的一些研究成果可以运用到音频水印和视频水印中。

(5) 空域水印和变换域水印

按水印嵌入的位置可以划分为空域水印和变换域水印。空域水印是通过直接修改数字图像的像素值或强度值来嵌入水印信息，即直接在信号空间上叠加水印信息。变换域水印是指先对宿主图像进行某种变换(如 DFT、DCT、DWT 等)，然后通过修改变换域系数来隐藏水印信息。变换域算法可嵌入水印数据量大、透明性好、安全性高，但算法复杂度也高。目前，大多数水印算法都是将水印嵌入到变换域，而本文研究的也正是变换域内的数字图像水印技术。变换域方法有两个优点：第一，在变换域中嵌入的水印信息能量可以分布到空域的所有像素上，从而有利于保证水印的不可见性；第二，在变换域，人类视觉系统的一些掩蔽特性可以方便的结合到水印编码过程中。

(6) 非盲水印、半盲水印和盲水印

按水印水印提取时是否需要原始数据可以划分为非盲水印(Nonblind watermarking)、半盲水印（Seminonblind watermarking）和盲水印(Blind watermarking)。非盲水印水印是指在水印检测过程中需要原始数据和原始水印的参与；半盲水印指不需要原始数据，但需要原始水印来进行检测；盲水印是指在水印检测过程中既不需要原始图

像也不需要原始水印。鉴于盲水印方案更适合公开的网络发布机制，具有更强的实用性，因此目前学术界研究的大多数是盲水印方案。

上述几种数字水印的分类并不是孤立的，它们之间相互联系，仅仅是在表现形式上有差异而已。

2.2 数字水印系统的基本框架

从信号处理的角度来看，水印嵌入载体中可以视为在强背景下叠加一个弱信号，只要叠加的水印信号强度低于人类视觉系统(HVS) 对比度门限或听觉系统（HAS）对声音的感知门限，那么人就无法感知到信号的存在。由于 HVS 和 HAS 受空间、时间和频率特性的限制，因此通过对载体对象做一定的调整，就有可能在不引起人感知的情况下嵌入一些信息。

从数字通信的角度来看，水印嵌入宿主中可理解为在一个宽带信道（载体对象）上采用扩频通信技术传输一个窄带信号（水印）。尽管水印信号具有一定的能量，但分布到信道中任一频率上的能量是难以检测到的。水印的译码（检测）则是一个有噪信道中弱信号的检测问题。

这里以数字水印在多媒体数字产品的产权保护中应用为例，介绍数字水印的基本框架。数字水印虽然形式众多，但我们可将水印信号统一表示为：

$$W=\{w(k)\in U,k\in W^d\} \tag{2-1}$$

其中W^d表示维数为d的水印域，当$d=1,2,3$时，分别表示声音、静止图像和视频中的水印。水印可以为二值形式或高斯噪声形式，其幅

值相对于要保护的数字产品的幅值应该是很小的。W有时被称为“原始水印”，用以区别于变换域水印形式$F(W)$。通用水印系统框架可以定义为六元体(X,W,K,G,E,D)，其中：

（1）X表示需保护的数字产品的集合。

（2）W表示水印信息的的集合。

（3）K是标示码（ID）的集合，也可以称为水印密钥。

（4）G表示利用密钥K与被保护数字产品X生成水印信息W的算法，即：

$$G:X\times K\rightarrow W \qquad W=G(X,K) \tag{2-2}$$

（5）E表示将W嵌入数字产品X_0中的嵌入算法，即：

$$E:X\times W\rightarrow X \qquad X_w=E(X_0,W) \tag{2-3}$$

其中，X_0表示原始数字产品，X_w表示嵌入水印信息后的数字产品。

（6）D代表水印信息检测算法，即：

$$D:X\times K\rightarrow\{0,1\} \tag{2-4}$$

$$D(X,W)=\begin{cases}1 & \text{如果}W\text{存在于}X\text{中}\\ 0 & \text{反之}\end{cases} \tag{2-5}$$

以上就是用于数字产品保护的水印系统框架模型，整个数字水印系统由水印信息的生成、嵌入和检测等几个算法模块组成。而在实际应用中，一个完整的数字水印处理系统可为水印的生成、嵌入以及提取三个部分。

2.2.1 数字水印的生成

数字水印信号根据其内容可以分为无意义的水印信号和有意义的水印信号两种。无意义的水印信号一般都对应于一个序列号或一段

随机数，没有具体的意义。无意义水印信号通常情况下都是使用均值为 0，方差为 1，即满足$N(0,1)$正态分布的伪随机实数序列。根据个人需求，可将产品的序列号、生产日期或无任何意义的一个数字作为“种子”，当序列发生器固定时，“种子”就是产生水印的密钥。将给定的“种子”作为伪噪声发生器的输入，就可以产生具有高斯分布的白噪声信号。在进行水印提取检测时，只要使用正确的密钥，就能产生和嵌入时相同的伪随机实数序列，用以检验待检测产品中是否含有该水印。比较常见的伪随机二值序列有：利用线性移位寄存器产生的 m 序列[20]，性能优良的 Legendre 序列[21]和对初值极其敏感的混沌序列[22,23]。

而有意义的水印信号一般是代表一定意义的文本、声音、图像或视频信号。对一个给定的有意义的水印，在嵌入载体之前绝大多数算法要求将其转化为二值序列，这些转化是各式各样的。使用 m 序列对水印进行扩频、对水印信号进行位分解、置乱技术等都可以提高水印的稳健性，这些方法将会在后面的章节进行介绍。

2.2.2 数字水印的嵌入

数字水印嵌入算法根据其所基于的域不同，主要可以分为时/空域算法、变换域算法和压缩域算法三类。水印嵌入过程如图 2-1 所示。

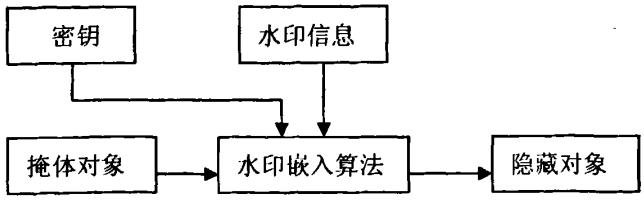


图 2-1 水印嵌入框图

水印嵌入就是把水印信号 $W=\{w(k)\}$ 嵌入到原始产品 $X_0=\{x_0(k)\}$ 中，一般的水印嵌入规则可描述为：

$$x_w(k)=x_0(k)\oplus h(k)w(k) \tag{2-6}$$

其中⊕为某种叠加操作，也可能包括合适的截断操作或量化操作。$H=\{h(k)\}$ 是 d 维（声音 1 维，图像 2 维，视频 3 维）的水印嵌入掩码。常用的嵌入准则有如下两种：

（1）加法准则

$$x_w(k)=x_0(k)+aw(k) \tag{2-7}$$

（2）乘法准则

$$x_w(k)=x_0(k)(1+aW(k)) \tag{2-8}$$

其中，变量 x 可以是掩体对象采样的幅值（时域），也可以是某种变换的系数值（变换域）；参数 a 可能随采样数据的不同而不同。早期许多水印嵌入算法都采用时域方法和加法准则，但是近年来，变换域算法得到了更广泛的研究。而且一般来说，乘性准则的抗失真性要更优于加法准则。

2.2.3 数字水印的提取和检测

数字水印提取是指根据与嵌入过程相同的密钥并通过一定的算法（一般是嵌入算法的逆过程）精确地提取出水印标志。而数字水印检测是指根据检测密钥通过一定的算法判断可疑作品中是否含有水印。图 2-2 和图 2-3 分别是水印提取与水印检测的框图，图中虚线框部分表示在水印提取或检测过程中不是必须的。

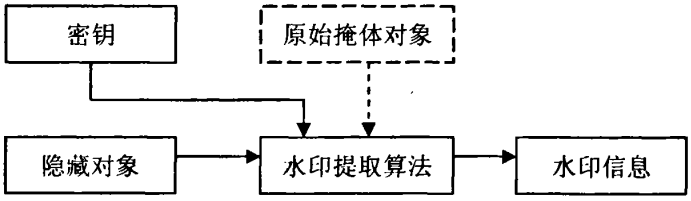


图 2-2 水印提取框图

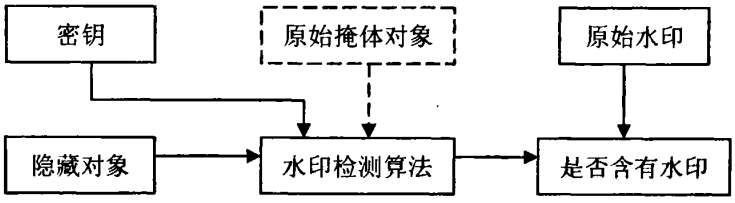


图 2-3 水印检测框图

2.3 数字水印的攻击

数字水印的攻击指的是任何一种可能削弱水印的检测或对水印所表达的信息传输的处理。在许多水印应用中，嵌入水印的图像在到达接收端的过程中总是会遇到有意或无意的攻击，而水印在受到这些攻击操作后被削弱。一个成功的水印系统应该在遭受一些处理后仍然能检测出水印的存在，或者当水印被破坏时，图像已经产生严重的失真而失去本身的价值。而水印生命周期中若任何一个阶段被攻击者破坏，水印对信息的保护都会被打破。在此，将水印系统的攻击分为以下几类，每一类都针对水印处理的某一阶段[24]。

（1）信号去除攻击

信号去除攻击涉及到水印信号的消除，它包括几种，最简单的就是“基本攻击“。基本攻击是通过简单的降低图像质量或采用常规的图像处理手段达到除去水印。这种攻击是对整个水印数据进行操作，而不是将水印区分和隔离出来。还有一种是在加有水印的图像中，再

加入一条水印，这种处理对于公有水印比私有水印有效，更容易通过第二条水印覆盖的方法来消除前一条水印。另一种攻击是共谋攻击，它采用几个带有不同水印的相同载体拷贝进行攻击。

（2）表示攻击

表示攻击就是采用一种使检测器无法检验到有效水印的方法。表示攻击又可以称为同步攻击，它是试图破坏相关性和使得水印检测器对水印的恢复变得不可能或不可实现的攻击方法，其中最典型的就是几何攻击和马赛克攻击。大部分水印不能够经受几何变形的攻击，因为对于所有给定的水印方法，水印检测器必须知道水印嵌入的确切位置，而几何变形趋向于破坏同步性，使得水印嵌入和检测位置偏离不再相符。

（3）解释攻击

解释攻击是通过试图产生假的嵌入水印数据来进行制造混乱的攻击方法。例如，通过加入一个或几个另外的水印而使得最先的原始水印不能清楚地区分出来，以致造成对水印权限的怀疑。

（4）合法性攻击

合法性攻击主要是通过法律上的一些条款上的漏洞达到攻击的目的。在实际应用中，含水印图像常会受到有意或无意的攻击破坏，因而就要求水印系统能从遭到破坏的图像中正确检测或提取出水印。这里的破坏是指图像未产生过度的降质，否则接收到的图像就没有使用价值了，对蓄意的攻击，攻击者的目标是对图像做最小的变动而对水印产生最大的影响，因此密钥就成为水印算法安全的关键所在。

常见的数字图像水印攻击手段有以下几种：

加噪：噪声的叠加主要来自于 A/D、D/A 转换，或由其他变换误差引入，攻击者也可能利用信号处理引入不被感知的噪声。噪声叠加使虚警率增加，只有提高相关检测器的检测门限才能改善检测性能。

滤波：滤波对图像质量不会产生严重破坏，但会极大的影响一些水印算法的检测性能。例如，由于水印扩展会产生不容忽视的高频成分，因此，低通滤波对扩频水印算法影响较大。

剪切：剪切是最常见的估计，因为攻击者往往只对图像的一部分感兴趣，为了抵抗剪切攻击，需要将水印扩展到整个图像中。

压缩：压缩通常是无恶意的攻击，常出现在多媒体应用中。实际上，当前在互联网上分布的媒体大多都要经过压缩处理。如果要求水印能抵抗压缩攻击，通常可取的方法是提高水印嵌入容量。

旋转与缩放：多数水印算法对这种攻击都很脆弱，由于嵌入的水印与本地产生的水印空间模式不同，含水印图像经过旋转和缩放处理后再用相关检测的方法检测或提取水印就很难得到正确的结果。当然，如果能在检验时提供原始图像，那么通过比较原始图像和水印图像就可估计出旋转角度和缩放因子，将大大简化水印的检测过程。Ruanaidh 等人提出过具有旋转、平移及缩放不变性的水印算法[25]，这种算法利用傅立叶-梅林变换旋转、缩放不变性的特点，但是大大降低了水印的潜入容量。

统计平均：攻击者可能会试图估计出水印，然后去除水印。如果水印不是充分的依赖原始图像数据，那么他们对多个含水印图像进行

简单的统计平均，就有可能消除水印。因而利用视觉掩蔽模型产生水印就是一个有效抵抗统计平均的办法。

多水印：攻击者可能会对一个已含有水印的产品嵌入新的水印，而后宣称自己是所有者。最简单的办法就是到认证机构登记隐藏信息。

其他攻击：还有一些针对水印处理的攻击。例如，通过过分扰乱数据使水印丢失，从而回避版权控制机构；或是通过创建一个可调整数据顺序的传输层来欺骗 Web 浏览器搜寻一定的水印，这种攻击方法称为“mosaic“攻击[26]。

2.4 数字水印的技术特点及性能评估

2.4.1 数字水印的技术特点

数字水印技术是用于版权保护的一种直观而有力的工具，它除了具备信息隐藏技术的一般特点外，还有着其自身固有的特点和研究方法。目前，该技术形成了几个公认的标准：

（1）不可察觉性

不可察觉性即水印的透明性，大多数数字水印系统都要求带水印的图像保持极高的品质，人眼基本上不能辨别它与原始图像。同时，由于在数字方式下，标志信息很容易被修改或去除，因此应该根据多媒体信息的类型和几何特征，将水印隐藏其中，使非法拦截者无法察觉。

（2）鲁棒性

鲁棒性即指水印在经受一些有意或无意的攻击操作后，仍然存在

于多媒体数据中并可以被恢复或检测出来。

（3）容量

一般要求水印算法能嵌入一定的水印信息量。容量太少水印鲁棒性不强，不足以确定产品的唯一性，而容量太大透明性不好，容易破坏产品的品质。通常要求根据不同的应用需求选择合适的水印容量。

（4）安全性

嵌入的水印信息必须只有授权的机构才能检测出来，非法用户不能判断水印是否存在，或者即使检测出水印，也不能获取或去除水印信息。

（5）盲检测性

水印在检测和解码过程中不需要未加水印的原始载体图像的具体信息。

2.4.2 数字水印的性能评估

水印的透明性和鲁棒性是数字水印技术最基本的两大特性，它们之间存在着一个折衷的问题。理想的水印算法应该既能不被感知地隐藏大量数据，又可以有效抵抗通信过程中遭遇的各种攻击。在实际应用中，这两个指标往往不能同时满足，应该根据实际需要侧重其一。通常采取的原则是在保证视觉质量的前提下，以最大强度嵌入水印。此外，水印的鲁棒性还受到嵌入的信息量、水印嵌入强度、图像的尺寸和特性、密钥等诸多参数的影响。

对水印的性能评估主要包括水印鲁棒性的评估以及嵌入水印对图像引起的失真的评估，即水印透明性的评估。数字水印技术目前尚

无通用的标准对水印系统的性能进行评价，通常的做法是首先对嵌入水印的图像进行一系列的攻击，然后从被攻击的图像中提取水印，并判断水印提取的成功与否。目前人们对与数字水印的透明性的评价主要使用两种方法：

（1）主观测试方法（Subjective Test）

评价一幅作品的好坏，最直接的方法就是采用主观打分。这种测试可以分两步：第一步把产生失真的数据集按照由好到坏的次序分为几个等级。第二步测试者根据每个数据集的失真程度进行打分并描述水印的可见性。这种打分可以基于 ITU-R Rec.500 的质量分数 Q，此值由下式计算：

$$Q=\frac{5}{1+N\times E} \tag{2-9}$$

其中，E 是计算得到的失真量，N 是标准化常数。表 2-1 给出了 ITU-R Rec.500 质量等级评判的分数和相应的视觉可察觉性指标以及图像质量。实验表明，这种测试方法对最终的图像质量评价和测试十分有用，但不利于学术上研究成果之间的相互比较。因此，在实际研究和开发过程中多采定量度量的方法。

表 2-1 ITU-R Rec.500 从 1 到 5 范围的质量等级级别

等级	对图像质量的损坏	质量
5	不可察觉	优
4	可察觉，但不令人厌烦	良
3	轻微令人厌烦	中
2	令人厌烦	差
1	很令人厌烦	极差

（2）定量方法（Quantitative Metric）

失真定量测试是一种客观的方法，它不依赖于主观评价，可以方便的用于对个中方法进行公正的比较。基于像素的图像质量评价度量方法属于量化失真度量（Quantitative Distortion Metric），用它得到的结果不依赖于主观评估，允许在不同方法之间进行公平的比较。在图像、视频编码和压缩域领域使用最多的度量指标是信噪比 SNR（Signal to Noise Ration）和峰值信噪比 PSNR(Peak Signal to Noise Ration)。为了适应不同的评价需要，我们给出几种参数的定义方法：

1. 归一化相关系数 NC（Normalized Cross-Correlation）：

原始水印 W 和提取出的水印 W' 之间的相似度可以通过相关性检验来衡量，当水印为序列时，将 W 和 W' 看作一维向量，通过计算一维相关系数 $Corrcoef(W,W')$，则归一化的相关系数 NC 的计算公式如下：

$$NC=\frac{WW'}{\sqrt{WW'}}=\frac{\sum_{i=1}^{n}W_iW_i'}{\sqrt{\sum_{i=1}^{n}W_i^2\sum_{i=1}^{n}W_i'^2}} \tag{2-10}$$

当水印为图形时，可以将 W 和 W' 看作二维向量，通过计算二维相关系数 $Corr2(W,W')$，则归一化相关系数 NC 的计算公式如下：

$$NC=\frac{WW'}{\sqrt{WW'}}=\frac{\sum_{i=1}^{n}\sum_{j=1}^{m}W_{ij}W_{ij}'}{\sqrt{\sum_{i=1}^{n}\sum_{j=1}^{m}W_{ij}^2\sum_{i=1}^{n}\sum_{j=1}^{m}W_{ij}'^2}} \tag{2-11}$$

同时，得到归一化相关系数 NC 后，也可以衡量水印的误差百分比，用 R 来表示，则计算公式如下：

$$R = 1 - NC \tag{2-12}$$

2. 峰值信噪比 PSNR(Peak Signal to Noise Ration)

$$PSNR = 10\log_{10}\frac{\max W_{m,n}^2}{MSE} \tag{2-13}$$

由式（2-11）中可以看出较高的峰值信噪比对应较高的图像间相似程度，也即表示嵌入水印后的图像具有较高的不可感知性。其中 MSE (Mean Square Error)为均方误差，也可以用来度量图像的客观保真度，与 PSNR 相反，MSE 越小表示图像的近似程度越高，计算公式如下：

$$MSE = \frac{1}{MN}\sum_{m,n}(W_{m,n} - W'_{m,n})^2 \tag{2-14}$$

3. 比特错误率

对于特定信息的字符码串，通常可以用比特错误率来度量，这和通信中的误码率概念比较相似，其计算公式为：

$$BER = \frac{\sum_{i=1}^{n}\sum_{j=1}^{m}(W(i,j) - W'(i,j))}{\sum_{i=1}^{n}\sum_{j=1}^{m}W(i,j)} \tag{2-15}$$

以上的度量方法虽然是客观的，但并不能完全反映人类感觉系统对数字作品的评价，有些时候可能会与人类感觉产生不一致。本文中使用的度量方法主要是归一化相关系数 NC 和峰值信噪比 PSNR 两种。

第 3 章 数字图像置乱技术

数字图像作为一种直观的信息表达方式，具有很大的迷惑性，如果我们把数字图像做一些“扰乱”，得到一幅完全杂乱无章、面目全非的图像，那么即使非法截获者得到它，如果不知道如何恢复，对它也无能为力，这就在一定程度上增加了图像的安全性。数字图像置乱技术正是这样一项研究课题，它能够扰乱图像的组成部分，破坏图像的自相关性，使得人眼无法从中提取有价值的信息，即使计算机使用“穷举法”计算各种组合，也要耗费大量的时间，这就在一定程度上保护了图像信息。置乱技术主要用于图像的预处理和后处理，目前，人们考虑较多的技术主要有以下几种：混沌、Arnold 变换、幻方、Hilbert 曲线、Conway 游戏、Tangram 算法、IFS 模型、广义 Gray 码变换、仿射变换、正交拉丁方变换等[27-29]。下面简单介绍几种常见的图像置乱算法。

3.1 基于混沌的图像置乱技术

3.1.1 混沌的概念

混沌现象是美国气象学家 Lorenz[30]早在 1963 年研究模拟天气预报时发现的。当时他是把大气的动态方程简化成了三阶非线性方程（后来被称之为 Lorenz 方程），应用当时的计算技术，结果发现这个确定性方程的动力学演化具有类似随机的性质，发现了著名的 Lorenz 吸引子，因而推断出长期的天气预报是不可能的结论（即著名的“蝴

蝶效应”)。后来，美国生物学家 Robert • May[31]在研究生物的种群变换的 Logistic 方程时也发现了这个确定性的动力学系统的演化具有混沌的性征，即对初始条件极端敏感。

混沌现象是在非线性动力系统中出现的确定性的、类似随机的过程，这种过程既非周期又不收敛，并且对初始值有极其敏感的依赖性。由于混沌现象的复杂性，到目前为止，对于混沌还没有一个统一严格的数学定义。一维离散时间非线性动力系统可以定义如下[32]：

$$X_{n+1} = F(X_n, u) \qquad n = 0,1,2\cdots \tag{3-1}$$

其中 F 表示混沌映射，u 为控制参数，x_n 为状态。映射 F 将当前状态 x_n 映射到下一个状态 x_{n+1}。目前，用于数字水印中的混沌方法主要有 Logistic 映射、Chebshev 映射、Reny 映射以及花托自同构四种。下面介绍一种基于 Logistic 映射的数字图像置乱算法。

3.1.2 基于 Logistic 映射的数字图像置乱算法

这里假设需要置乱的水印 W 是大小为 $N \times N$ 的灰度图像。而 Logistic 映射可以定义为：

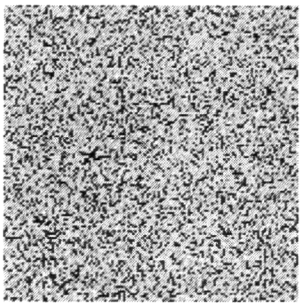
$$X_{n+1} = uX_n(1 - X_n) \qquad n = 0,1,2\cdots \tag{3-2}$$

其中，$X_n \in (0,1)$，当 $u \in (3.57,4]$ 时，系统处于混沌状态。首先选定初始值 X_0 作为水印图像置乱和置乱还原的密钥，从该初始值 X_0 开始迭代 $N \times N + 1$ 次，然后去掉初始值，使用 Matlab 命令 sort 对所获得的 $N \times N$ 个值按从大到小进行排序，得到相应的一维排序序号 $Index(k)$，其中 $k = N \times N$。接下来将水印图像按列排成一维向量 $W(i)$，将 $W(i)$ 对应的值放入下标为 $Index(k) = i$ 的位置即可得到

$W_1(Index(k))$，最后将该长度为$N \times N$的一维向量$W_1(Index(k))$按列转换为N行N列的二维矩阵$W_2(N,N)$，该矩阵即为置乱后的图像矩阵。若按上述方法使用不同的密钥进行多次置乱则可进一步增加水印图像的安全性。

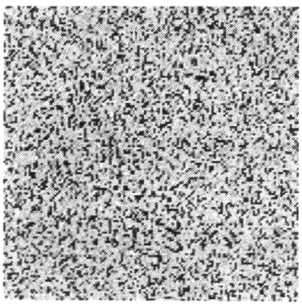
置乱图像的恢复算法是上述置乱算法的逆过程。图 3-1 是水印图像的置乱与还原过程，置乱过程中的密钥取$X_0 = 0.0254$，（d）是用错误密钥$X_0 = 0.0253$对置乱图像进行恢复的结果，可以看出，由于 logistic 序列对初值的极端敏感性，即使是 0.0001 的误差也不能正确的恢复图像，只有获得正确的密钥才能恢复出水印图像。

（a）原始水印图像



（b）置乱后的水印图像

（c）恢复的水印图像



（d）错误密钥恢复的图像

图 3-1 水印图像的置乱与还原

3.2 基于 Arnold 变换的图像加密算法

Arnold 变换，也称为猫映射(cat map)[33]，是 V. I. Arnold 在研究环面上的自同态时所提出的。设需要置乱的是一幅大小为$N \times N$的数字

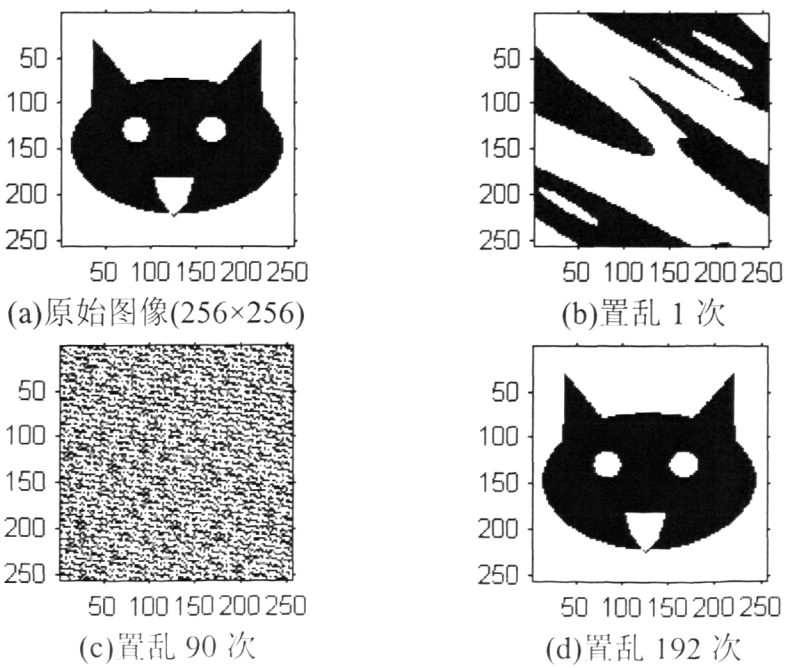
图像，像素的坐标$x,y\in S=\{0,1,2,\cdots,N-1\}$，则 Arnold 变换的矩阵式如公式(3-3)所示。

$$\begin{pmatrix}x_{i+1}\\y_{i+1}\end{pmatrix}=\begin{pmatrix}1&1\\1&2\end{pmatrix}\begin{pmatrix}x_i\\y_i\end{pmatrix}(\mathrm{mod}\,N) \qquad (3\text{-}3)$$

其中，x_i,y_i分别表示原始图像中像素的横坐标和纵坐标，x_{i+1},y_{i+1}分别表示置乱后图像相应像素所在的横坐标和纵坐标。由于 Arnold 变换具有周期性，即存在一个正整数P满足公式(3-4)。

$$A^P r_i(\mathrm{mod}\,N)=r_i \qquad (3\text{-}4)$$

其中，$A=\begin{bmatrix}1&1\\1&2\end{bmatrix}$称为二维 Arnold 矩阵，$r_i=(x_i,y_i)'$，$P$即为 Arnold 变换的周期，即原始图像经过$m=\{m\,|\,m\in Z^+,1\le m\le P\}$次 Arnold 变换后将变得“混乱不堪”，但是再经$(P-m)$次 Arnold 变换后又能恢复到原图，图 3-2 演示了这一变化过程。而变换的周期P的大小又与图像大小参数N有关[34]，如表 3-1 所示。



(a)原始图像(256×256)　(b)置乱 1 次

(c)置乱 90 次　(d)置乱 192 次

图 3-2 Arnold 变换用于图像置乱

表 3-1 Arnold 变换周期 P 与图像大小 N 的关系

N	8	16	32	64	128	256	512	1024
P	6	12	24	48	96	192	384	768

在实际应用中，数字水印技术正是利用 Arnold 变换的周期性，先将要嵌入到数字产品中的数字水印图像进行置乱，然后再利用各种算法将其嵌入到数字产品中。当该数字产品遭到用户的修改或恶意攻击时，数字产品的某一部分通常会遭到损坏或丢失(例如裁剪)，这样一来嵌入的数字水印的某一部分也会遭到损坏或丢失，当将该遭到损坏的数字水印提取出来后，再继续利用 Arnold 变换可以恢复数字水印图像。由于在恢复的过程中, Arnold 变换将会把原先遭到损坏的比特分散开来，减少其对人视觉的影响，相应地提高了数字水印的鲁棒性。

3.3 基于幻方的图像置乱技术

幻方是一个非常古老而有趣的数学问题，它的定义及数学表达式如下：

以1,2,…,n^2 个自然数为元素构成的 n 阶矩阵为：

$$A=\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix} \tag{3-5}$$

若 A 中的元素满足如下条件：

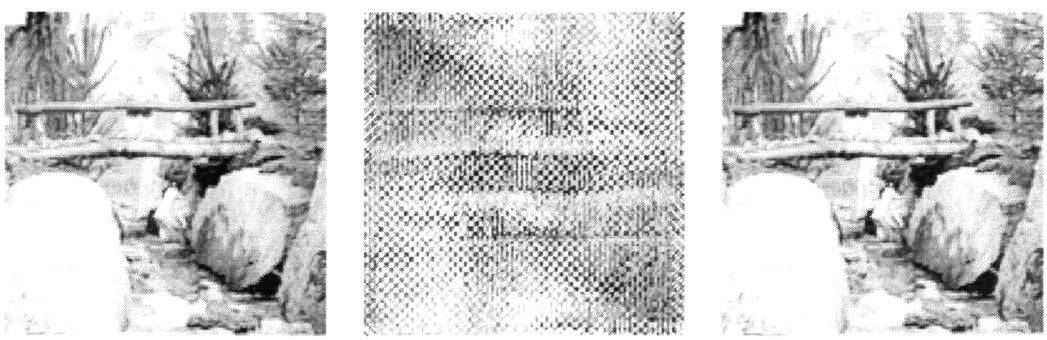
$$\sum_{i=1}^{n} a_{ij}=\sum_{j=1}^{n} a_{ij}=\sum_{i=1}^{n} a_{ii}=\sum_{i+j=n+1} a_{ij}=\frac{n(n^2+1)}{2} \tag{3-6}$$

则称 A 为 n 阶幻方。“九宫格”就是一个典型的三阶幻方，图 3-3 是它的一种排列方案，图中的每行、每列以及对角线上的元素之和均为 15。

4	9	2
3	5	7
8	1	6

图 3-3　3 阶幻方

在利用幻方变换进行图像置乱时，应首先使图像的行数与列数与标准幻方阵一一对应，若不对应，则应通过某种变换或图像分块的方法使得图像矩阵或各图像分块的大小能与标准幻方大小对应。这里假设原始图像大小为 $N \times N$，幻方矩阵内的元素代表图像像素的坐标，在置乱时，图像像素 1 移到像素 2 的位置，像素 2 移到像素 3 的位置，其余类推，最后，像素 N^2 移到像素 1 的位置。如此重复几次幻方变换后，图像将变得面目全非，而经过 N^2 次变换之后，又会恢复到原图像。图 3-4 演示的就是这样一个变换过程。



（a）原始图像（128×128）　（b）5 次幻方变换后　（c）16384 次幻方变换后

图 3-4　幻方变换用于图像置乱

幻方变换算法易于实现，且其重复置乱的次数可以作为水印系统的密钥使用，从而可以增强水印系统的安全性和保密性，同时，基于幻方的图像置乱算法可以克服随机置乱的不可复位性，因此，在数字

水印技术中得到了较为广泛的应用。

第 4 章 基于 DCT 域的灰度级盲水印算法

4.1 离散余弦变换

离散余弦变换(Discrete Cosine Transform)简称 DCT，是数字信号处理技术中最常用的线性变换之一。与傅立叶变换的参数都是复数相比，DCT 变换避免了傅立叶变换中的复数运算，在实现将信号从时域变换到频域的同时，大大减小了数据量，是一种基于实数的正交变换，因此它在数字音频信号压缩和图像压缩等领域得到了广泛的应用。值得一提的是，数字图像的 JPEG 压缩标准就是建立在离散余弦变换基础上的。基于 JPEG 压缩标准模型的水印嵌入算法可以增强水印抵抗 JPEG 压缩的能力，因此，DCT 变换在数字水印处理技术中受到了普遍重视。

一幅静止的数字图像可看作是二维数据阵列，因此，在数字图像水印技术中一般采用的是二维 DCT 变换，其定义如下[35]：

$$F(u,\upsilon)=\frac{2}{\sqrt{MN}}c(u)c(v)\sum_{x=0}^{M-1}\sum_{y=0}^{N-1}f(x,y)\cos\frac{(2x+1)u\pi}{2N}\cos\frac{(2y+1)\upsilon\pi}{2M} \quad (4\text{-}1)$$

其中：

$$c(u)=\begin{cases}\frac{1}{\sqrt{2}}, & u=0\\ 1, & 0\le u\le M-1\end{cases}, \quad c(v)=\begin{cases}\frac{1}{\sqrt{2}}, & v=0\\ 1, & 0\le v\le N-1\end{cases} \quad (4\text{-}2)$$

$f(x,y)$是空域二维向量中的元素，$F(u,\upsilon)$是变换后系数阵列的元素，阵列的大小为$M\times N$。

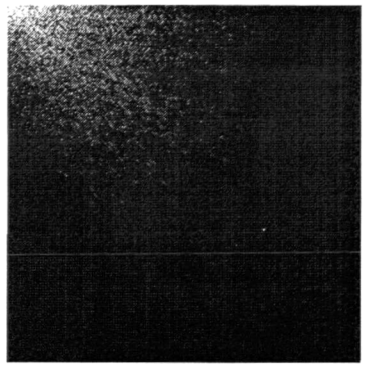
二维的逆 DCT 变换定义如下：

$$f(x,y)=\frac{2}{\sqrt{MN}}\sum_{u=0}^{M-1}\sum_{v=0}^{N-1}c(u)c(v)F(u,v)\cos\frac{(2x+1)u\pi}{2N}\cos\frac{(2y+1)v\pi}{2N} \quad (4\text{-}3)$$

式（4-3）中系数$c(u)$，$c(v)$的定义与式（4-2）相同。

接下来对原始图像 Lena 进行二维 DCT 变换，结果如图 4-1 所示，由图我们可以看出，变换后的 DCT 系数能量主要集中在左上角，而其余大部分系数都接近与零。

(a)原始图像 Lena



(b)DCT 变换系数能量分布

图 4-1 图像的 DCT 变换

二维 DCT 变换不但能够将自然图像的主要信息集中到最少的低频系数上，而且引起的图像块效应最小，能够实现信息集中能力和计算复杂性的良好折中，同时，它的去相关能力、可以通过快速算法计算等优点使得它在数字水印嵌入算法中具有很强的吸引力。

4.2 灰度图像位分解

本章中所采用的水印图像为灰度图像，因此，在水印嵌入原始图像前首先要对灰度图像进行二值化分解。目前采用较多的方法有图像的位分解[36](bit decomposition)、阈值分解[37](threshold decomposition)、高斯-拉普拉斯金字塔分解[38](Gaussian pyramid decomposition)等。本文采用位分解法对灰度水印进行分解。下面给出它的具体过程。

对一幅大小为$M\times N$的 8bit、256 灰度级的图像，可以将其按位

分解为 8 层位图，每层每个像素点对应的值只含有 1 或 0。令 X 是大小为 $M\times N$、灰度级为 2^L(L 为正整数)的图像，$X_P(m,n)$ 是图像的一个像素值，其中，$1\le m\le M$，$1\le n\le N$，位分解算法如下：

$$x^l(m,n)=B^l(X_P(m,n))=\begin{cases}1, & if(Integer[X_P(m,n)/2^l]\bmod 2=1\\ 0, & else\end{cases} \quad (4\text{-}4)$$

其中 $B^l(\cdot)$ 表示位分解算子，$x^l(m,n)\in\{0,1\}$。对 $x^l(m,n)$ 的重构公式为：

$$X_P(m,n)=\sum_{l=0}^{L-1}x^l(m,n)\times 2^l \quad (4\text{-}5)$$

254	210	118	127
110	98	64	101
88	56	77	24
96	22	11	36

(a)原始图像

1	1	0	0
0	0	0	0
0	0	0	0
0	0	0	0

(b) b_8

1	1	1	1
1	1	1	1
1	0	1	0
1	0	0	0

(c) b_7

1	0	1	1
1	1	0	1
0	1	0	0
1	0	0	1

(d) b_6

1	1	1	1
0	0	0	0
1	1	0	1
0	1	0	0

(e) b_5

1	0	0	1
1	0	0	0
1	1	1	1
0	0	1	0

(f) b_4

1	0	1	1
1	0	0	1
0	0	1	0
0	1	0	1

(g) b_3

1	1	1	1
1	1	0	0
0	0	0	0
0	1	1	0

(h) b_2

0	0	0	1
0	0	0	1
0	0	1	0
0	0	1	0

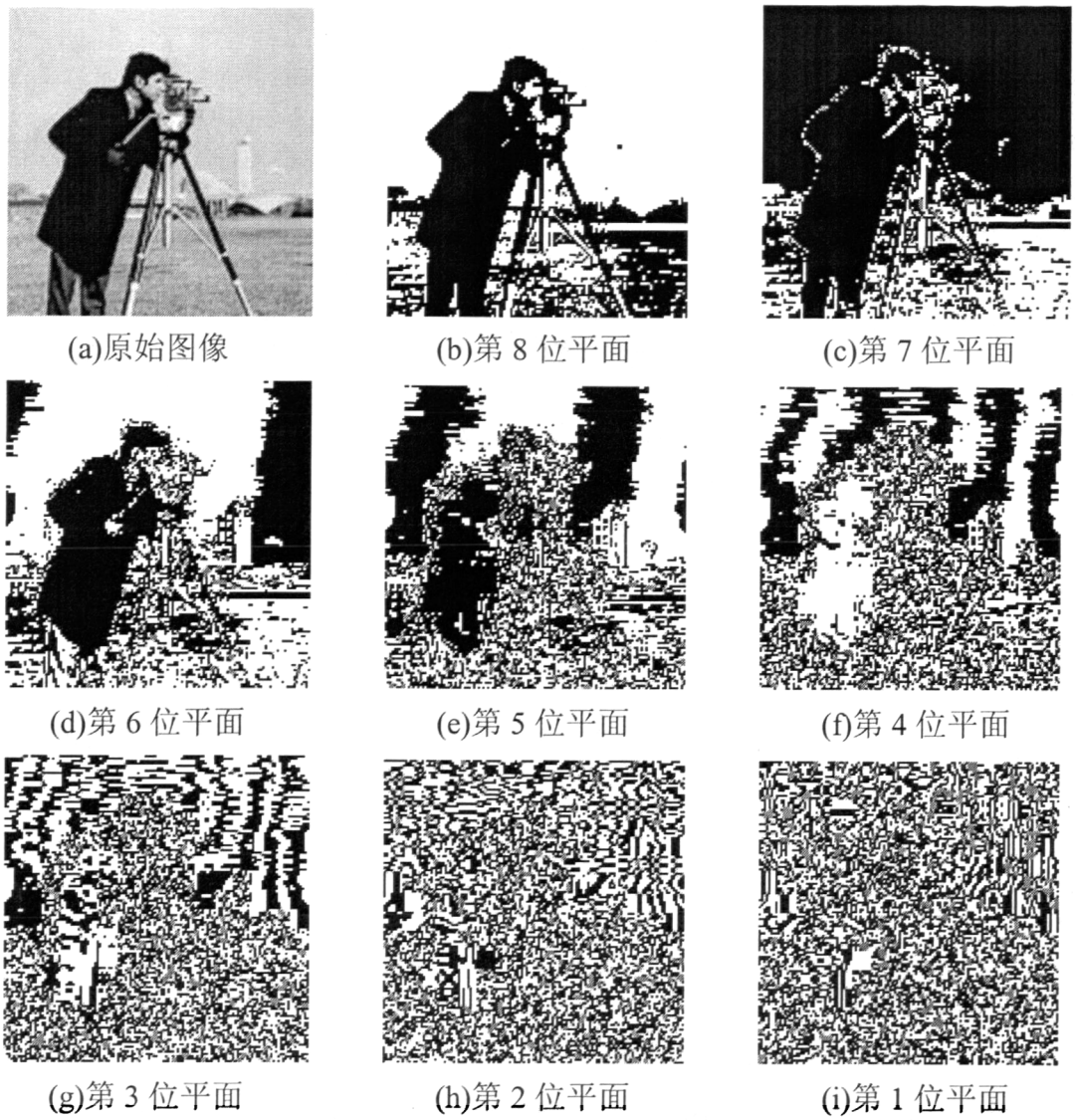
(i) b_1

图 4-2　一个 8bit 灰度图像信号的位分解示意图

对一幅 4×4 的 8bit 灰度级图像的分解如图 4-2 所示，其中 b_8 是最高有效位，b_1 是最低有效位。

一幅图像在经过位分解后得到的各位平面在原始图像中的权重

是不同的，为了更直观的看出其影响，我们对一幅128×128的灰度图像进行了位分解，如图 4-3 所示。



(a)原始图像　(b)第 8 位平面　(c)第 7 位平面

(d)第 6 位平面　(e)第 5 位平面　(f)第 4 位平面

(g)第 3 位平面　(h)第 2 位平面　(i)第 1 位平面

图 4-3 灰度图像的位分解示意图

由图我们可以看出，高位位平面所包含的信息要比低位位平面所包含的信息重要的多。因此，在实际嵌入过程中，应根据水印各位平面权重的不同，尽量考虑那些高权重位平面的鲁棒性。

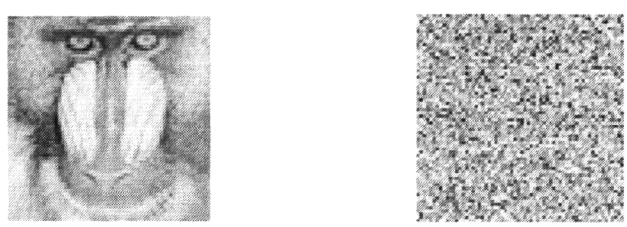
4.3 基于混沌置乱的 DCT 域灰度级盲水印算法

这里以大小为$M \times M \times 8$的灰度图像作为载体图像，而水印则选择大小为$N \times N \times 8$的灰度图像，其中，$N \le M/8$，为了增加产权保护

的信息量一般取等于。水印嵌入的过程在 DCT 域完成以增加算法抗 JPEG 压缩的能力，水印在嵌入载体图像之前先经过置乱处理，具体算法如下。

4.3.1 水印的置乱与还原

水印图像置乱不仅能去掉图像的相关性，避免块效应的产生，增加水印的安全性，同时还能增加水印嵌入的鲁棒性，使图像信息的灰度值均匀分布在整幅载体图像中，使其具有较强的抗剪切、破损和污染的能力。这里采用由 logistic 映射所描述的简单动力系统，用生成的混沌序列对原始水印图像做置乱处理。置乱过程如第三章所述，这里不再重复。图 4-4 是原始水印图像和经 logistic 映射置乱后的水印图像。



（a）原始水印图像　　（b）置乱后的水印图像

图 4-4 水印的置乱和还原

4.3.2 数字水印的嵌入

1. 对载体图像 I 做互不覆盖的8×8的分块 DCT 变换，共有$M\times M/64$块，其中第k块的系数为$F_k(u,v)$，对所得的块按从左至右、从上至下的顺序依次嵌入一个水印像素，每一个 DCT 块中嵌入水印的系数是坐标为（1,2），（1,3），（1,4），（2,1），（2,2），（2,3），（3,1）及（3,2）的这八个最低频系数，如图 4-5 所示。之所以选择这八个系数是因为低频部分集中了图像的绝大部分能量，水印嵌入于此能增加

其鲁棒性[39]。

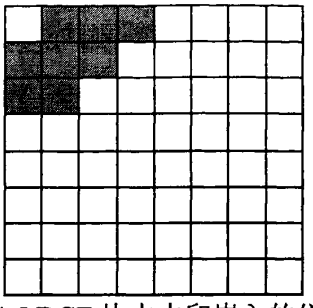


图 4-5 DCT 块中水印嵌入的位置

2. 每一个水印像素$W_2(i,j)$按从左至右、从上至下的顺序分解为8位，得到每一位的信息值$W_{2k}(L)\in\{0,1\}$，k表示第k个像素，L取1到8的整数，得到的水印位按从左至右、从上至下的顺序依次嵌入到载体图像第k块中所选的八个低频系数中。水印嵌入使用文献[40]中提出的系数量化的方法，量化值为Q。由于量化误差及其它误差的存在，要求Q尽可能取得大一些，而Q值过大又影响水印的不可见性，由大量实验结果得出，Q取24时算法具有较好的鲁棒性和不可见性。水印的嵌入规则如下：

（1）如果$W_{2k}(L)$等于1：

$$\begin{cases} F_k(u,v)=F_k(u,v)-\mathrm{mod}(F_k(u,v),Q)-Q/4; & \mathrm{mod}(F_k(u,v)\le Q/4 \\ F_k(u,v)=F_k(u,v)-\mathrm{mod}(F_k(u,v),Q)+3Q/4; & \text{其它} \end{cases} \tag{4-6}$$

（2）如果$W_{2k}(L)$等于0：

$$\begin{cases} F_k(u,v)=F_k(u,v)-\mathrm{mod}(F_k(u,v),Q)+5Q/4; & \mathrm{mod}(F_k(u,v),Q)\ge 3Q/4 \\ F_k(u,v)=F_k(u,v)-\mathrm{mod}(F_k(u,v),Q)+Q/4; & \text{其它} \end{cases} \tag{4-7}$$

3. 位分解后的8位值都嵌入后，对经过调整的该块系数$F_k(u,v)$做反DCT变换，得到嵌入水印后的图像块。

4. 继续按上述方法嵌入下一个水印像素，直到所有的水印像素

都嵌入到载体图像块中。整合所有嵌入水印后的图像块，得到嵌入水印后的图像 J。

4.3.3 数字水印的提取

水印提取实际上是上述嵌入算法的逆过程，首先对嵌入水印后图像 J 做8×8的分块 DCT 变换，在每一块中提取出上述八个位置处对应的系数，用该系数值对量化值 Q 求余，若所得的结果比$Q/2$小，则嵌入的水印位为 0，否则为 1，这里的$Q/2$是预先设定的一个判断水印嵌入的阈值。接着将该块中所得的 8 个水印位进行重组，则得到嵌入于该块中的一个水印图像的像素值，最后对所有块中提取出的像素进行置乱还原，得到最终提取出的水印。

4.3.4 实验结果与分析

仿真实验在 MATLAB7.0 平台上进行，实验用的载体图像采用标准图像库中的512×512×8的 Lena 图片，而水印图像使用64×64×8的 baboon 图片，如图 4-6 所示。含水印图像的质量使用峰值信噪比 PSNR(dB)来评价，提取出的水印则用归一化互相关系数 NC 来评价。

（a）原始载体图像

（b）原始水印

图 4-6　实验采用的原始图片

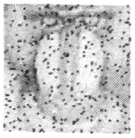
在没有攻击的情况下，实验测得含水印图像的峰值信噪比为

39.9594dB，很好的实现了水印的不可见性，提取出的水印 *NC* 值为 1，能完全正确的实现盲提取。含水印图像和提取出的水印如图 4-7 所示。

（a）含水印图像（PSNR=39.9594dB）　（b）提取的水印（NC=1）

图 4-7 无攻击情况下的含水印图像及提取的水印

为了对算法的鲁棒性进行分析，接下来我们对嵌入水印后的含水印图像进行一系列的攻击处理，包括 JPEG 有损压缩、添加噪声、几何剪切等，然后再从中提取水印。图 4-8 是对含水印图像任意剪切 2 块并用黑色填充的结果和提取出的水印，由图可以看出，算法对恶意剪切具有很好的鲁棒性。图 4-9 至图 4-12 是对含水印图像进行各种加噪和滤波攻击的结果，图 4-13 和图 4-14 是对含水印图像分别做 JPEG 有损压缩因子 Q 为 60 和 90 后的结果。由图可以看出，算法对各种常见图像处理操作具有很好的鲁棒性。

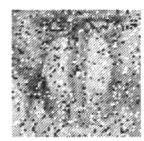


（a）PSNR=15.5343dB　　（b）NC=0.9936

图 4-8 任意剪切后的含水印图像和提取出的水印

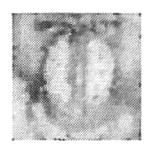

（a）PSNR=24.9231dB　　（b）NC=0.8848

图 4-9 添加 0.01 椒盐噪声后的含水印图像和提取出的水印

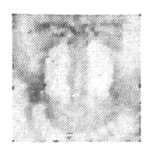
（a）PSNR=29.2998dB　　（b）NC=0.7480

图 4-10 添加 0.001 高斯噪声后的含水印图像和提取出的水印

（a）PSNR=34.9750dB　　（b）NC=0.9016

图 4-11 中值滤波后的含水印图像和提取出的水印

（a）PSNR=36.9871dB　　（b）NC=0.9001

图 4-12 维纳滤波后的含水印图像和提取出的水印


（a）PSNR=34.4089　　（b）NC=0.9955

图 4-13 JPEG 压缩因子 Q=60 及提取的水印


（a）PSNR=37.5007　　（b）NC=1

图 4-14 JPEG 压缩因子 Q=90 及提取的水印

为了更好的进行数据分析，将各攻击实验的数据列表如下。其中，表 4-1 是对含水印图像进行滤波、加噪等图像处理操作的结果，表 4-2 是含水印图像经 JPEG 有损压缩后的结果。由表 4-1、表 4-2 可以看出，算法对一些基本的图像处理操作都有较好的鲁棒性，尤其是对 JPEG 压缩有着非常好的抵抗力，即使图像压缩至 60%仍然能基本正确的提取出信息。

表 4-1 攻击实验结果

攻击方式	含水印图像 PSNR(dB）	提取水印 NC
0.001 高斯噪声	19.4806	0.7449
0.01 椒盐噪声	24.9179	0.8775
均值滤波	28.3128	0.7907
中值滤波	34.9720	0.9027
维纳滤波	36.9955	0.9056

表 4-2.JPEG 压缩实验结果

JPEG 压缩 质量因子 Q	含水印图像 PSNR(dB)	提取水印 NC
50	34.5561	0.7867
60	34.4089	0.9955
70	35.2531	1
80	36.3866	1
90	37.5007	1

本章所提出的数字水印算法简单、易实现，且水印信息的提取无需原始水印，对彩色图像来说，若将其分解为红、绿、蓝三个亮度分量并分别进行水印的嵌入，该算法也同样适用，因此具有较好的实用价值。同时，在描述算法的基础上，给出了实验结果和一系列的攻击分析，实验结果表明，该算法具有较强的不可见性与鲁棒性。

第 5 章　基于超混沌和 HVS 的小波域盲水印算法

5.1 小波理论基础

小波分析是 20 世纪 80 年代后期形成的一个新兴的数学分支，它是在傅立叶分析的基础上发展起来的。与傅立叶分析相比，小波变换是时间和频率的局部变换，能更加有效的提取信号和分析局部信号。

小波技术可以将信号或图像分层，按小波基展开，根据图像信号的性质和事先给顶的处理需求确定需要展开到哪一级为止，能有效的控制计算量，满足实时处理的需要。同时，小波变换具有放大、缩小和平移的数学显微镜的功能。正是由于小波的这一系列的优点，使得它在图像处理尤其是图像压缩方面得到了广泛的应用。在新出现的图像压缩标准“JPEG 2000”及最近颁布的运动图像压缩标准“MPEG 4”中，小波成为了其主要的技术。

此外，小波变换还可以应用于许多其他的领域，如信号分析、静态图像识别、量子场论、地震勘探、声音压缩与合成、视频图像分析、雷达、CT 成像、彩色复印、流体湍流、天体识别、计算机视觉和分形力学等领域。总之，能使用傅立叶分析的地方，都可以进行小波分析，其应用前景非常广泛。

5.1.1 连续小波变换的定义

小波分析把一个信号分解成由基本小波（小波母函数）$\psi(t)$经过移位和缩放后的一系列小波，因此，小波是小波变换的基函数。在给

出小波变换的定义之前，需要解释空间$L^1(R)$和$L^2(R)$的含义。$L^1(R)$是指绝对可积函数空间（L表示线性空间，R表示自变量为实数，但函数值可以为复数），即：

$$若\ f(t)\in L^1(R)，\ 则\ \int_{-\infty}^{+\infty}|f(t)|dt<+\infty \tag{5-1}$$

$L^2(R)$是指能量有限函数空间（也是线性的），即：

$$若\ f(t)\in L^2(R)，\ 则\ \int_{-\infty}^{+\infty}|f(t)|^2 dt<+\infty \tag{5-2}$$

下面引出连续小波变换的定义。对$\forall\psi(t)\in L^2(R)$，若其傅立叶变换$\hat{\psi}(\omega)$满足

$$C_\psi=\int_{-\infty}^{+\infty}\left|\hat{\psi}(\omega)\right|^2|\omega|^{-1}d\omega<\infty \tag{5-3}$$

则称$\psi(t)$是一个基本小波、母小波或小波母函数（简称为小波函数），而称

$$\psi_{a,b}(t)=\frac{1}{\sqrt{a}}\psi(\frac{t-b}{a})\qquad(a\neq 0,b\in R) \tag{5-4}$$

为由$\psi(t)$生成的依赖于参数a和b的连续小波。实际上，由式（5-3）可知，$\psi(t)$在原点处的傅立叶变换必须为 0，即$\hat{\psi}(0)=0$，因此基本小波$\psi(t)$的积分为 0。小波之所以称之为“小”是指它绝对可积，具有衰减特性。之所以称之为“波”是指它的平均值为 0，具有波动性。

基于上述定义，可以引出如下连续小波变换对：

$$W_f(a,b)=\int_{-\infty}^{+\infty}f(t)\overline{\psi_{a,b}(t)}dt \tag{5-5}$$

$$f(t)=\frac{1}{\sqrt{C_\psi}}\int_{-\infty}^{+\infty}\int_{-\infty}^{+\infty}W_f(a,b)\psi_{a,b}(t)\frac{dadb}{a^2} \tag{5-6}$$

式中，$\overline{\psi_{a,b}(t)}$表示$\psi_{a,b}(t)$的共轭。

5.1.2 离散小波变换的定义

针对尺度参数a和平移参数b可以对连续小波$\psi_{a,b}(t)$和小波变换$W_f(a,b)$离散化。通常，尺度参数a和平移参数b的离散化公式分别取作$a=a_0^j$和$b=ka_0^jb_0$，则离散小波$\psi_{j,k}(t)$可表示为：

$$\psi_{j,k}(t)=a_0^{\frac{-j}{2}}\psi(a_0^{-j}t-kb_0) \tag{5-7}$$

从而离散小波变换对可表示为：

$$W_f(j,k)=\left\langle f(t),\psi_{j,k}(t)\right\rangle=\int_{-\infty}^{+\infty}f(t)\overline{\psi_{j,k}(t)}dt \tag{5-8}$$

$$f(t)=c\sum_{j=-\infty}^{\infty}\sum_{k=-\infty}^{\infty}W_f(j,k)\psi_{j,k}(t) \tag{5-9}$$

式中，$\langle\cdot,\cdot\rangle$为内积操作，$c$是与信号无关的常数，对应于式（5-6）中的$C_\psi^{-1/2}$。

当离散化参数$a_0=2$和$b_0=1$时，对母小波$\psi(t)$作二进伸缩和平移（$a=2^j$，$b=2^jk$，$j,k\in Z$），可得到如下二进小波(Dyadic Wavelet)：

$$\psi_{j,k}(t)=2^{\frac{-j}{2}}\psi(2^{-j}t-k) \tag{5-10}$$

5.1.3 图像的小波分解

在数字图像处理技术中，当图像经过一次离散小波变换后，会将原始图像划分成4个子带：一个低频子带LL1（即垂直和水平方向的低通子带）；一个高频子带 HH1（即垂直和水平方向的高通子带）；两个中频子带 LH1（即水平方向的低通和垂直方向的高通子带）和HL1（即水平方向的高通和垂直方向的低通子带）。若再对低频子带LL1进行分解，又可以得到更低分辨率的4个子带LL2，LH2，HL2，HH2，如此反复可以对图像进行多次小波分解。图5-1为一个二级小

波分解的示意图。图 5-2 是对大小为 256×256 的灰度图像 Lena 进行二级小波分解后的结果。由图可见，LL 子带图像集中了原始图像的绝大多数能量，称为原始图像的逼近子图。子带图像 HL、LH 和 HH 分别保持了原始图像的垂直边缘细节、水平边缘细节和对角边缘细节，它们刻画了图像的细节特性，称为细节子图。逼近子图具有较强的抵抗外来影响的能力，稳定性较好；边缘细节子图易受外来噪声、图像处理操作等的影响，稳定性差。

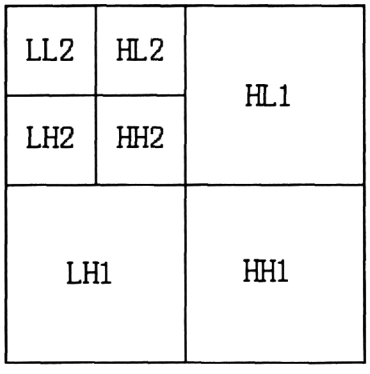


图 5-1 二级小波分解示意

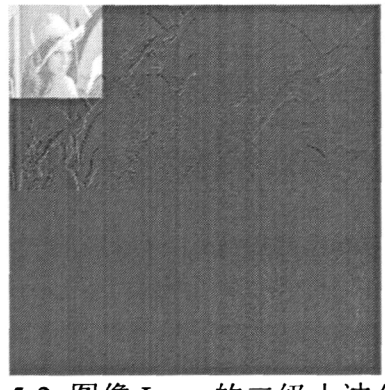


图 5-2 图像 Lena 的二级小波分解

5.2 基于超混沌和 HVS 的小波域盲水印算法

5.2.1 超混沌加密与解密

近年来，混沌特性在图像处理领域得到了较广泛的认识，并提出了一些基于混沌加密的数字水印算法，大部分用于水印图像加密的混沌模型都是一维离散模型，具有密钥空间太小的缺陷。而超混沌随机性好、可确定再生密钥空间较大的特性使其在图像加密的应用中受到了重视，基于超混沌的图像加密算法得到了广泛研究[41,42]。本文采用的二维超混沌系统形式如下：

$$\begin{cases} x(n+1) = a_1 y(n) + a_2 y^2(n) \\ y(n+1) = a_3 x(n) + a_4 y(n) \end{cases} \tag{5-11}$$

当$a_1=1.66$，$a_2=-1.3$，$a_3=-1.1$，$a_4=0.1$时，系统进入超混沌状态，图 5-3 给出对应该组参数的超混沌吸引子：

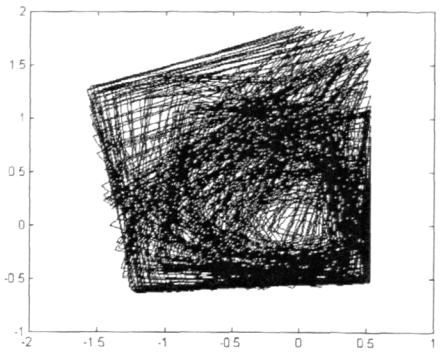


图 5-3　超混沌吸引子

显然，由式（5-11）得到的实数值超混沌序列不宜直接应用于图像加密，而且理论研究表明，这种无误差的平凡混沌加密方法是可破解的。设水印$W(i,j)$是$N\times N$的二值图像，水印图像的加密方法如下：

（1）给定初始条件$x(0)$和$y(0)$，由式（5-11）生成超混沌序列后，去掉初始段，分别取$x(n)$，$y(n)$中长为 N 的一段，初始条件和所选序列的起始点位置作为密钥使用；

（2）将这两段长为 N 的实数值超混沌序列阈值化为[0，1]的二值序列$X(i)$和$Y(j)$；

（3）水印图像加密算法中采用的加密阵列由阈值化后的二值序列进行向量相乘得到：

$$C(i,j)=X(i)^{T}Y(j) \tag{5-12}$$

（4）用生成的加密阵列对水印图像进行异或加密，方法如下：

$$W^{*}(i,j)=C(i,j)\oplus W(i,j) \tag{5-13}$$

其中$W^{*}(i,j)$为加密后的水印图像。

（5）重复步骤（1）到（4），重复次数也作为密钥使用。

图像解密是加密的逆过程，只需根据密钥将生成的加密阵列与加密后的水印图像进行异或即可。图 5-4 演示了图像的超混沌加密与解密。

(a) 水印图像 (b) 加密图像 (c) 解密图像 (d) 错误密钥解密图

图 5-4 超混沌加密解密

5.2.2 人类视觉系统（HVS）模型

前面已经提到过，图像经过离散小波变换可分成 4 个子带，1 个低频子带和 3 个高频细节子带，低频子带还可以继续分解，为了方便描述，我们将一个 4 级小波分解的示意图表示如下：

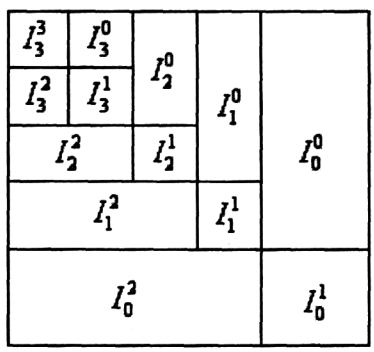


图 5-5 四级小波分解示意图

定义I_l^θ为第l层小波变换θ方向的子带，$l=0,1,2,3$、$\theta=0,1,2,3$，则本文采用的 HVS 模型如下：

（1）人眼对不同亮度区域的噪声敏感性不同，对很暗或很亮的区域的噪声不敏感，设分解层l中某空间位置(i,j)处的亮度因子为$L(l,i,j)$，则$L(l,i,j)$可由式（5-14）估计：

$$L(l,i,j)=\frac{1}{256}I_3^3(1+[\frac{i}{2^{3-l}}],1+[\frac{j}{2^{3-l}}]) \qquad (5\text{-}14)$$

（2）人眼对图像纹理区域的噪声不敏感。令$T(l,i,j)$为纹理掩盖效应的因子，用不同细节子图局部均值的平方和低频子带的方差两部

分进行刻画，分别由像素(i,j)处的2×2的邻域计算，计算方法如式（5-15）所示：

$$T(l,i,j)=\sum_{k=0}^{3-l}\frac{1}{16^k}\sum_{\theta=1}^{3}\sum_{x=0}^{1}\sum_{y=0}^{1}[I_{k+l}^{\theta}(y+\frac{i}{2^k},x+\frac{j}{2^k})]^2 \\ *Var\{I_3^3(1+y+\frac{i}{2^{3-l}},1+x+\frac{j}{2^{3-l}})\} \tag{5-15}$$

由于水印嵌入到第l层后，嵌入水印的位置系数值已经发生改变，在提取水印时，再次计算的纹理掩盖因子与水印嵌入前相比改变很大，会影响水印提取的准确性，因此，在计算纹理掩盖效应因子时只考虑第l层之后的细节子图局部均值的平方和低频子带的方差。

由以上公式可以看出，该HVS模型考虑了人类视觉系统对亮度、纹理复杂度的掩盖效应，为水印的嵌入位置提供了依据。文献[43]提出了一种基于HVS中亮度特性的小波域水印算法，但没有考虑图像的纹理掩蔽特性。文献[44]也采用了HVS模型，但将水印嵌入到第一级小波变换的高频部分，水印对JPEG压缩的鲁棒性不强。本文算法结合式（5-14）和式（5-15）进行系数的选择，将水印嵌入到亮度因子与纹理掩盖因子相对较大的区域。

5.2.3 数字水印的嵌入

宿主图像经过四级小波变换之后，将$N\times N$的加密水印$W^*(i,j)$分成W_1和W_2两部分，分别嵌入到第三级小波变换的垂直细节子带I_2^2和水平细节子带I_2^0中，以I_2^2为例，水印的嵌入规则如下：

（1）根据式（5-14）和式（5-15）求出I_2^2系数的亮度因子和纹理掩盖因子，则图像对噪声的视觉掩盖特性值可以由下式来表示：

$$J(l,i,j)=L(l,i,j)T(l,i,j) \tag{5-16}$$

（2）由于并未考虑第l层的细节子图局部均值的平方，I_2^2中每2×2的块视觉掩盖特性值是相同的，选择前$N\times N/2$个视觉掩盖特性值最大的块进行水印的嵌入，水印嵌入到块中左上角的系数上。

（3）设嵌入点的坐标为(p,q)，位于该点的小波系数为$f(p,q)$，计算以(p,q)为左上角的2×2的系数块中除嵌入点外各点的绝对值的均值m，嵌入方法如下：

1）水印为 1 时：

若$|f(p,q)|<m$，则$f(p,q)=sign(f(p,q))\cdot\beta_1\cdot m$；

否则，$f(p,q)=\beta_1\cdot f(p,q)$。

2）水印为 0 时：

若$|f(p,q)|<m$，则$f(p,q)=\beta_2\cdot f(p,q)$；

否则，$f(p,q)=sign(f(p,q))\cdot\beta_2\cdot m$。

其中，$\beta_1>1$、$\beta_2<1$为嵌入强度因子，$sign(\ )$为符号函数。

（4）利用小波逆变换进行小波重构，生成含水印图像。

5.2.4 数字水印的提取

I_2^2和I_2^0子带水印信息的嵌入方法是一样的，以I_2^2为例，水印的提取步骤如下：

（1）含水印图像四级小波变换后，利用与嵌入相同的方法计算I_2^2的视觉掩蔽特性值，找出水印嵌入点的位置(p,q)。

（2）计算以(p,q)为左上角的2×2的系数块中除嵌入点外各点的绝对值的均值m，水印提取规则为：

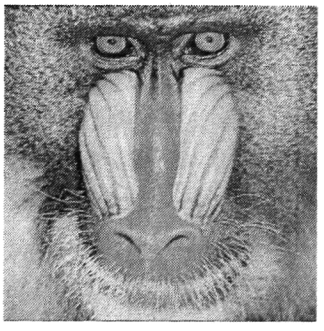
若$|f(p,q)|>m$，则$W_1^{'}=1$；

若$|f(p,q)|<m$，则$W_1^{'}=0$。

同理可以由I_2^0中提取出水印$W_2^{'}$，合并$W_1^{'}$和$W_2^{'}$，得到提取出的加密水印$W^*(i,j)$，使用密钥对$W^*(i,j)$解密后即得提取出的水印$W^{'}(i,j)$。

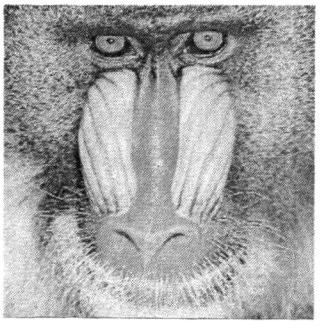
5.2.5 实验结果与分析

仿真实验在MATLAB7.0平台上进行，实验用的宿主图像采用标准图像库中512×512的Lena、Pepper、Plane、Baboon、Boat五张图片，而水印图像则使用32×32的二值图片。对含水印图像的质量评估除了采用人眼主观测试之外，还可使用峰值信噪比*PSNR(dB)*来度量，提取出的水印则用归一化互相关系数*NC*来评价。图片Lena、Pepper、Plane、Baboon、Boat 嵌入水印后的含水印图峰值信噪比分别为40.4978dB、38.4084dB、37.5038dB、41.2229dB、38.5676dB。



（a）原始载体图像　　（b）原始水印图像

图 5-6 原始载体与原始水印图像



（a）PSNR=41.2229　　（b）NC=1

图 5-7 嵌入水印后的图像和提取出的水印

图 5-6（a）是原始载体图像 Baboon，图 5-6（b）为原始的二值水印图像，图 5-7（a）是载体图像 Baboon 嵌入水印后的含水印图像，图 5-7（b）为从中提取出的水印，其归一化互相关值为 1。

对含水印图像进行攻击实验的类型有：均值为 0，方差为 0.001 的高斯噪声；0.01 的椒盐噪声；3×3的中值滤波；50%的剪切；放大两倍再缩小为原来的尺寸；逆时针旋转2°。表 5-1 为攻击实验的数据结果，表中的数值为攻击后提取出的水印的归一化互相关系数。对含水印图像进行 JPEG 压缩处理，不同压缩率下由各图像中提取出的水印归一化互相关系数由表 5-2 给出。

表 5-1 攻击实验结果

图像名称	Lena	Pepper	Plane	Baboon	Boat
高斯噪声	0.8193	0.8514	0.8273	0.8164	0.8247
椒盐噪声	0.8076	0.8270	0.7993	0.8321	0.8036
中值滤波	0.7682	0.7639	0.7643	0.7614	0.7504
剪切	0.8460	0.8276	0.8436	0.8729	0.8669
缩放	1	1	1	1	1
旋转	0.7569	0.7617	0.7674	0.7707	0.7691

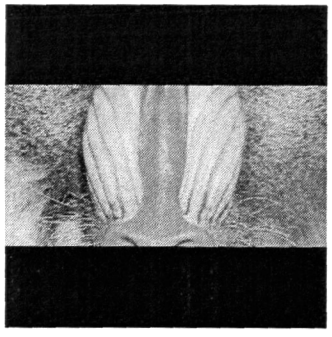
表 5-2 JPEG 压缩实验结果

质量因子	压缩比	各图像的归一化互相关系数值				
		Lena	Peppers	Plane	Baboon	Boat
90	3:1	0.8969	0.9405	0.9115	0.9579	0.9124
70	6:1	0.8667	0.8908	0.8803	0.9078	0.8752
50	8:1	0.8418	0.8613	0.8576	0.8922	0.8691
30	11:1	0.7879	0.8011	0.8318	0.8540	0.8394
10	22:1	0.7398	0.7246	0.7293	0.7877	0.7757

由表 5-1、表 5-2 可以看出，算法对常见的图像处理操作尤其是缩放和剪切具有较好的鲁棒性，图像的缩放对水印提取基本上没有影响，含水印图像剪切掉一半之后，仍然能正确的提取出水印。同时，

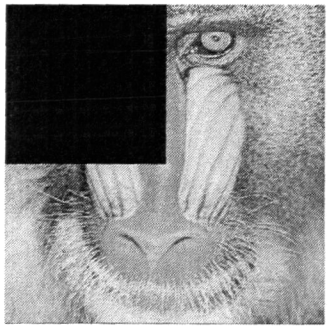
分析实验数据可以看出，对亮度偏大或纹理比较复杂的图像，如Pepper、Baboon，算法的鲁棒性比其他相对平滑的图像更好一些。

为了更好的说明算法的有效性，这里贴出部分对含水印图像Baboon进行攻击的实验结果。图5-8和图5-9是对含水印图像进行剪切攻击的结果，图5-10和图5-11是对含水印图像添加高斯噪声的结果，图5-12和图5-13是对含水印图像添加椒盐噪声的结果，图5-14至图5-17是对含水印图像进行JPEG有损压缩后的结果。



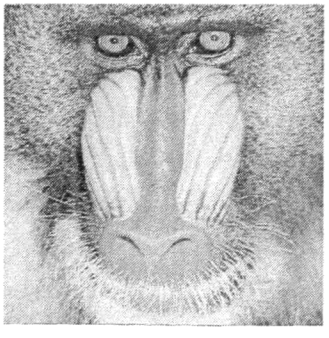
(a)PSNR=7.2699dB　　(b)NC=0.8729

图5-8 对含水印图像进行50%的剪切



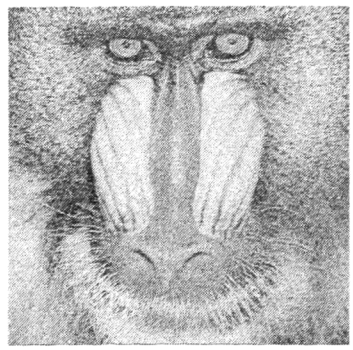
(a)PSNR=10.5887 dB　　(b)NC=0.9271

图5-9 对含水印图像进行25%的剪切



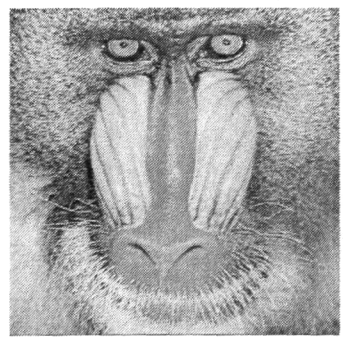
(a)PSNR=28.2343dB　　(b)NC=0.8624

图5-10 对含水印图像添加0.001的高斯噪声



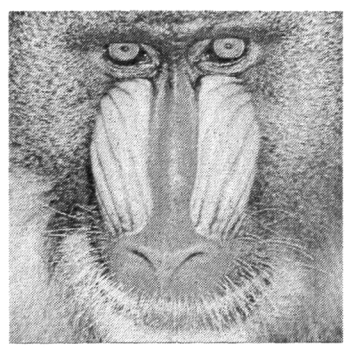
(a)PSNR=18.4711dB (b)NC=0.7709

图5-11 对含水印图像添加0.01的高斯噪声



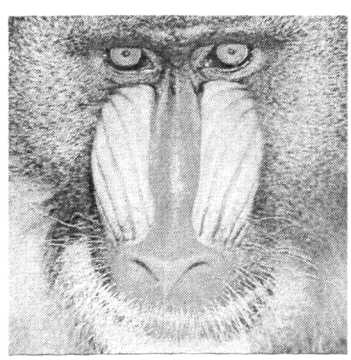
(a)PSNR=33.3067dB (b)NC=0.9635

图 5-12 对含水印图像添加 0.001 的椒盐噪声



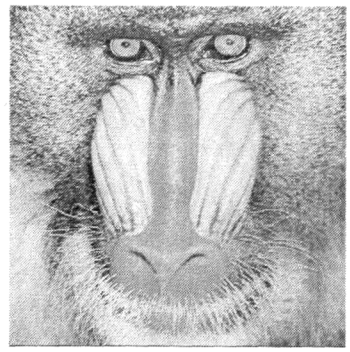
(a)PSNR=24.1383dB (b)NC=0.8501

图 5-13 对含水印图像添加 0.01 的椒盐噪声



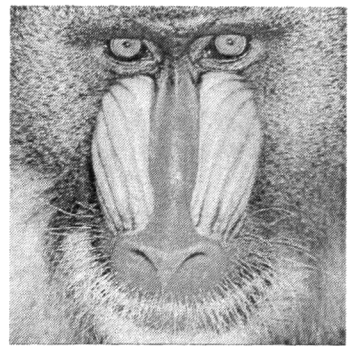
(a)PSNR=31.0971dB (b)NC=0.9231

图 5-14 对含水印图像进行 80%的 JPEG 压缩



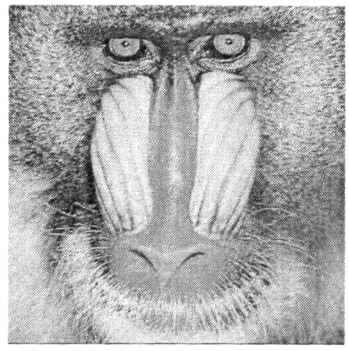
(a)PSNR=29.2669dB (b)NC=0.9078

图 5-15 对含水印图像进行 70%的 JPEG 压缩



(a)PSNR=28.0862dB (b)NC=0.8970

图 5-16 对含水印图像进行 60%的 JPEG 压缩



(a)PSNR=26.5077dB (b)NC=0.8516

图 5-17 对含水印图像进行 40%的 JPEG 压缩

本章提出了一种基于超混沌和人类视觉系统的小波域盲水印算法，利用 HVS 模型选择水印嵌入点的位置，将水印嵌入到图像小波变换后的中频系数上，水印提取时无须原始宿主图像的参与。由攻击实验结果可以看出，算法具有良好的透明性和鲁棒性，具有一定的实用价值。

第6章　总结与展望

数字水印技术是一门新兴的边缘科学，它涉及到通信与信息理论、图像与语音处理、信号检测与估计、数据压缩技术、人类视觉与听觉系统、计算机网络与应用、密码学等多种学科的知识。虽然近几年来在理论和应用中取得了巨大的发展，但是到目前为止尚未形成一个完整的理论体系，特别是没有一个统一的评判标准，仍有许多尚未解决的问题。可以说，数字水印技术是一个充满活力但有待开拓的研究领域，而国内对于这一问题的研究还不深入。

本文围绕静态图像对变换域内的数字水印技术进行了深入的研究。归纳起来，本文所作的工作主要包括以下几个方面：

(1)查阅了大量有关数字水印技术的国内外文献，对目前数字水印技术的发展状况，包括数字水印的基本特征及分类，数字水印系统的基本框架和基本问题以及目前的一些主要算法进行了论述。

(2)研究了混沌基础理论，探讨了各种图像加密技术在数字水印中的应用。

(3)研究了离散余弦变换、离散小波变换理论及其在数字水印领域的应用。

(4)研究了人类视觉系统的特性。

(5)提出了一种基于DCT域的灰度级盲水印算法及一种基于超混沌和人类视觉系统的小波域盲水印算法。设计程序实现了上述两种算

法，并对算法进行了各种攻击实验，取得了大量的实验结果，证明算法的有效性。

数字水印技术作为版权保护的主要手段，正得到广泛的研究与应用。然而，由于这一课题牵涉众多的学科领域，对这个较新领域的研究还没有形成一个全面而统一的标准，数字水印系统的理论基础仍然很弱，缺乏公平统一的水印性能测试与评价体系。应该注意到，数字水印要得到更广泛的应用必须建立一系列的标准或协议，如加载或嵌入数字水印的标准、提取或检测数字水印的标准、数字水印认证的标准等等都是急需的，因为不同的数字水印算法如果不具备兼容性，显然是不利于推广数字水印的应用的。同时，需要建立一些测试标准，如 Stir Mark 几乎已成为事实上的测试标准软件，用以衡量数字水印的稳健性和抗攻击能力。这些标准的建立将会大大促进数字水印技术的应用和发展。

近年来，随着小波分析技术在图像处理应用上取得的新进展以及 JPEG2000 采用基于小波的压缩算法，基于小波变换的数字水印技术将会是数字水印算法研究的热点。另外，最近比较流行的零水印技术，由于突破了传统的水印嵌入式思维，采取提取式嵌入的方法，对原始图像没有任何损坏，也是目前水印研究中的一个热点。随着各大研究机构对此项技术研究的不断深入，数字水印技术必会向其它技术一样将形成统一的国际标准，并得到广泛的应用。

数字水印技术是一个新兴的正处于发展上升期的研究领域，还有许多未触及的研究课题，现有算法需要进一步的改进和提高，理论算

法如何变成商业应用，视、音频数字水印技术，新方法在数字水印技术中的应用，这些都是值得研究的课题，在今后的研究中将作进一步的探讨。

参考文献

[1] F. A. P. Petitcolas, R. J. Anderson, M. G. Kuhn. Information Hiding-A Survey[J]. Proceedings of IEEE, 1999, 87(7): 1062-1078.

[2] G. Voyatzis, I. Pitas. The Use of Watermarks in the Protection of Digital Multimedia Products[J]. Proceedings of the IEEE, 1999, 87(7): 1197-1207.

[3] R. Barnett. Digital Watermarking: Applications Techniques and Challenges[J]. Electronics & Communication Engineering Journal, 1999, 11(4): 173-183.

[4] J. M. Acken. How Watermarking Adds Value to Digital Content[J]. Communications of the ACM, 1998, 41(7): 74-77.

[5] 王炳锡，陈琦，邓峰森. 数字水印技术[M]. 西安：西安电子科技大学出版社，2003: 13-17.

[6] I. J. Cox, M. L. Miller. The first 50 years of electronic watermarking[J]. Journal of Applied Signal Processing, 2002, (2):126-132.

[7] A. Z. Tirkel, G. A. Rankin, R. van S. Chyndel. Electronic Watermark[C]. Proceedings of Digital Image Computing Technology and Applications-DICTA 93. Sidney: Macquarie University, 1993: 666-673.

[8] G. A. Rankin, A. Z. Tirkel, N. Mee, et al. A Digital Watermark[C].

Proceedings of IEEE International Conference on Image Processing. Austin, 1994, (2): 86-90.

[9] I. J. Cox, et al. Secure Spread Spectrum Watermarking for Multimedia[R]. IEEE Transaction on Image Processing, 1997, 6(12): 1673-1687.

[10] I. Pitas. A Method for Signature Casting on Digital Images[C]. IEEE International Conference on Image Processing, 1996, (3): 215-218.

[11] 汪小帆，戴跃伟，茅耀斌. 信息隐藏技术-方法与应用[M]. 北京：机械工业出版社，2001: 18-176.

[12] 刘振华，尹萍. 信息隐藏技术及其应用[M]. 北京：科学出版社，2002: 1-149.

[13] 孙圣和，陆哲明，牛夏牧. 数字水印技术及应用[M]. 北京：科学出版社，2004: 32-37.

[14] D. J. Fleet, D. J. Heeger. Embedding Invisible Information in Color Images[J]. Proceedings of IEEE International Conference on Image Processing, 1997,(1): 532-535.

[15] D. Kundur, D. Hatzinakos. Digital Watermarking for Telltale Tamper: Proofing and Authentication[C]. Proceedings of the IEEE Special Issue on Identification and Protection of Multimedia Information, 1999, 87(7):1167-1180.

[16] W. Bender, et al. Techniques for Data Hiding[J]. IBM System Journal, 1996, 35(3&4):313-336.

[17] L. Boney, A. Tewfik, K. Hamdy. Digital Watermarks for Audio Signals[J]. IEEE Int. Conf. on Multimedia Computing and Systems, 1996, (1):473-480.

[18] 张春田，苏育挺. 信息产品的版权保护技术-数字水印[J]. 电信科学, 1998, 14(12): 15-17.

[19] 孙圣和，陆哲明. 数字水印处理技术[J]. 电子学报, 2000, 28(8): 85-90.

[20] 周利军，周源华. 基于 m 序列的多重图像水印[J]. 上海交通大学学报，2001，35(9):1317-1320.

[21] 钟伟，马希俊，余松煌. 一种使用 Legendre 阵列的图像水印[J]. 通信学报，2001，22(1):1-6.

[22] S. Tsekeridou, et al. Bernoulli Shift Generated Chaotic Watermarks: Theoretic Investigation[J]. IEEE International Conference on Acoustics, Speech, and Signal Processing, 2001, (3): 1989-1992.

[23] A. Nikolaidis, I. Pitas. Comparison of different chaotic maps with application to image watermarking[J]. IEEE International Symposium on Circuits and Systems, 2000, (5): 509-512.

[24] 胡岚，周琳娜，郭云彪.信息隐藏分析与攻击[C]. 第四届信息隐藏全国学术研讨会论文集. 北京: 机械工业出版社，2002: 34-41.

[25] J. K. O. Ruanaidh, W. J. Dowling, F. M. Boland. Rotation, Scale and Translation Invariant Spread Spectrum Digital Image Watermarks[J]. Signal Processing, 1998, 66(3): 303-317.

[26] F. Petitcolas, R. Anderson, M. Kuhn. Attacks on Copyright Marking Systems[J]. Computer Science Information Hiding. 1998, (5): 218-238.

[27] 孙鑫，易开祥，孙优贤. 基于混沌系统的图像加密算法[J]. 计算机辅助设计与图形学学报，2002，14(2):136-139.

[28] 丁玮，齐东旭. 数字图像变换及信息隐藏与伪装技术[J]. 计算机学报，1998，21(9):838-843.

[29] 李国富. 基于正交拉丁方的数字图像置乱方法[J]. 北方工业大学学报，2001，13(1):14-16.

[30] E. N. Lorenz. 混沌的本质[M]. 北京:气象出版社，1997: 28-37.

[31] R. M. May. Simple Mathematical Model with very Complicated Dynamics[J]. Nature, 1976, 261(2): 459-467.

[32] Hui Xiang, et al. Digital watermarking systems with chaotic sequences[C]. Proceedings of Electronic Imaging Security and Watermarking of Multimedia Contents. San Jose: SPIE, 1999: 449-457.

[33] G. R. Feng, L. G. Jiang, C. He, D. J. Wang. A Novel Algorithm for Embedding and Detecting Digital Watermarks[J]. IEEE International Conference on Acoustics, Speech, and Signal Processing, 2003, (3): 549-552.

[34] 孙伟. 关于 Arnold 变换的周期性[J]. 北方工业大学学报，1999，11(1)：29-32.

[35] 罗军辉，冯平. MATLAB 7.0 在图像处理中的应用[M]. 北京：机械工业出版社，2005: 102-103.

[36] Niu Xiamu, Lu Zheming, Sun Shenghe. Digital Watermarking of Still Images with Gray-level Digital Watermarks[J]. IEEE Trans. on Consumer Electronics, 2000, 46(1):137-145.

[37] L. Yin. Stack Filter Design: A Structural Approach[J]. IEEE Transactions on Signal Processing, 1995, 43(4): 831-840.

[38] P. J. Burt, E. H. Adeison. The Laplacian Pyramid as a Compact Image Code[J]. IEEE Transactions on Communications, 1983, 31(4): 532-540.

[39] I. J. Cox, J. Kilian, T. Leighton, T. Shamoon. Secure Spread Spectrum Watermarking for Images, Audio and Video[C]. IEEE International Conference on Image Processing, Lausanne, Switzerland, 1996, 3: 243-246.

[40] 杨蕊，普杰信，刘敏红，卢振泰，一种基于 DCT 系数特性的盲检水印算法[J]. 计算机应用研究，2006，(2)：243-245.

[41] 李雄军，彭建华，徐宁等，基于二维超混沌序列的图像加密算法[J]. 中国图象图形学报，2003, 8(10): 1172-1177.

[42] 殷红，陈增强，袁著祉，基于超混沌和小波变换的鲁棒性数字水印算法. 控制与决策，2006, 21(9): 1024-1027.

[43] 董彬，林小竹，徐凤，基于人类视觉系统的小波域数字水印算法. 计算机工程[J]，2006, 32(24): 138-143.

[44] V. V. F. Guzman, M. N. Miyatake, H. M. H. Meana. Analysis of a Wavelet-based Watermarking Algorithm[J]. Proceedings of the 14th International Conference on Electronics, Communications and Computers, 2004,(2): 283-287.

攻读硕士期间发表的论文

[1] 赵永，王玲. 基于混沌置乱的 DCT 域灰度级盲水印算法. 信息安全与通信保密，2007，(6)：215-216，219

致　谢

时光飞逝，转眼就要结束三年的研究生生活了。过去的三年里，无论是学业还是社会经验都有了很大的提高，这当中有我自己的努力，但更少不了周围的老师、同学和朋友的帮助。

首先要感谢我的导师王玲教授，三年来，王老师不仅在学业上给予了我悉心的指导和帮助，在生活等各方面也给我无微不至的关怀和照顾。她对学科前沿敏锐的把握能力、严谨的治学态度、积极进取的探索精神、对工作的责任感和积极乐观的生活态度给我留下了深刻的印象，并让我受益匪浅。在此，向我的恩师王玲教授表示我最诚挚的感谢和敬意。

同时，感谢系里的同学们，他们刻苦学习的精神深深影响了我，在我的学习和生活上给予了我很多的帮助。也是他们，让我的研究生生活过得充实而精彩。

还要感谢我的朋友们，他们在我遇到困难时总是能给予我帮助和鼓励，也是他们，教会了我乐观的生活态度。

特别感谢我深爱的家人，正是因为他们的支持和关怀使我能够顺利完成学业，他们在背后的默默支持是我求学的动力。

最后，忠心感谢各位评审专家在百忙之中抽出宝贵的时间来审阅我的论文，感谢各位专家的赐教和指正。