摘 要

随着网络技术和计算机信息技术的飞速发展，人类社会已经进入一个全新的数字信息化时代。以数字媒介为载体的作品由于其具有获取容易、复制简单和传播迅速等优点，极大的丰富了人类的生活。但是利用计算机网络的开放性和共享性所进行的一些恶意的行为，严重的损害了数字作品的创作者和使用者的利益，因此，对多媒体信息的所有者的权益保护问题就成了当今数字技术的一个重要研究课题。

本文主要对静态图像的水印技术进行了研究，主要工作如下：

（1）首先介绍了数字水印的相关概念，研究背景和研究现状。

（2）比较系统的数字水印的定义、分类、水印的应用领域及其数字水印的通用模型，并介绍了数字图像水印常见的攻击方法、评价标准和典型算法。

（3）对小波分析理论做了比较详细的介绍，包括小波的概念，性质，在数字图像处理中的应用以及多分辨率的特性。

（4）分析了 shamir 理论及其门限方案，提出了基于 shamir 理论的小波域数字水印算法，利用秘密共享信息分存的思想将秘密信息嵌入载体图像中。

（5）在该算法上改进了以往采用非盲检测的图像水印方案，设计了基于 shamir 理论的盲检测算法，实验证明：该算法对数字图像水印不仅具有较好的不可见性，而且对图像的噪声、压缩、剪切具有较好的鲁棒性。

（6）为了提高对旋转攻击的鲁棒性，又提出了基于 shamir 理论的 DWT 和 SVD 的水印方案，实验证明：该算法具有很好的鲁棒性。

关键字：数字水印， 奇异值分解， shamir 理论 ，信息分存， 小波变换

ABSTRACT

With the rapid development of networks technology and computer information technology, human society has already entered into a new one era of digital information. With easy access, copying simple and rapid dissemination, the works based on digital media have enriched the people's life enormously. But the benefits of digital works' composers and users are injured seriously because of malicious acts in the opened and shared computer networks. Therefore, the protection problem of the owners having the rights with multimedia information becomes one of the most important research subjects.

In this paper, the static image watermarking techniques are studied, mainly the following:

(1) Introduced the concepts of digital watermarking, research background and the present status.

(2) Compared the definitions, classifications, applications and versatile models in different watermarking system, and introduced some common attack methods, evaluation criteria and typical algorithms in digital watermarking.

(3)A more detailed description, in wavelet analysis theory, was introduced. It is include the concept and properties of wavelets, the application in digital image processing and the features of multi-resolution.

(4) Analyzed the shamir theory and threshold scheme, and proposed DWT-based digital watermarking algorithm. Based on the idea of secret sharing information divided-storage technology, the secret information could be embedded into the carrier images.

(5) Improved the image watermarking scheme in the previous of non-blind detection, and designed a new blind detection arithmetic based on shamir theory. Experiments prove that this algorithm is not only good for the invisibility of digital image watermarking, but also has a better robustness in image noise, compression and cutting.

(6) To improve the robustness of the rotation attack, the scheme of DWT and SVD based on shamir theory was proposed. Experiments show that the algorithm has good robustness.

Key words: Digital watermarking, Singular value decomposition, Shamir theory, Information divided-storage, Wavelet transform

西北大学学位论文知识产权声明书

本人完全了解西北大学关于收集、保存、使用学位论文的规定。学校有权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。本人允许论文被查阅和借阅。本人授权西北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。同时授权中国科学技术信息研究所等机构将本学位论文收录到《中国学位论文全文数据库》或其它相关数据库。

保密论文待解密后适用本声明。

学位论文作者签名：李秋菊　　指导教师签名：

2010年 6月 10日　　年　月　日

西北大学学位论文独创性声明

本人声明：所呈交的学位论文是本人在导师指导下进行的研究工作及取得的研究成果。据我所知，除了文中特别加以标注和致谢的地方外，本论文不包含其他人已经发表或撰写过的研究成果，也不包含为获得西北大学或其它教育机构的学位或证书而使用过的材料。与我一同工作的同志对本研究所做的任何贡献均已在论文中作了明确的说明并表示谢意。

学位论文作者签名：李秋菊

2010年 6 月 10 日

第一章　绪　论

1.1　选题背景

当前的信息安全技术大多以密码学理论为基础，其保护方式都是以通过控制多媒体信息的读取来实现的，即对机密信息进行编码，形成不可识别的密文，使得非法用户不能读取信息。这种方法在一定程度上存在一定的局限性，加密的根本目的是保护信息的安全，随着计算机处理数据能力的提高，通过不断增加密钥的长度来提高系统保密级别的方法变得越来越不可靠，因此保护网络上多媒体信息的安全就不能单纯的靠密码学的安全体制，而要研究新的方法来弥补密码学技术的不足。

信息隐藏技术是一门古老而又崭新的学科，信息隐藏技术与传统的加密技术有着本质的区别。加密技术意在隐藏信息的内容，加密数据在解密之后不再受到保护；而信息隐藏技术的目的是在隐藏信息存在的存在性，从而为数字媒体提供进一步的保护。在实际的应用中，信息隐藏技术与加密技术通常是相互结合使用的。

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。它将特定的标记采用一定的嵌入算法隐藏在数字多媒体载体中，目的就是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，数字水印被视做抵抗多媒体盗版的“最后一道防线”。因此从水印技术自身来说，它具有广泛的应用前景和巨大的经济价值。

1.2　国内外研究现状

1993 年数字水印被提出[1]，正是由于其在信息安全和经济领域上具有极其重要的地位，吸引了来自不同领域的国内外专家学者的目光，世界各国的研究机构和商业集团都积极地参与或投资支持此方面的研究，如 IBM,NEC、HP、INTEL 等许多大公司都参与了这项技术的研究。并且随着大量的人力物力的投入，许多相关的定义、算法、概念和技术不断涌出。在 1994 年的 ICIP’会议上 Van Schyndel 发表了一篇题为“A digital watermark”的文章，该文章中阐述了关于数字水印的一些主要概念。学术界在 1996 年，1998 年，1999 年召开了三次关于信息隐藏学术研讨会，使得数字水印技术成为当前信息科学前沿的一个研究热点。在近几年，国内外关于数字水印的科研论文数量增长迅速，从 1999 年开始，摄影光学仪器工程师学会召开了关于“多媒体内容安全和水印”的研讨

会，在该研讨会上，数字水印越来越受到大家的关注。全部会议论文 33 篇文章中有 18 篇是关于数字水印的研究。在图像水印研究方面，任何的电子图片，无论是 Word 文档、电子邮件、还是出版物，都可以借助于隐藏的标记知道它的原始出处，在现阶段，图像水印的研究主要集中在版权保护和多媒体认证两个方面。

随着信息技术交流的加快和数字水印技术的迅速发展，我国在数字水印技术发展的方面也非常迅速，1999 年 12 月，第一届信息隐藏学术研讨会在北京电子技术应用研究所召开。并且在 2000 年 1 月，多家科研机构参加了由国家“863”智能机专家组和中科院自动化所组织召开的数字水印学术研讨会上，这些都进一步推进了国内数字水印技术的发展，也充分说明了国家对于数字水印这一研究领域的高度重视[2-3]。

在这十几年中，数字水印技术得到蓬勃发展，各种关于水印的技术和算法研究不断涌现，水印的研究可以归结为模型研究，算法研究，攻击研究三个方面，其具体研究内容包括鲁棒性研究，容量研究，认证研究等等。

1.2.1 模型研究

在关于水印的模型研究方面，Mauro Barni 等[4]提出了能够抵抗常见攻击的一种框架模型结构，对水印的攻击研究上了一个新台阶；随后 Ingemar J.Cox 和 Matt L.Miller 提出了水印的盲嵌模型和明嵌模型，更进一步深入的对模型进行了研究[5]，盲嵌模型简单，在提取水印信息的时候，不需要原始载体，但是鲁棒性较差，也就是抗攻击能力较差；明嵌模型是把水印信息堪称载体信息的函数，因此有较强的鲁棒性，能够抵抗常见的攻击测试。

1.2.2 算法研究

随着对数字水印技术研究的深入，现在数字水印的算法层出不穷，这些算法可以归结为空间域算法和频域算法。

（1）空间域算法

早期的空间域算法主要是 LSB 法，它是通过改变图像的最低有效位来实现的。最低有效位方法(LSB)是一种典型的空间域数据隐藏算法，不需要对载体图像进行任何时频变换，它是通过直接修改数字媒体的时域采样值的方法将水印信息隐藏于数字媒体的最不重要比特（LSB）。L. F. Tumer 与 R. G. Van Schyadel 等[6]采用此方法将水印信息隐藏于载体多媒体信息中.， 该方法也是利用原始数据的最低几位来隐藏信息的。Wolfgang 等人[7]将 m 序列产生的伪随机信号以编码形式嵌入到灰度图像数据的 LSB 中，并利用

相关函数嵌入方式改善了检测过程，这种算法的优点是嵌入数据量很大，缺点是对抗攻击缺乏鲁棒性。为了提高时域水印的稳健性, Bender 等[8]提出"Patchwork"算法，其基本思想是嵌入时任意选择 N 对图像像素点，增加图像某一点亮度的同时，降低另一点的亮度值，这样整个图像的平均亮度值保持不变，采用的理论基础是通过改变图像数据的统计特征来嵌入水印，此算法优点是水印的隐藏性较好，但是也有缺点，其缺点是不能抵抗共谋攻击，还有就是隐藏的信息量不大； Fridrich 和 Goljan 等[9]给出了一种具有篡改自修复能力的图像认证算法， Fridrich 提出的方法是将图像块的压缩信息和签名信息隐藏于图像的 LSB 位[25]。Friendman 等[10]人分别提出通过修改最不重要比特（LSB）来嵌入认证信息。Walton 基于此思想将图像分割为大小相同的图像块，然后将 MSB 的求和校验信息作为认证信息经加密后隐藏于图像的 LSB 位[11]。Yeung 等[12]人在嵌入水印前构造一查询表，将嵌入的水印比特与图像像素的灰度值关联起来，这样就不只是局限于 LSB。由于此类技术中每一个图像子块所隐藏的水印信息只与宿主图像块相关，因此如果攻击者得到多幅使用相同密钥或隐藏相同水印的可信图像时，就很容易实施攻击。在空域算法和 shamir 理论相结合方面，牛少彰等[23]提出了基于 shamir 理论的水印算法，将载体图像，在嵌入水印前对水印进行加密，并根据 shamir 理论中的多项式进行水印图像的分存处理，这样对水印图像就进行了二次加密处理，采用够了 LSB 方法进行了水印的嵌入，该算法能够抵抗大面积的剪切攻击。

（2）离散余弦变换（DCT）域方法

Cox 等[13]人首先提出了一种嵌入水印的思想，这一思想也被许多文献所使用，那就是将水印信息嵌入到图像中感知最重要的区域中，这样当攻击者破坏水印的同时必然要破坏图像的重要信息，这样可以防止图像遭到攻击的时候将水印信息也破坏掉。Koch 等[14]人也提出了一种基于 DCT 域的水印算法，该算法具有很好的抗压缩攻击的能力，基本思想是通过修改由伪随机序列所选定的中频系数对差值的方式来嵌入水印。Tao 等[15]人提出了一种自适应的基于 DCT 变换的数字水印技术，该算法具有很好的抗攻击效果，其基本思想是将图像按照噪声敏感特性将其分为六份，然后在每一份中嵌入不同强度的水印信息，该算法对于抗压缩攻击可以借鉴。Swanson 等[16]人提出利用频域伪装技术来改善 DCT 域水印的性能。Podilchuk 等[17]人提出了一种算法，在该算法中利用人眼的视觉模型，在变换域中通过计算临界可见误差 JND(Just Noticeable Difference)的大小的方式来确定水印的最大嵌入大小，该算法具有很好的稳健性和不可感知性，也得到了水印的稳健性和不可感知性的最佳折中。Hernandez 等[18]人结合视觉模型提出了一种

DCT 域盲数字水印技术算法，在该算法中检测水印时不需要原始载体图像，也就是采用盲检测来实现水印的检测。Jian Zhao 等[19-20]人提出了非线性技术在水印技术中的应用，主要介绍了分形、混沌、神经网络这些非线性技术，应用这些非线性技术对水印图像进行加密预处理，大大提高了水印被破解的难度。赵健，周明全等[21]提出了 DCT 变换的数字水印的改进算法，其基本思想是将图像进行 DCT 变换，并将其系数按照对角线图案进行扫描，并将其重新排列为一维向量，按照一定的方式选择部分系数进行水印的嵌入，实验表明该算法具有较好的鲁棒性。

在 DCT 域和 shamir 理论相结合的数字水印算法中，牛少彰等[22]提出了一种在 DCT 域中利用 Shamir 理论对数字水印进行嵌入和提取得算法。基本思想是根据 shamir 理论中的 (t,n) 门限方案，对原始水印图像进行分存处理，在提取的时候结合拉格朗日插值公式，从中提取 $t(t \le n)$ 份子水印即可恢复出原始水印图像。这种秘密共享思想对于剪切攻击具有很好的鲁棒性，甚至可以从攻击者所剪切拼凑作品中恢复出原始水印，进一步增强了版权保护的能力。

（3）离散傅里叶变换（DFT）域水印：

离散傅里叶变换（DFT）方法是将图像进行 DFT 变换，得到其幅频和相频特性，然后选择在相位特性上来嵌入信息，从图像的可理解性角度，相位信息比振幅信息更重要。通常情况下绝大多数的水印算法在经受了几何变换攻击之后，提取出的水印信息都会有所失真。为了改善其稳健性，又根据 Mellin-Fourier 变换具有旋转不变特性，能够抵抗仿射几何变换，Oruanaidh 等人[24]提出了一种用 Mellin-Fourier 变换的方式来嵌入水印，实验表明该算法对于旋转攻击具有很好的鲁棒性。DFT 域水印算法是 DCT 域水印算法基础上的一些改进，由于利用了 DFT 变换的缩放和旋转不变特性，因而这类变换域水印能抵抗图像的 RST 操作。这是针对几何攻击所提出的算法，DFT 算法的优点是可以信号分解为相位信息和幅值信息，具有更丰富的细节信息，对几何失真能够实现较好的稳健性，但是也有其缺点，其缺点是抗压缩的能力比较差。

（4）离散小波变换（DWT）域方法：

现在大多数水印算法都是基于小波变换的水印算法，主要的一个就是是因为 DWT 变换可以比较好的模仿人类视觉系统（Human Visual System）。将小波变换与 DCT 变换和 DFT 变换相比，它具有更好的时频变换特性，并且小波变换还与 JPEG2000 和 MPEG-4 等压缩标准兼容，更加符合人类视觉系统，这些优势大大促进了小波域数字水印的进一

步发展。

Barni 等[25]人把感知模型用到到每一个图像小波系数，从而最大程度地提高了水印能量。Kundur 等[26]人提出了一种基于多分辨层上嵌入水印以及分层的检测方法。Deepa Kunder 等[27-28]中提出了基于小波变换的私有水印和公开水印算法，前者在提取时需要原始图像，是采用的非盲检测方案；后者在提取水印时不需要原始水印，采用的盲检测方案。Zhu 等[29]人基于二维和三维离散小波变换提出了一种图像和视频水印的统一的方法，其特点是可以大大减少了计算量。刘九芬等[30]人研究了水印算法中的小波基的选择问题，得到的结论是：Haar 小波比较适合于数字图像水印。这一点对于在 DWT 域研究水印算法具有极其重要的意思。Jian Zhao 等[31][32]提出了利用神经网络与混沌相结合在小波数字水印算法中进行图像置乱的方法，该算法对水印图像进行了加密处理，使水印信息不容易被破解。

周欣利用 Shamir 理论的信息分存思想，选择小波变换的各个子带作为水印的嵌入区域，在提取算法中，用类似汉字描红的方法取代 Shamir 理论中阐述的拉格朗日插值来恢复原始水印[33]。这种算法在对抗某些图像处理的攻击有良好的鲁棒性，并且提高了计算速度，但是这种算法在水印的盲检测方面还要进一步研究。

1.2.3 攻击研究

尽管目前数字水印算法很多，新的算法层出不穷，但是其鲁棒性仍然难以达到实际应用的要求，因此通过对现有的水印系统进行攻击分析，找出弱点所在，进而加以改进，是可以提高系统鲁棒性。Xinpeng Zhang 等[35]提出了一种基于伪造的水印算法，并对该攻击算法提出了相应的解决方案。袁源等[34]提出了一种新的方法：带确定性的数字水印攻击方法，并提出了相应的解决方案。王慧琴等[36]在对常见的水印攻击的研究的基础上提出了一些反攻击对策，并建立了水印攻击规则库和质量评估指标库。

1.3 课题主要研究工作

本文是在导师主持的陕西省自然科学基金“Shamir 理论在图像混沌水印中的应用研究”(2006F42)资助下完成的. 本课题的工作是导师前期工作基础上的延续.

本课题的目标是：根据水印系统的基本框架，在水印嵌入部分，在保证水印信息不可见的前提下，以 Shamir 理论中所阐述的关于秘密信息分存的思想和现有小波域数字水印技术作为基础，结合数字图像经过小波变换后的特点提出相应的数字水印算法。课

题将从水印信息的预处理、嵌入与检测和攻击测试这三个方面开展对图像数字水印的研究，并给出具体的算法，要求该水印算法具有很好的不可见性和良好的鲁棒性。

1.4 论文组织结构

本文以灰度图像作为原始载体图像，二值图像作为原始水印图像，在小波域中实现图像数字水印的隐藏和提取。本论文全文共有五章，各章节的具体安排如下：

第一章 绪论，介绍本课题的选题背景、国内外研究现状和应用领域。

第二章 介绍数字水印的基本概念。

第三章 介绍小波变换基本理论及其应用，并介绍图像置乱的方法

第四章 介绍了 shamir 理论相关概念，并提出了基于 shamir 理论的小波域盲水印算法，提出的算法进行了实验测试，并作出了相关的性能分析。

第五章 提出了基于 shamir 理论的小波域和奇异值分解的数字水印方案，并对提出的算法进行实验测试，得出相关结论。

第二章 数字水印技术理论

2.1 信息隐藏

2.1.1 信息隐藏的含义

信息隐藏和密码学一样，属于信息安全学的分支，是与密码学、多媒体、计算机网络等学科紧密相关的交叉学科，但又与传统密码学有所不同，传统密码学主要是将敏感信息进行特殊的处理，从而形成不可识别的密文进行传递，但是当受到攻击之后，密文就没有了保密的作用，信息隐藏主要是借助于公开载体信息，并将其秘密信息隐藏在公开的载体信息里面，以公开载体信息为媒介实现秘密信息的传输。另一方面，在传统密码学中，攻击者一般采用非法拦截的方法得到密文，由于得到的密文是一些难理解信息，攻击者会试图破译密文并将其恢复成明文，或者对密文进行恶意的攻击，这样就会导致密文可能恢复不出来。在信息隐藏学中，是将一个秘密的信息隐藏于原始的多媒体载体信息之中，利用人类的视觉系统对数字信号的感觉上的冗余，从而使隐藏的秘密信息具有不可见性。利用人眼根本就看不出原始载体信息的改变程度，在一定程度上，并不会改变载体信息的基本的特征和使用价值，所以用信息隐藏的方法和用密码加密的方法进行保密通信各有自己的优势。

在信息隐藏学中，被隐藏的敏感信息称为隐秘信息，称公开信息载体信息.信息隐藏技术分类如图 1 所示[37]。

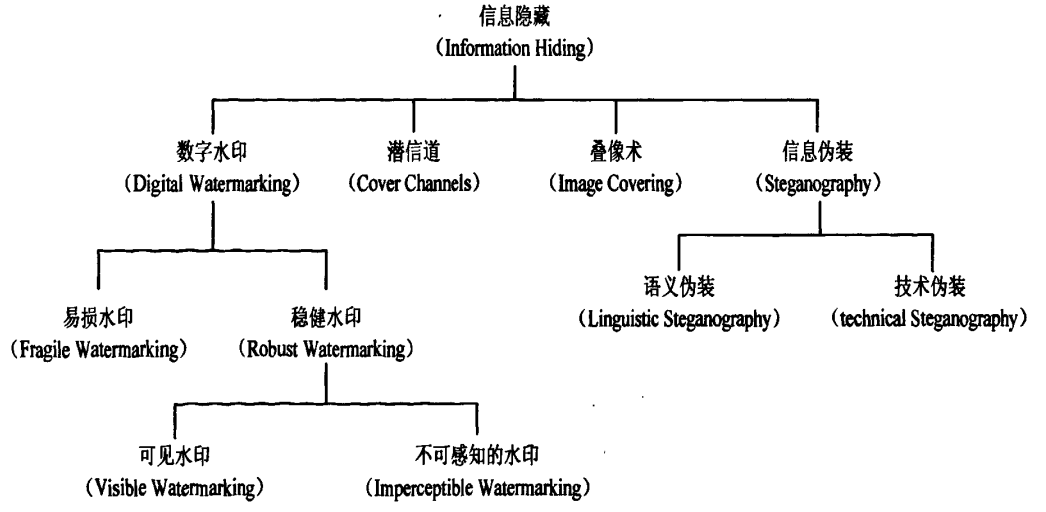


图 1 信息隐藏技术分类

信息隐藏系统的一般化模型[37]可以用图 2 表示，系统主要包含一个嵌入过程和提取

过程。嵌入过程是指信息隐藏者利用嵌入密钥，将嵌入对象加载到载体图像中，从而生成隐藏对象。提取过程是指利用密钥从接收到的隐藏图像中恢复嵌入对象。这样，在密钥未知的情况下，第三者很难从隐藏对象中得到或者删除秘密信息。

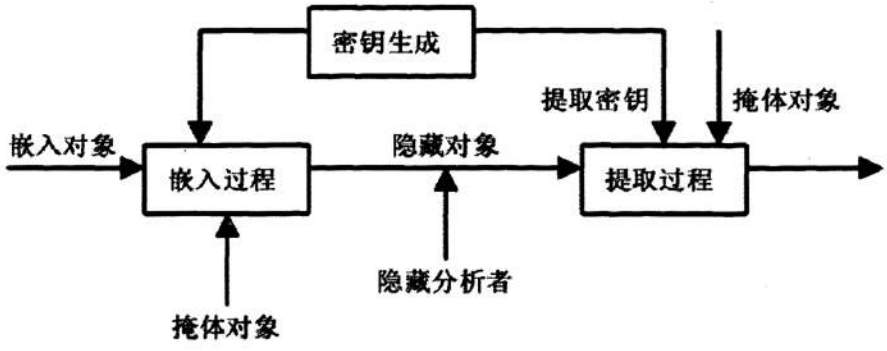


图 2　信息隐藏系统的一般化模型

2.1.2　数字图像

图像是用各种观测系统以不同手段和形式观测世界而获得的，可以直接或间接的作用于人眼并产生视觉的实体。

一般从客观景物所得到的图像是二维的，一幅图像可以用二维函数 $f(x,y)$ 来表示，也可看坐是一个二维数组，x 和 y 表示二维空间 XY 中的一个坐标点的位置。例如常用的图像是灰度图像，此时 f 表示灰度值，它常对应客观景物被观察到的亮度。

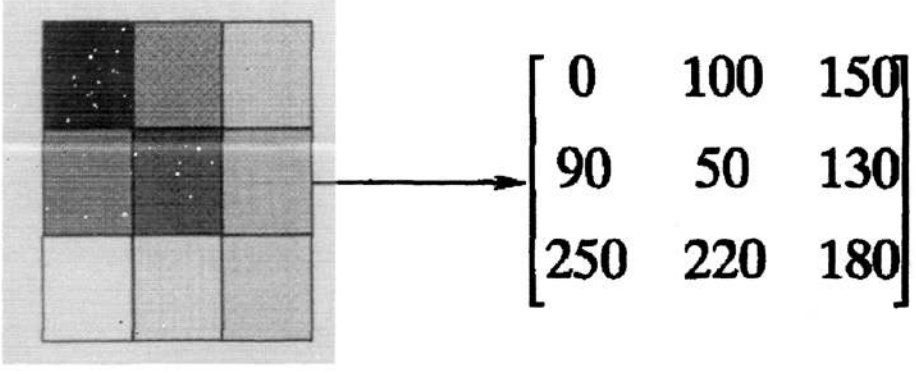


图 3　灰度图像的矩阵对照图

2.2 数字水印理论

2.2.1 数字水印的概念及特征

作为信息隐藏技术的一个重要分支，数字水印技术是其一个很重要的研究方向，在信息隐藏技术的基础上，引出了数字水印的许多概念和技术。

数字水印（Digital Watermark）技术是指通过一定的算法将一些标识信息隐藏到数字多媒体数据中，隐藏之后不影响原多媒体的使用价值，这种标记通常是不可见的，不能被人的知觉系统察觉到，只有通过专用的检测器或阅读器才能提取[30]。这种被嵌入的标记（水印）可以是一段文字、序列号、图像等。隐藏的信息能成为数字水印至少应具有以下特征[38]：

（1） 保真度

保真度也叫不可感知性。水印的嵌入不能影响多媒体数据的正常使用，不能降质，不能改变数据文件的大小：即不带水印的作品和带水印的作品呈现给用户时，两者之间感觉上的相似程度，即水印是不可见的，但也存在可见水印。大多数水印算法中要求水印信息不可感知性，在本设计中要求水印不可见。

（2） 鲁棒性

水印的鲁棒性也叫水印的稳健性，是指水印系统能抵抗一般的数字信号处理和恶意的攻击。数字在使用的过程中不可避免的的一些处理比如压缩、去噪等，对这样的处理之后的作品要求依然能够检测出水印信息。同时要求嵌入水印后的载体图像能够承受大量的物理和几何失真，如嵌入水印后的载体在经受了滤波、数/模与模/数转换、旋转，重采样、剪切、位移、尺度变化以及有损压缩编码、中值滤波、图像尺度变换、图像增强等，稳健的水印算法应该仍然能够从含水印的载体中提取水印信息，因而鲁棒性是数字水印的主要特点之一。

（3） 确定性

水印的确定性要求从嵌入水印后的载体中提取水印信息是很容易的，即使是图像遭到了破坏，也应该很容易从中提取出水印信息，而且在提取时不需要消耗太大的人力无力，也不需要另外的专业设备或专门的技术，提取的过程应该是很简单的。

（4） 安全性：是指将水印信息隐藏于目标数据的内容之内，而非文件头等处，防止数据因为格式转换而遭到破坏。也就是说数字水印的信息应该是难以篡改或伪造的。所以要求即使一般用户知道该数字作品中隐藏有水印，用一般的方法也无法删除或

篡改水印信息。

（5） 无歧义性：要求嵌入的水印信息必须是能够足以证明该多媒体内容所有者的标志信息，该标志信息是确定的，这样有利于解决版权纠纷，保护数字产品的所有者的合法权益，进而实现版权的保护。

（6） 通用性：任何的水印算法不可能适合所有的多媒体信息，所以希望有一种好的水印算法能尽可能的适合多钟数字媒体。

2.2.2 数字水印的分类

从不同的应用角度对水印算法进行分类，可以分为以下几类：

（1）按特性划分：将数字水印分为鲁棒性（稳健性）数字水印和脆弱数字水印两类。

（2）按检测过程分：将数字水印划分为明文水印和盲水印。盲水印在检测过程中不需要原始数据信息，只需要密钥就能提取隐藏的水印信息；明文水印在检测过程中，需要有原始数据。两者的最大的区别是明文水印的鲁棒性比较强，盲水印抗攻击能力比较差，因而在目前学术界研究的水印主要是明文水印，盲水印应该是一个研究的方向。

（3）按内容划分：将水印划分为有意义水印和无意义水印。有意义水印是指水印本身也是一个确定的数字图像或数字音频或者是序列号等等；无意义水印是指水印是一个序列号。两者的区别是即使在受到攻击后所提取的水印破损，有意义水印方案仍然能通过视觉观察来确定水印是否存在，而无意义水印方案在受到攻击后，只能通过统计决策来确定载体中是否有水印存在。

（4）按水印所嵌入的载体划分： 数字水印可以分为图像水印、音频水印、视频水印、文本水印以及用于三维网络模型的网络水印等。随着多种数字媒体的出现，一些新的水印技术会不断出现。

（5）按水印的用途划分：将数字水印划分为票据防伪数字水印、版权保护数字水印、篡改提示数字水印以及隐蔽标识数字水印。

（6）按水印隐藏的位置：分为时域数字水印和变换域数字水印。时域数字水印直接在信号空间上叠加水印信息，常见的 LSB 法嵌入。变换域水印技术是将图像进行从空域到频域的变换，相对于空域算法，由于变换域能较好的满足了数字水印技术不可见性和鲁棒性的要求，因此该算法成为当前热门的水印算法。

2.2.3 数字水印的应用

目前，数字水印技术最主要的作用是实现版权保护，随着数字水印技术的不断发展以及不同的应用需求造就了不同的水印技术。随着计算机技术的不断发展，关于数字水印的一些应用会不断出现。

目前的典型的应用[34]主要体现在如下几个方面：

（1）数字作品知识产权保护：信息技术的飞速发展，使得数字化多媒体产品的拷贝、修改非常容易，进而使得数字媒体产品的版权保护非常困难。原创者不得不采用一些措施来保护自己的版权，原创者通常将水印嵌入原始数据，之后才公开他的水印版本作品。如在当前的 DVD 系统中，原创者将数字水印信息嵌入到 DVD 作品中，这样对该作品的复制就能得到很好的控制，一旦该作品被盗版或出现版权纠纷时，版权所有者就可以从盗版作品中提取水印信号作为依据，达到实现版权保护的目的。还比如说 IBM 公司在其“数字图书馆”软件中提供了水印的功能。

（2）数字指纹：数字指纹是指在每个数字产品中嵌入该用户的 ID 或者是序列号，通过这个带有版权的标记来识别可能的非法使用，实现版权的保护。

篡改提示：数据的标识信息往往比数据本身更具有保密价值，现在的信号拼接技术可以做到“移花接木”而不为人知。当数字多媒体作品应用于医学、新闻、法学、商业时，就需要确定该数字作品是否被篡改或经过特殊处理，这时候就可以利用数字水印对其进行鉴别，在进行水印嵌入时，先将原始数字作品分成多个独立块，对每一块分别嵌入水印，在检测水印时，不需要原始数字作品，只需要通过检测每一个数据块中的水印信号就可以确定该作品的版权，这实际上也是一种盲检测方案。

（3）商务交易中的票据防伪：伴随着高质量的图像输入输出设备的发展，特别是高精度的打印机和复印机的出现，使得票据（支票、货币）的伪造就变得更加容易，应用数字水印能更好的防止票据防伪，实现版权的保护。

（4）多语言影视系统和影视分级：在数字水印的应用中，这是数字水印技术中唯一不用于版权保护的应用领域。在电视节目的制作过程中，由于处理和传输链路的不同，会出现声图不同步的情况，采用数字水印技术可以很好的解决这一情况，可以将影视的语言配音和字母嵌入到视频图像中，在确保图像视觉质量不受影响的前提下节省了声音的传输信道。类似的还有可以把影视分级信息嵌入到视频图像中，用于控制画片的放音，控制影视分级播放。另外还可以对电视作品进行监视，利用水印监视功能可以准确监视作品播出的次数、时间等。

2.2.4 数字水印系统基本框架

从图像处理的角度上看，在图像中嵌入水印，相当于在一个强信号中叠加一个弱信号，只要叠加的弱信号强度在一定范围之内，根据人眼视觉系统（HVS）的对比门限，人眼视觉系统就无法感觉到信号的存在。因此，通过对原始图像作一定的调整，在不改变视觉效果的情况下嵌入一些信息。

传统通信系统模型[35]如图 4 所示，其中 m 是输入信息，也是准备要发送的信息，通过信道编码器对信息 m 编码，并将所有的信息映射为码字，码字序列标记为 X，X 经过编码后在有噪声的信道上传输信息 Y，在接收端，信息 Y 通过信道解码器进行解码，解码信息为 m'，由于信道中存在噪声干扰信号，因而在解码的过程中还应该纠正传输中因为噪声所带来的错误信息，因此对带有噪声的码字也必须有可能进行正确的解码。

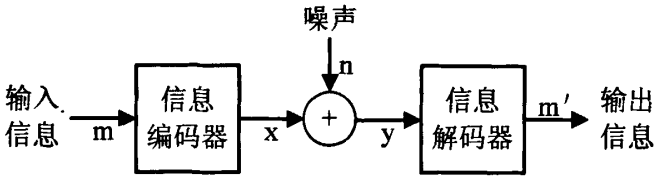


图 4 传统通信系统模型

同样地，嵌入水印的过程从数字通信的角度上来理解，就相当于在一个宽带信道（原始载体图像）上采用用扩频技术原理来传输一个窄带信号（原始水印信息）。由于分布在信道上任意频率上的能量难以检测，则提取水印相当于在一个有噪声的信道中提取出微弱的噪声信号。

2.2.5 数字水印系统的基本结构

一般情况下，数字水印技术包括三个方面的环节：水印的嵌入、水印检测/提取和水印攻击测试环节。

通用数字水印结构图如图 5 所示[37]：

在图 5 中，将 M,X,W,K,G,Em,At,D,Ex 这个九元体分别定义如下：

a) M 代表原始秘密信息，也就是水印信息。

b) X 代表所要保护的数字产品 x（或称载体作品）。

c) W 代表所有可能水印信号 w 的集合。

d) K 代表水印密钥集合。

e) G 表示利用原始水印信息 m、密钥 K 和原始数字产品 x 共同生成的水印算法，

即 $G:M\times X\times K\to W, w=G(m,x,k)$，需要说明的是，原始数字产品不一定参与水印生成过程，如果原始产品不参与水印的提取操作，则就是盲水印方案，如果原始产品参与了水印的提取操作，则就是非盲检测方案，因此这里用虚线表示。

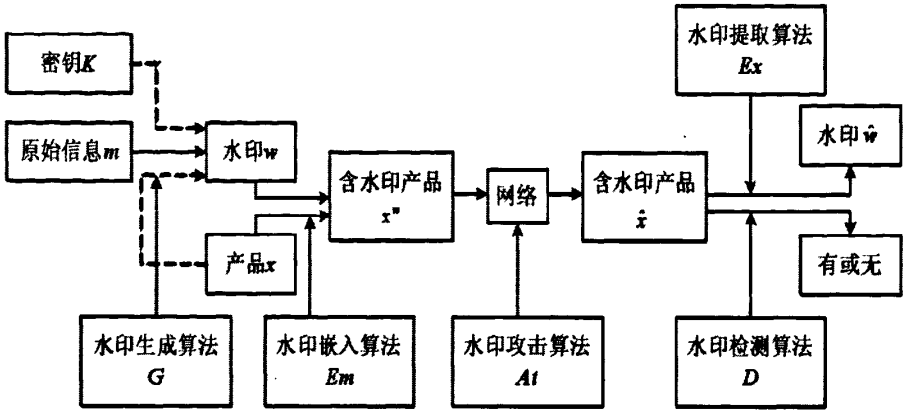


图 5　通用数字水印结构图

f)　*Em* 表示将水印 w 嵌入数字媒体产品 x 中的嵌入算法，即

$$Em:X\times W\to X, x^w=Em(x,w) \tag{2.1}$$

这里 x 代表原始产品，x^w 代表含水印产品。嵌入水印的方法比较多，各种方法各有优缺点，为了提高安全性，有时在嵌入算法中包含嵌入密钥。

g)　*At* 表示对含水印的数字媒体产品 x^w 的攻击测试算法

$$At:X\times K\to X, \hat{x}=At(x^m,K') \tag{2.2}$$

这里，对含水印产品 x^w 的攻击算法有很多种，包括抖动、加噪、压缩、缩放、图像增强、增加对比度、旋转、剪切和几何攻击等。

h)　*D* 表示水印检测算法，即

$$D:X\times K\to\{0,1\}, D(\hat{x},K)=\begin{cases}1 & \text{如果}\hat{x}\text{中存在}w \quad (H_1)\\ 0 & \text{若}\hat{x}\text{中不存在}w \quad (H_0)\end{cases} \tag{2:3}$$

这里，H_1 和 H_0 代表二值假设，分别表示水印的有或者无。

i)　*Ex* 表示水印的提取算法，即

$$Ex:X\times K\to W, \hat{w}=Ex(\hat{x},K) \tag{2.4}$$

在水印嵌入阶段主要包括水印信息的生成和水印嵌入算法的实现，水印可以是一个序列号、文本、图像或者伪随机数，嵌入算法的目标是使水印在不可感知性（透明性）和鲁棒性之间找到一个较好的折中，其中，不可感知性可以用峰值信噪比来衡量，鲁棒性可以用相似度来衡量。水印检测/提取模块主要是从嵌入水印的载体中提取水印信息。检测时可以是明水印，也可以是盲检测，检测的结果是原始水印 m，或是基于统计特性来确定数字产品中是否有水印。攻击测试模块主要是检测该算法的鲁棒性，一般要求水印算法的鲁棒性较强，算法能抵抗常见的噪声、滤波、数/模与模/数转换、压缩，旋转，尺度变化以及有损压缩编码等等攻击。一般情况下，鲁棒性强，水印的透明性较差，所以在设计算法的时候要综合考虑着两个方面。

2.2.6 水印系统的构成

一个完整的水印系统的设计必需包括水印的生成、嵌入和提取三部[37]。

（1）水印的产生

水印的产生可以由伪随机数发生器或混沌系统产生水印。产生的水印信号 W 往往需要进一步的变换以适应水印嵌入算法。这种变换包括可以对水印数据进行预处理，处理后的水印数据为 W',预处理的过程中，可以对水印进行置乱或者是加密处理，使得待嵌入的水印信息失去了统计特性，进一步增强了水印的不可感知性，使得水印系统具有更高的安全性。

（2）水印嵌入

水印嵌入过程如图 6 所示。

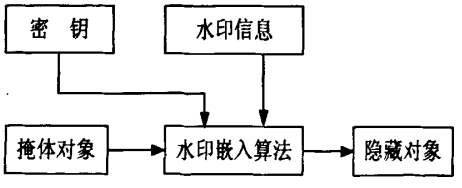


图 6 水印嵌入框图

嵌入算法需要考虑水印的不可感知性和鲁棒性。以下是三种常用的水印嵌入公式：

$$v_i^w = v_i + \alpha\omega_i \tag{2.5}$$

$$v_i^w = v_i(1+\alpha\omega_i) \tag{2.6}$$

$$v_i^w = v_i + a(v_i)^2\omega_i \tag{2.7}$$

其中，v_i，v_i^w分别表示原始载体图像像素和嵌入水印后的载体图像像素；ω_i为水印分量，α为嵌入水印的强度因子。α越大，水印鲁棒性越好，但是为了保证在不可见的前提下尽可能提高嵌入水印的强度，α的选择必须考虑图像的性质和视觉系统的特性，在保证不可见性和鲁棒性的前提下选择合适的嵌入强度因子α。(2.50)式表示加性嵌入方式，(2.6)表示乘性嵌入方式，(2.7)表示平方嵌入方式。

（3）水印的提取

水印的提取/检测是指根据具体应用的要求检测水印的存在性，检测分为盲检测和非盲检测，提取/检测时可以需要原始产品的参与，也可以不需要原始产品的参与就是盲检测；明文水印的提取需要原始图像作为辅助就是非盲检测，检测过程是数字水印嵌入算法的逆过程。非盲检测较之盲检测具有很高的稳健性，但是盲检测在计算效率和应用范围上有更大的优势，因为盲检测并不需要原始载体图像的参与，应用范围更广泛。

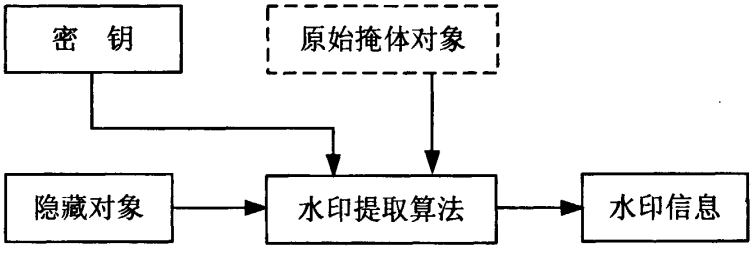


图 7 水印提取框图

一般情况下要求水印检测算法具有很高的可靠性和计算效率，只是计算效率在适当的时候可以降低要求。通常的水印检测主要有相关检测，最大释然检测和最大后验概率检测，还可以采用统计检测等方法。

2.2.7 数字水印理论算法研究

数字水印的具体算法过程包括水印嵌入前的处理、水印嵌入、水印的检测和提取。随着数字水印技术的不断发展，数字水印的典型算法包括空域算法、变换域算法。下面将对相应的算法做简单的介绍。

（1） 空域算法

空间域算法对图像不进行从时域到频域的变换，比较典型的算法有最低有效位(LSB)法、Patchwork 方法及纹理映射编码方法和文档结构微调法[12]。较早的数字水印算法都是基于空间域的，基本思想是通过改变点的像素值来嵌入水印，空间域方法具有算法简单、速度快、容易实现的优点，它能几乎无损失的恢复载体图像和水印信息。

LSB 方法一般是通过简单的修改图像的最低有效位部分来实现水印的嵌入，以保证水印的不可感知性，该算法简单，比较容易实现。但是由于使用了图像不重要的像素位，算法的鲁棒性差，水印信息很容易为滤波、图像旋转、几何变形等操作破坏。

将一幅灰度图像经过位平面分解够得到的 8 个位平面如图 8 所示：基本思想就是把灰度图像的每一个像素用 8 位二进制数表示，将第 0 位至第 7 位分别提取出来，就得到了相应的位平面。

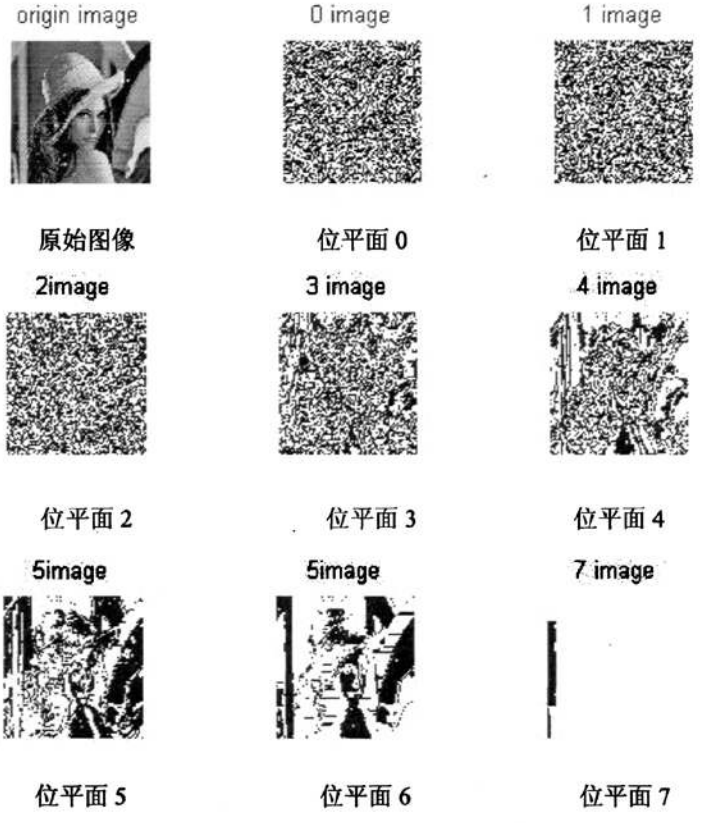


图 8　图像位平面分解图

从分解的位平面来看，从位平面 0~位平面 7，位平面的特征逐渐变的复杂，细节也不断增强。由于低位平面代表的能量很少，所以改变低位对图像的质量并没有很大的影响，LSB 方法正是利用这一点在图像的低位隐藏水印信息。

空域算法的另一种算法，Patchwork 方法是通过任意选择 N 对图像中的像素点，增加一点的像素的同时，降低相应另一点的像素值，这样做以后整个图像的亮度值保持不变，其基本思想是改变图像的统计特性来加载数字水印[37]。通过实验表明：该方法的鲁棒性强，对于滤波、压缩、旋转等操作具有抵抗能力，但是对多于多拷贝平均攻击的抵抗力较弱，而且该方法只适用于大量任意纹理区域的图像，该算法尚不能完全自适应。

（2）变换域算法

基于变换域的水印算法大体上可以分为三类：离散傅里叶变换域，离散余弦变换域和离散小波变换 DWT 域。信号经过从空间域到频率域的变换后，得到的低频分量代表了信号的平滑部分，得到的高频分量表示信号的抖动部分，根据变换后其能量集中的特点，利用人类视觉模型(HVS)，在选择合适的嵌入算法和嵌入强度的基础上就能够很好的保证水印的不可见性。

①DFT 域变换方法

数字图像在进行了离散傅里叶变换之后，得到其幅频特性和相频特性，通常在其相位特性中嵌入水印信息，这样有利于实现水印的仿射不变性，抗攻击能力也会增强，而且具有良好的抗 RST 特性。

②DCT 域变换方法

数字图像经过 DCT 变换之后，在 DCT 变换域上选择相应的系数来进行水印的嵌入，嵌入水印信息后在经过 DCT 反变换就得到了嵌入水印后的图像。DCT 域数字水印算法具有鲁棒性强和隐蔽性好的特点。在选择嵌入系数上，一般选择中低频系数叠加水印信息。因为人眼的对于中低频系数比较敏感，所以当攻击者攻击水印时不可避免的会引起图像质量的严重下降；并且一般的图像处理过程也不会改变这部分数据。这也是绝大多数都选择在中频系数上嵌入水印的原因所在。大多 DCT 域的水印算法为了和已有国际压缩标准（JPEG，MPEG）兼容，采用基于 8×8 图像块进行 DCT 变换。

③DWT 域变换方法

由于小波变换有自身的一些优势，同时离散小波变换在图像处理和图像分析领域中的广泛应用，使得 DWT 域数字水印算法成为这几年数字水印研究领域中的一个热点。目前基于 DWT 域的水印算法在算法上主要包括水印的预处理、水印嵌入子带的选择、水印嵌入强度的选择。对于高频信号，小波变换采用由粗到细渐进的取样间隔对其进行变换，这样可以对细节进行任意放大。比如可以应用多分辨率分析算法对载体图像进行多重分解，在相应的层次上选择合适的频率分量应用嵌入算法进行水印嵌入，嵌入后经过反变换就得到了嵌入水印后的载体图像。由于小波变换有其自身的优点，基于小波变换的图像数字水印技术是目前研究的一个热点。

2.3 混沌理论

2.3.1 混沌理论定义

混沌是确定性系统中由于系统内在随机性而产生的一种外在复杂的、貌似无规则的一种运动形式，但是混沌并不是无序和紊乱，是系统从有序突然变为无序状态的一种演化的过程和理论，是对确定性系统中出现的内在"随机过程"形成的途径、机制的研讨。混沌现象起因于物体以不断地以某种规则复制前一阶段的运动状态，最后结果是产生无法预测的结果。混沌现象发生于易变动的物体或系统，该物体在行动之初极其单纯，但经过一定规则的连续变动之后，却会产生始料所未及的后果，这就是我们所说的混沌状态。但是此种混沌状态不同于一般杂乱无章的的混乱状况，此一混沌现象经过长期及完整分析之后，可以从中理出某种规则出来。人们对于混沌动态学的最初认识应当归功于 Weis(1991)，而 Weis 又是从几百年前从事天体力学的法国数学家 Henry Poincare 那里得到的启示。Poincare 提出，由运动的非线性方程所支配的动态系统是非线性的。19 世纪法国的数学家、物理学家和天文学家庞架莱先生（J.H.Poincare）致力于研究太阳系中三体运动的引力相互的作用的时候发现这些引力的相互作用有很惊人的复杂性，这其实就是一种混沌现象。

2.3.2 混沌的特性

混沌作为一种自然界与人类社会中普遍存在的运动形态，虽然它在不同的学科范畴和领域中都在被研究，各个领域对于混沌的定义可能有所不同但它们应该有共同的内涵和各自的特殊性，概括地说，混沌系统如下的几个基本特征：

（1）随机性：混沌是一种伪随机的运动，在不同的初始值条件下产生的序列具体有非周期性，对于初始条件的微小变化具有高度的敏感依赖特性。

（2）有界性：有界性是指在相空间内混沌吸引子是有界的，但是在吸引子内相轨迹具有高度不稳定性；

（3）分维性：指系统运动轨道在相空间的几何形态可以用分维来描述。混沌吸引子的几何特征是具有分形（分数维数）和自相似嵌套结构；具有连续功率谱。

（4）普适性：混沌吸引子具有遍历性，当某一系统处于混沌时，所表现出来的特征具有遍历性，其特征不会因为系统的不同和系统运动方程的不同而发生变化。

（5）标度律：经常与分岔、分形和多种奇怪吸引子甚至排斥子其他复杂动力现象共存等等。

2.3.3 混沌置乱

为了提高水印信息的安全性，一般需要对水印信息进行预处理，常用的方法就是采用置乱技术扰乱图像的组成部分，让图像变的杂乱无章，目的就是为了破坏图像的自相关性。图像置乱变换是一种可逆的变换，经过置乱变换后的图像看起来杂乱无章，如果不知道采用什么样的方式进行置乱，就很难恢复出原始图像信息，而且经过置乱后的图像大小也不会发生变化。

通常情况下是对水印图像进行置乱处理，主要的原因就是载体图像一般都比较大，变换时间较长，因此通常情况下对水印图像进行置乱处理。而且对水印图像进行置乱处理之后一方面能增强水印信息的保密性，另一方面对于图像剪切、加噪声等攻击具有很好的鲁棒性。

常用混沌模型：

（1）Logistic 混沌模型[33]

Logistic 模型是混沌模型中比较常见的一种，很多文献中都应用这种混沌映射来讲图像进行置乱，以加强水印的安全性，其离散时间动态系统在[0,1]上的定义如下：

$$x_{k+1} = \lambda x_k (1 - x_k), \quad x_k \in (0,1) \tag{2.8}$$

其中，$x_k \in (0,1)$，参数$0 \le \lambda \le 4$，当$3.5699456... < \lambda \le 4$时，Logistic 映射工作于混沌态。

经过变换，Logistic 映射在[-1，1]上的定义可以表示为

$$x_{k+1} = f(x_k) = 1 - \lambda x_k^2, \quad \lambda \in (0,2) \tag{2.9}$$

其中x_k是当前状态，f把当前状态x_k映射到下一个状态x_{k+1}，λ是参数，随着λ的逐渐增大，迭代会出现多次突变，系统进入混沌状态。一般在设计水印算法的时候，用户应该记住混沌的初始值才能进行水印的解密恢复。Logistic 映射生成混沌序列的方法有实数值序列，二值序列，比特序列。实数值序列由选定的x_0和λ代入式（2.9）得到实数值$\{x_k; k = 1,2,3...\}$，是混沌映射的轨迹点所形成的序列。二值序列通过定义一个符号函数*Sign*来对二值序列进行置乱加密。由实数值混沌序列得到的二值序列也具有混沌特性。常用算法如：

$$Sign=\begin{cases}0,-1\le x_k\le 0\\1,0\le x_k\le 1\end{cases}\quad 或\quad Sign=\begin{cases}-1,-1\le x_k\le 0\\1,0\le x_k\le 1\end{cases}\tag{2.10}$$

比特序列是由实数值混沌序列得到，和实数值混沌序列所不同的是比特序列是通过 $\{x_k;k=1,2,3...\}$ 中的 x_k 改写为 $L-bit$ 的浮点数形式得到的。

$$|x_k|=0.b_0(x_k)b_1(x_k)..b_i(x_k)b_{L-1}(x_k)\tag{2.11}$$

其中 $\{b_i(x_k),i=0,1,2,...,L-1;k=1,2,3...\}$。比特序列同样具有混沌特性。

（2）整数型混沌发生器

文献[41]提出了一个很好的混沌发生器，由它生成的混沌序列是一个整数值混沌序列，其定义如下：

$$x_{k+1}=f_a(x_k)=\begin{Bmatrix}\max Int[(m/a)x_k & 1\le x_k\le a\\ \min Int[m(m-x_k)/(m-a)] & a\prec x_k\le m\end{Bmatrix}\tag{2.12}$$

其中：$\max Int(z)$ 表示大于等于 z 的最小整数；$\min Int(z)$ 表示小于等于 z 的最大整数；$x_k\in\{1,2,...,m\}$；参数 $a\in\{1,2,3,...,m\}$。

混沌发生器经过 n 次迭代后就得到一个混沌随机序列，它的优点是生成的混沌序列是整数型混沌序列。

本文算法中利用 Logistic 混沌序列对水印图像进行预处理，得到解密后水印图像。

2.4 本章小结

随着网络技术和计算机信息技术的飞速发展，数字作品的权益保护问题就成了各国比较关心的问题。信息隐藏和数字水印技术作为信息安全的分支学科，合理地应用这些技术可以为权益保护提供一种可行的方案，实现产权保护的目的。本章的主要工作可概括如下：

（1）介绍了数字水印的基本概念，并给出了数字水印算法的基本框架，在对水印框架进一步说明的基础上对水印系统的三个方面（嵌入、提取、攻击）进行了介绍。

（2）阐述数字水印的理论知识。介绍了数字水印的概念，水印的分类，水印的特征，水印的应用，明确指出作为数字水印应当具备的一些特征。在此基础上，进一步介绍了现有数字水印算法较为通用的几种分类，并比较不同的分类算法各自的优缺点。

（3） 阐述了水印预处理的方法，介绍了 Logistic 混沌映射的基本原理和混沌映射的特征。

第三章 小波变换理论

3.1 小波概述

1822 年法国人傅里叶提出了傅里叶变换，小波变换是在傅里叶变换的基础上发展起来的，它是近年来兴起的数学分支，是继傅里叶变换后的又一里程式发展。由于小波变换具有良好的时频局部性，在工程中得到了很广泛的应用，它的思想来源于函数的伸缩和平移方法。小波分析被数学家认为是一种调和分析，它可以解决很多傅立叶不能解决的问题。傅立叶变换在信号处理领域已有广泛应用，如果处理的信号是平稳信号（也就是不随着时间变化的信号），傅里叶变换不会有什么缺陷，但是如果处理的信号是非平稳信号，比如 Internet 流量控制，如果需要区分各种频率成分，而且是每个时刻附近的频率成分，那么傅里叶变换的方法就无能为力了，于是出现了小波变换。小波变换是在傅里叶变换的基础上发展起来的，它克服了傅里叶变换中固定分辨率的特点，对信号进行小波变换之后，既可以分析信号的概貌，又可以分析信号的细节。在小波变换后，图像的细节部分集中在低频部分，边缘信息集中的高频部分。

小波理论的突破性成果，其作用相当于 Fourier 分析中的 FFT 算法。信号经过传统的傅里叶变换之后，得到其幅频特性和相频特性，并用其频率特性进行分析，该变换的缺点是不能区分平稳信号和非平稳信号。和传统傅里叶变换相比，离散傅里叶变换可以确定一个信号所包含的频率分量，但是不能确定每一个频率分量出现的时间。根据以上的分析，针对这些问题，解决这些问题的基本思想进行离散小波变换，因为这样可以缩短时间窗口。当采用离散小波变换取代短时 DFT 变换时，针对信号中的不同频率分量，根据小波变换的多分辨率特性，小波变换可以用不同的分辨率来对信号进行分析和处理，这样分析高频信号时可以采用好的时间分辨率来进行分析，分析低频信号时可以采用好的频率分辨率来进行信号处理。

小波变换对时间窗和频率窗都可以根据信号的具体形态进行动态调整，因而小波分析可以探测正常信号中的瞬态成分，并展示其频率成分，所以也常常称小波变换为数学显微镜，广泛应用于各个时频分析的领域。

综上，将小波分析用于信号分析有以下特点：

a. 可以用不同尺度对信号进行由粗到精的多分辨率分析，可以由粗到细逐步观察信号，可以在不同的空间方向和独立的频带上进行分解而且还不丢失原信号的信息。

b. 具有突出信号在时、频域的局部特征的能力，因而是检测瞬态和边沿的良好，具有放大、缩小和平移的数学显微镜功能，通过检查不同放大倍数下的信号的变化来研究相关动态特征。

c. 可以将信号和图像分层次展开，尺度不同情况下离散的小波变换有快速算法，可以加快运算速度，满足实时处理的要求。

3.2 小波变换基础

在介绍小波变换之前，首先对一些符号进行简单的说明：

（1）$L^2(R)$表示一维函数$f(x)$的平方可积的 Hilbert 空间。

（2）若$f \in L^2(R)$和$g \in L^2(R)$，则$f(x)$和$g(x)$的内积可表示为：

$$\langle g(x), f(x) \rangle = \int_{-\infty}^{\infty} f(x)g(x)dx \tag{3.1}$$

（3）若$f \in L^2(R)$和$g \in L^2(R)$，则$f(x)$和$g(x)$的卷积可以表示为：

$$f(x) * g(x) = \int_{-\infty}^{\infty} f(u)g(x-u)du \tag{3.2}$$

（4）$f \in L^2(R)$的傅立叶变换定义可以表示为：

$$\hat{f}(\omega) = \int_{-\infty}^{\infty} f(x)e^{-j\omega x}dx \tag{3.3}$$

（5）$L^2(R^2)$表示平方可积的二维函数$f(x,y)$的 Hilbert 空间。

（6）$f(x,y) \in L^2(R^2)$的傅立叶变换可以表示为：

$$\hat{f}(\omega,\omega) = \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} f(x,y)e^{-j(\omega_x x+\omega,y)}dxdy \tag{3.4}$$

3.2.1 小波变换的概念

（1） 小波变换的定义:

$$W_f(a,b) = \int_R f(t)\overline{\psi_{a,b}(t)}dt \tag{3.5}$$

把形如式(3.5)的积分变换称为函数$f(t)$的小波变换，其中

$$\psi_{a,b}(t)=|a|^{1/2}\psi(at-b) \tag{3.6}$$

在式(3.6)中，经由$\psi(t)$经平移和放缩后得到$\psi(at-b)$，a称为尺度因子，b称为平移量，参数b确定了函数的"中心位置"，参数a确定了小波函数的时域宽度。它将一个一维函数变换为一个二维函数。当满足一定条件(允许条件)时，$\psi(t)$称为允许小波函数。允许条件可如式(3.7)所示，其中$\overline{\psi}(t)$为$\psi(t)$的共轭函数

$$C_{\varpi}=\int_R\frac{\left|\psi(\varpi)^2\right|}{|\varpi|}d\varpi<\infty \tag{3.7}$$

（2） 小波变换的逆变换 IDWT

小波变换的逆变换公式可见式(3.8)所示，它将频域信号转换为时域信号。

$$f(t)=\frac{1}{C_{\psi}}\int_R\left\{\int_R W_f(a,b)\psi_{ab}(t)db\right\}\frac{1}{a}da \tag{3.8}$$

3.2.2 连续小波变换概念

将任意$L^2(R)$空间中的连续函数函数$f(t)$在小波基下进行展开，如式(3.9)所示，表示为函数$f(t)$ 的小波变换。

$$W_f(a,b)=\langle f(t),\psi_{ab}(t)\rangle=\frac{1}{\sqrt{a}}\int_R f(t)\overline{\psi}\left(\frac{t-b}{a}\right)dt \tag{3.9}$$

其中，$\overline{\psi}\left(\frac{t-b}{a}\right)$为$\psi\left(\frac{t-b}{a}\right)$的共轭函数。称式$W_f(a,b)$为小波变换系数。

3.2.3 离散小波变换

在实际应用中，不管是音频信号还是视频信息，都是经过采样后得到的一些离散数据，因此我们还应将上述连续变换离散化，以利于对离散信号进行处理。

（1） 离散小波函数

实际上，连续小波变换在实际计算机应用中没有意义，只是在理论推导和性质证明中我们会用到连续小波变换的相关理论去分析。这是因为如果在实际应用中采用连续小波变换，需要用每个可能的尺度去计算小波系数，这样将产生大量的冗余数据，会降低计算速度，因此，必须将连续小波离散化。把连续小波变换中尺度参数a和平移参数b的离散化，得到离散小波函数为如式(3.10)所示，可见，一维信号$f(x)$经离散小波变换

后得到的是一个二维数组，这样计算机在分析和处理数据的过程中，计算工作量就大大减少了，也不会产生大量的冗余数据。

$$\psi_{j,k}(t)=2^{j/2}\psi(2^j t-k) \tag{3.10}$$

离散小波变换系数则可表示为式(3.11)所示。

$$C_{j,k}=\int_R f(t)\overline{\psi}_{j,k}(t)dt \tag{3.11}$$

其小波变换重构公式为式(3.12)所示。

$$f(t)=C\sum_{-\infty}^{+\infty}\sum_{-\infty}^{+\infty}C_{j,k}\psi_{j,k}(t) \tag{3.12}$$

在上式中C是一个与信号无关的常数。

在离散小波变换中，正交小波变换是一种最简单的小波变换，因为它的对偶就是它本身。为了将小波变换应用于信号处理，首先我们希望有一些正交小波可供选用，很著名的有 Haar 小波。Haar 小波是正交的，但是其缺点是光滑性很差，因此如何构造优良性质的正交小波也是需要解决的问题。

（2）离散小波变换(DWT)及其逆变换(IDWT)

对任意给定函数$f(t)$的离散小波变换(DWT)及其逆变换($IDWT$)分别为式(3.13)、式(3.14)所示。

$$W_f(j,k)=\int_R f(t)\overline{\psi}_{j,k}(t)dt \tag{3.13}$$

$$f(t)=\sum_{j,k}\langle f,\psi_{j,k}\rangle\cdot\psi_{j,k}(t)=\sum_{j,k}W_f(j,k)\cdot\psi_{j,k}(t) \tag{3.14}$$

$W_f(j,k)$为离散小波变换系数，$\psi_{j,k}(t)=2^{j/2}\psi(2^j t-k)$，$\overline{\psi}(t)$为$\psi(t)$的共轭。

3.2.4 多分辨率分析

我们通常所说的信号大部分是复杂的瞬变信号，都是由高频分量和低频分量叠加而成的。任意信号包含高频成分、低频成分甚至还有滞留成分，为了获得一个信号的低频信息，将$f(t)$中的低频成分用另外一类基函数展开，这样就引入了尺度函数，尺度空间和多分辨率分析等一系列概念。考虑一个以时间t为变量的离散随机信号$f(t)$，概率分布函数为$p_{f(t)}(X)$,将$p_{f(t)}(X)$的小波变换具有不同的分辨率因此称为多分辨率分析。对信号进行这样的分析需要有一组中心频率不同的带通滤波器组，同时需要一组带宽不同

的低通滤波器组来处理信号。

多分辨逼近(*MRA*)是指一串嵌套式闭子空间逼近序列$\{V_m\}_{j\in Z}$，它满足(3.15)所示的下列要求：

$$\begin{aligned}
&1^\circ \cdots \subset V_j \subset V_{j+1} \subset \cdots \subseteq L^2(R), \bigcap_{j\in Z} V_j = \{0\}, \bigcup_{j\in Z} V_j = L^2(R)\\
&2^\circ V_j = span\{\phi_{j,k}(t) \mid \phi_{j,k}(t) = 2^{j/2}\phi(2/t-k), k\in Z\}\\
&3^\circ \phi(t) = \sum_n h_n \phi(2t-n), \{h_n \in l^2\}\\
&4^\circ \{\phi(t-k)\} \text{是 } Riesz \text{ 基}
\end{aligned} \tag{3.15}$$

由$\phi(t)$生成了多分辨率分析（*MRA*），其中式(3.15)称为双尺度方程，$\phi(t)$称为尺度函数或*MRA*的生成元。满足如式(3.16)条件的基函数$\{\phi_{j,k}(t)\}$为*Riesz*基函数。

$$A\sum_k |C_k^j|^2 \le \left\|\sum C_k^j \phi_{j,k}(t)\right\|_0^2 \le B\sum_k |C_k^j|^2, \quad \{c_k^j\} \in l^2 \tag{3.16}$$

其中，*A*和*B*都是正常数。

3.2.5 正交小波级数

若对$\forall f, g \in L^2(R)$，都满足表达式(3.17)的要求，即：

$$(f(t), g(t)) = 0 \tag{3.17}$$

则称$f(t)$和$g(t)$是正交的。如果$L^2(R)$的中所有基函数族$\{\phi_k(t)\}_{k=1}^{\infty}$中的基函数，都是两两正交的，则称这种基函数为标准正交基。

设$\phi(t)$生成多分辨率分析，其中$\phi(t)$为尺度函数，$\varphi(t)$为小波函数，记双尺度方程为：

$$\begin{cases}
\phi(t) = \sum h_n \phi(2t-n)\\
\varphi(t) = \sum g_n \phi(2t-n)\\
g_n = (-1)^n h_{1-n}
\end{cases} \tag{3.18}$$

设$\{\phi(t-n)\}$是标准正交的，$\phi(t) \in L^2(R)$，则$\{\varphi_{j,k}(t)\}, j,k \in Z$是$L^2(R)$的标准正交基，$f(t) \in L^2(R)$可展开为正交小波级数，如式(3.19)所示：

$$\begin{cases} f(t)=\sum_{j,k\in Z} d_k^j \varphi_{j,k}(t) \\ d_k^j=\left(f(t),\varphi_{j,k}(t)\right) \end{cases} \tag{3.19}$$

3.2.6 Mallat 分解算法

Mallat 在 1986 年经计算机的多分辨率的思想引入到了小波变换中，从而有了统一的小波基的构造方法在此基础上，给出了一种基于子带滤波器结构的离散小波变换及其离散小波重构算法。根据正交小波多分辨分析的特点和尺度方程以及小波方程的系数，可以得到信号小波变换及逆变换的递推的 *Mallat* 算法。其基本思想是将被分析的函数分解成不同尺度下的“像”和对该“像”细节的补充。

将 $L^2(R)$ 上的多分辨分析记为 $\left(\{V_j, j\in Z\},\phi(t)\right)$，其中尺度方程 $\phi(t)$ 和小波函数 $\varphi(t)$ 及其关系分别为式（3.20）所示：

$$\begin{cases} \phi(t)=\sum h_n \phi(2t-n) \\ \varphi(t)=\sum g_n \phi(2t-n) \\ g_n=(-1)^n h_{1-n} \end{cases} \tag{3.20}$$

设 $f(t)\in L^2(R)$，$c_{j,k}=\int_R f(t)\overline{\phi}_{j,k}(t)dt$ 成为 $f(t)$ 的尺度系数与 $d_{j,k}=\int_R f(t)\overline{\varphi}_{j,k}(t)dt$ 称为 $f(t)$ 小波变换系数，同时，将 $f(t)$ 在闭子空间 V_j 和 W_j 上的正交投 $y-\bar{y}$ 影分别记为 $f_j(t)$ 和 $g_j(t)$，这样就得到式(3.21)。

$$f_j(t)=\sum_{k\in Z} c_{j,k}\phi_{j,k}(t) \tag{3.21}$$

$$g_j(t)=\sum_{k\in Z} d_{j,k}\varphi_{j,k}(t) \tag{3.22}$$

$$V_{j+1}=V_j\oplus W_j \tag{3.23}$$

由 （3.23）式可得

$$f_{j+1}(x)=f_j(x)+g_j(x) \tag{3.24}$$

这样就得到了信号的尺度变换系数和小波变换系数之间的关系，如式(3.25)所示。

$$\sum_{l\in Z} c_{j+1,l}\phi_{j+1,l}(t)=\sum_{k\in Z} c_{j+1,k}\phi_{j+1,k}(t)+\sum_{k\in Z} c_{j,k}\phi_{j,k}(t) \tag{3.25}$$

（1） 一维 *Mallat* 算法

①*Mallat* 分解算法

Mallat 分解算法如式(3.26)所示：

$$c_{j,n}=\sum_{m\in Z}\bar{h}_{m-2n}c_{j+1,m}$$
$$d_{j,n}=\sum_{m\in Z}\bar{g}_{m-2n}c_{j+1,m} \tag{3.26}$$

② *Mallat* 合成算法

将 $\bar{\phi}_{j+1,m}(t)$ 乘以信号级数分解式（3.26）两端之后求求取积分运算，可以得到式(3.27)，这就是 *Mallat* 合成算法

$$c_{j+1,m}=\sum_{n\in Z}\left(h_{m-2n}c_{j,n}+g_{m-2n}d_{j,n}\right) \tag{3.27}$$

（2）二维小波变换 *Mallat* 算法

对于二维函数空间 $L^2(R\times R)$ 上的任意信号 $f(x,y)$，我们可以利用式（3.28）和（3.29）所示的二维小波变换 *Mallat* 算法对其进行二维小波分解和合成。

$$\begin{cases} d_{j,m,n}^{(0)}=\sum\limits_{(m,n)\in Z\times Z}\bar{h}^{(0)}(m-2M,n-2N)d_{j+1,m,n}^{(0)} \\ d_{j,m,n}^{(1)}=\sum\limits_{(m,n)\in Z\times Z}\bar{h}^{(1)}(m-2M,n-2N)d_{j+1,m,n}^{(0)} \\ d_{j,m,n}^{(2)}=\sum\limits_{(m,n)\in Z\times Z}\bar{h}^{(2)}(m-2M,n-2N)d_{j+1,m,n}^{(0)} \\ d_{j,m,n}^{(3)}=\sum\limits_{(m,n)\in Z\times Z}\bar{h}^{(3)}(m-2M,n-2N)d_{j+1,m,n}^{(0)} \\ \vdots \end{cases} \quad \text{（分解算法）} \tag{3.28}$$

$$\begin{aligned} d_{j,m,n}^{(0)}=&\sum_{(m,n)\in Z\times Z}h^{(0)}(m-2M,n-2N)d_{j,m,n}^{(0)} \\ &+\sum_{(m,n)\in Z\times Z}h^{(1)}(m-2M,n-2N)d_{j,m,n}^{(1)} \\ &+\sum_{(m,n)\in Z\times Z}h^{(2)}(m-2M,n-2N)d_{j,m,n}^{(2)} \\ &+\sum_{(m,n)\in Z\times Z}h^{(3)}(m-2M,n-2N)d_{j+1,m,n}^{(3)} \\ &\vdots \end{aligned} \quad \text{（合成算法）} \tag{3.29}$$

（3）二维离散小波变换

一维连续小波变换和一维离散小波变换可以对一维信号进行处理，比如音频信号，但是对于二维信号，比如图像信号就不能采用一维小波变换来进行处理。对于二维信号的处理就不能采用一维小波变换来处理图像问题，因此必须要引入二维小波变换来对图像进行处理。二维离散小波变换是在一维小波变换的基础上得到的，其基本思想就是通过分离变量的方法将一维小波函数和尺度函数构造成所需要的二维函数，分离方式如式(3.30)所示。

$$\begin{cases}\Phi(x,y)=\varphi(x)\varphi(y)\\ \Psi^{(1)}(x,y)=\varphi(x)\psi(y)\\ \Psi^{(2)}(x,y)=\psi(x)\varphi(y)\\ \Psi^{(3)}(x,y)=\psi(y)\psi(y)\end{cases} \tag{3.30}$$

图像的二维小波分解过程可以通过行处理和列处理的方式来完成。基本过程如下：首先将二维信号 $a_j(m,n)$ 的每一行作为一个一维信号，分别通过低通滤波器 $\{h'\}$ 和高通滤波器 $\{g'\}$ 进行滤波处理，然后将这两个中间结果的每一列看成一维信号，然后再次通过低通滤波器 $\{h'\}$ 和高通滤波器 $\{g'\}$ 进行滤波处理，这样就可以得到四个二维数据 $a_{j-1}(p,q)$，$b_{j-1}^{(1)}(p,q)$，$b_{j-1}^{(2)}(p,q)$ 和 $b_{j-1}^{(3)}(p,q)$，图 9 表示了二维信号的分解过程[38]。

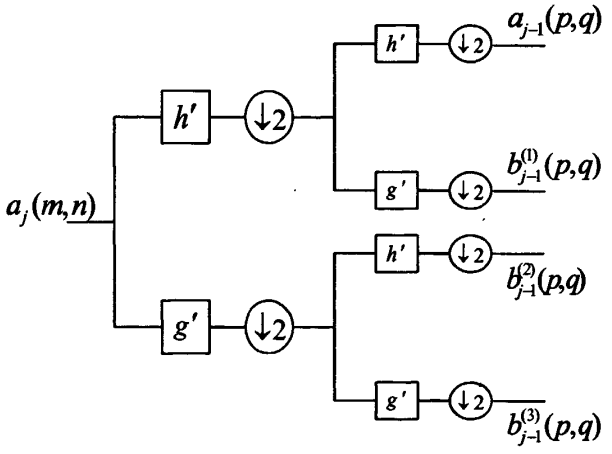


图 9 二维信号二维分解

3.3 本章小结

本章主要介绍了小波变换的基本原理，介绍了连续小波变换、离散小波变换、多分辨率分析和二维图像的小波变换的基本原理，离散小波变换可以用不同的尺度对信号进行多分辨率分析，通过小波变换可以将图像分解为高频部分、低频部分和中频部分，正是由于小波变换具有不同分辨率下恒定的品质因素和良好的检测瞬态和边缘的这些优点，因而小波变换在图像处理中应用广泛。

第四章 基于 shamir 门限方案小波域数字水印算法

4.1 shamir 理论概论

信息安全包含密码学和信息隐藏两个部分，现代密码体制的设计思想取决于密钥，密钥的泄露意味着体制已经丧失了安全性，同时密钥的丢失还有可能导致对方也不能从密文中恢复出明文信息，在密码体制中，解决该问题的一般方法是频繁地更换密钥，但是这种方法在大信息量的今天是不太现实的，于是就出现了密钥管理和密钥共享控制的问题。针对于密钥管理和密钥共享控制的问题，Blakley 和 Shamir 在这样的背景下分别于 1979 年各自提出了密钥共享的概念，并分别设计了具体的体制，门限体制是最早提出的密钥共享体制，不同的是 Blakley 体制给出的算法是基于有限几何的，而 Shamir 体制则基于多项式插值，本文的方案是基于门限的多项式插值的秘密共享方案。

4.2 shamir 理论门限体制和秘密共享

在shamir理论(t,n)门限体制中，秘密分存就是将一个秘密分解成n份，每一份称为一个子秘密，并将这n份子密钥分发给一组参与者$C=\{C_1,C_2...C_n\}$，只有知道了其中的至少$t(t\le n)$份才能恢复出原来的秘密信息。这种秘密共享方案提高了系统的安全性和健壮性。当攻击者试图提取隐藏在载体中的秘密信息时，他必须要获得足够的子秘密才能恢复出秘密信息，另一方面，由于某种原因当一部分子秘密丢失时或者遭到破坏时，通过剩余的足够的子秘密也能恢复出原始秘密信息，这就是shamir秘密共享方案，在该方案中，t称为门限值[39]。

4.3 拉格朗日插值（Lagrange）多项式方案

1）实数域 Lagrange 插值多项式方案

Shamir 提出了实数域 Lagrange 插值算法，根据 shamir 理论中的(t,n)门限方案，要按照 shamir 的分存算法将秘密信息分存，如果是(t,n)门限方案，要将这n份子秘密分配给n个参与者，假设秘密信息为y，首先要生成多项式：

$$F(x)=y+m_1x+m_2x^2+...+m_tx^{t-1} \tag{4.1}$$

（1）在该多项式中，$t \le n$，即t是不大于n的整数。

（2）$m_1, m_2, ...m_{t-1}$是随机的整数。

（3）对于每一个选定的x_n，要求每个x_n是不能重复的，然后分别代入表达式(4.1)计算出$F(x_n)$，一般情况下，x的个数就是分存的个数，即$i = 1,2,...n$。

（4）将方程的每一组解$(x_n, F(x_n))$作为子秘密传送给n个参与者，由这n个参与者共同保存子秘密信息。

通过上述这样一个过程就实现了秘密信息的分存处理。从n个子秘密中恢复原始秘密信息的过程如下：、

假设从n份中提取至少t份子秘密进行恢复，构造如下的多项式：

$$\begin{cases} F(x_1) = y + m_1 x_1 + m_2 x_2^2 + \ldots + m_{t-1} x_1^{t-1} \\ F(x_2) = y + m_1 x_2 + m_2 x_2^2 + \ldots + m_{t-1} x_2^{t-1} \\ \cdots\cdots\cdots \\ F(x_t) = y + m_1 x_t + m_2 x_t^2 + \ldots + m_{t-1} x_t^{t-1} \end{cases} \tag{4.2}$$

根据拉格朗日插值公式，表达式(4.2)中的的$(t-1)$次多项式可以表示如下：

$$F(x) = F(x_1)\frac{(x-x_2)(x-x_3)\ldots(x-x_t)}{(x_1-x_2)(x_1-x_3)\ldots(x_1-x_t)} + F(x_2)\frac{(x-x_1)(x-x_3)\ldots(x-x_t)}{(x_2-x_1)(x_2-x_3)\ldots(x_2-x_t)} + \ldots + F(x_t)\frac{(x-x_2)(x-x_3)\ldots(x-x_t)}{(x_t-x_1)(x_t-x_3)\ldots(x_t-x_{t-1})} \tag{4.3}$$

由表达式(4.3)可知，只有知道了至少t份子秘密才能恢复出秘密信息y，如果提取出的子秘密少于t份就不能恢复出秘密信息y。

2）有限域 Lagrange 插值多项式方案

该方案是利用有限域中的方式来构造门限方案的。具体的思想如下：

设$GP(q)$是一个有限域，且$q > n$，若将密钥y分成n分，交给n个人保管，按照门限体制的要求，只要知道了其中任意$t(t \le n)$个人合作可以得到密钥y。

现在假设要构成$(3,n)$门限方案，也就是在恢复秘密信息的时候要从n份中提取出其中的3份，按照这样的要求，产生一个多项式：

$$F(x) = (ax^2 + bx + M) \bmod q \tag{4.4}$$

由该多项式生成影子图像，在表达式(4.4)中，a,b 是随机选择的整数，M 是消息，q 是门限素数，其中门限素数的值要求比所有的系数要大。当取不同的 x 时，通过多项式就得到不同的结果：

$$F(x_j)=(ax_j^2+bx_j+M)\bmod q \tag{4.5}$$

在(4.5)中，q 是一个公开的素数，系数 a 和 b 为秘密随机整数，M 是消息。

秘密影子 t_i 可以通过计算多项式(4.5)在几个不同点上的值得到：

$$t_j=F(x_j) \tag{4.6}$$

由于多项式(4.5)有 3 个未知系数 a，b，M，理论上如果联立方程组来求解未知数，只需要三个方程就可以求解出方程组的解。对于信息分存而言，任意 3 个或 3 个以上的影子就能够求解出未知系数，即恢复消息 M。

设 M =11，构造(3,5)门限方案，素数为 13，在这个方案中 5 个人中任意 3 个都能重构 M，首先产生一个二次方程（7 和 8 为随机选择的数据）：

$$F(x)=(7x^2+8x+M)\bmod 13 \tag{4.7}$$

根据（4.7）的分存方案所得到的 5 个影子是：

$$\begin{cases} t_1=F(1)=7\times1^2+8\times1+11\equiv0(\bmod13)\\ t_2=F(2)=7\times2^2+8\times2+11\equiv3(\bmod13)\\ t_3=F(3)=7\times3^2+8\times3+11\equiv7(\bmod13)\\ t_4=F(4)=7\times4^2+8\times4+11\equiv12(\bmod13)\\ t_5=F(5)=7\times5^2+8\times5+11\equiv5(\bmod13) \end{cases} \tag{4.8}$$

要得出 M 的值，只需要若从 5 个影子中任选 3 个影子（比如 t_2，t_3，t_4）来重构 M，解线性方案组（4.9）

$$\begin{cases} 3=a\times2^2+b\times2+M(\bmod13)\\ 7=a\times3^2+b\times3+M(\bmod13)\\ 5=a\times4^2+b\times4+M(\bmod13) \end{cases} \tag{4.9}$$

解得：a=7，b=8 和 M =11。这样就恢复了 M。

这就是 shamir 门限方案，一方面能够实现秘密信息的分存处理，另一方面在秘密信息部分丢失的情况下只要有足够的子秘密就能实现对秘密信息的恢复和提取[39][40]。

4.4 基于 shamir 理论的数字水印算法

数字水印一般以版权保护为应用目的，因而要求对水印的鲁棒性较高。针对这一要求，在设计过程中，首先要考虑水印类型的选择，为了提高水印抗攻击的能力，对水印信息如何加密处理需要考虑；另一方面，选择在哪一种变换域上设计水印算法，选择好变换域后，还要选择水印的嵌入位置，还要考虑抗攻击测试的能力，因此根据这几个方面的因素，设计了如下的数字水印算法。

4.4.1 算法步骤

（1）水印预处理：

第一步：读取水印图像 W 并进行二值化处理得到二值化图像 B。

第二步：利用 Logistic 模型 $x_{k+1}=\lambda x_k(1-x_k),\quad x_k\in(0,1)$ 对二值化图像 B 进行置乱处理。

第三步：对二值化矩阵进行适当分组，每 8bit 分为一组，使得经过十进制转换后每组数据 $p_i(i=1,2,...,L;L$ 为十进制的个数）在 $(0,q)$ 范围内。

第四步：构造 r-1 次多项式 $h_j(x_j)=(k_i^*+a_1x+a_2x^2+...+a_{t-1}x^{t-1})\bmod q$。

第五步：分别取 n 个不同的 x_j，以每个十进制数 $p_i(i=1,2,...,L;)$ 代替 k_i^* 代入多项式，得到子水印图像 $l_i^j\ (i=1,2,...,L,j=1,2,...,n)$，也就是 n 幅影子图像。

（2）非盲检测水印的嵌入：

第一步：读取载体图像 M 将载体图像 M 进行分块，分成 n 块，每一块为 $m_j,(j=1,2,3,...n)$。分块的原则是每一小块用一个矩阵来表示，并且将每一小块的坐标与图像的坐标相对应，也就是说每一小块用两组参数来表示，这两组参数分别是（beginX,endY）和（beginY,endY）.

第二步：对每一个分块图像 $m_j,(j=1,2,3,...n)$ 分别进行 2 级 haar 小波分解，得到不同子带的小波系数：$(LL2_j,LH2_j,HL2_j,HH2_j,LH1_j,HL1_j,HH1_j)$.

第三步：将水印信息 l_i^j (i=1,2,...L)分别替换到每一块图像 $m_j,(j=1,2,3,...n)$ 的中频系数 $(LH2_j,HL2_j,HH2_j)$ 中。

第四步：对嵌入水印后的每一块图像$m_j,(j=1,2,3,...n)$进行二级 haar 小波逆变换。

第五步：对小波逆变换后的图像$m_j,(j=1,2,3,...n)$进行重组，就可以得到嵌入后的水印图像。

（3）非盲水印检测过程：

第一步：:对已经嵌入的水印图像分成n块子图像$m_j,(j=1,2,3,...n)$。

第二步：:对 n 块子图像分别进行小波 haar 变换，比较嵌入后图像小波变换系数与原始载体图像小波中频系数$(LH2_j,HL2_j,HH2_j)$，得到子水印图像l_i^j。

第三步：计算拉格朗日算子

$n_i=[(i-k)(i-j)]^{-1},n_j=[(j-k)(j-i)]^{-1},n_k=[(k-j)(k-i)]^{-1}$，则有

$$a_0=kjn_il_i+kin_jl_j+ijn_kl_k,$$

$$a_1=-[n_il_i(k+j)+n_jl_j(k+i)+n_kl_k(i+j),$$

$$a_2=n_il_i+n_jl_j+n_kl_k$$

由拉格朗日插值公式：$p^*(x)=a_0+a_1x+a_2x^2$，可得，$k_i^*=a_0$。

第四步：将k_i^*转换为二进制数，这样就得到置乱后的二值水印图像。

第五步: 利用Logistic对置乱后的二值水印图像进行反置乱处理，就提取出了水印图像。

4.4.2 改进算法

在非盲检测水印嵌入算法中，水印的提取需要原始图像，而且在嵌入信息到小波中频系数时如果集中嵌入到中频系数的某一段范围，图像会出现部分失真。另一方面，在嵌入的时候采用替换法进行水印的嵌入处理，当嵌入水印后的图像在受到攻击时，由于嵌入位是确定的，因而如果对特定位进行攻击就很容易使水印信息遭到破坏。在此基础上，设计了盲检测水印算法。

改进的算法的基本思想是采取利用 Logistic 进行随机位置选取嵌入，使得既可以避免出现部分位置失真，又可以防止攻击者对嵌入水印后的图像进行特定位的攻击使得水印被破坏，在改进算法中采用盲检测水印方案。

（1）改进算法中水印预处理：

在改进的算法中，对水印图像的预处理和非盲检测水印预处理上是一致的。

（2）改进算法水印嵌入：

第一步：读取载体图像 M 将载体图像 M 进行分块，分成 n 块,每一块为 $m_j(j=1,2,3,...n)$。

第二步：对每一个分块图像 $m_j(j=1,2,3,...n)$ 分别进行 2 级 haar 小波分解，得到不同子带的小波系数：$(LL2_j,LH2_j,HL2_j,HH2_j,LH1_j,HL1_j,HH1_j)$

第三步：对水印信息 l_i^j，利用 *Logistic* 混沌映射来确定嵌入位置，并用 l_i^j 来代替原来的中频系数 $(LH2_j,HL2_j,HH2_j)$ 中，具体过程如下：

① 选择待嵌入的子块，即选择嵌入空间 $C\{i\},i=1,2,3,....,n)$。

② 设置混沌初值，利用混沌映射计算嵌入的比例位。

③ 根据所选择的嵌入子块和通过混沌所确定的在该子块中的比例位来确定嵌入位置。

第四步：对嵌入水印后的每一块图像 $m_j(j=1,2,3,...n)$ 进行二级 haar 小波逆变换。

第五步：对小波逆变换后的图像 $m_j(j=1,2,3,...n)$ 进行重组，就可以得到嵌入后的图像

（3）改进算法水印检测：

在水印检测过程中，盲水印检测步骤与非盲水印检测步骤基本相同，但是第二步需要修改为：

第二步：对 n 块子图像分别进行小波 haar 变换，提取载体图像小波中频系数 $(LH2_j,HL2_j)$。

第三步：根据嵌入时应用 Logistic 映射确定嵌入点的基本思想，确定每一块中水印嵌入点，提取每一块中的水印信息。

第四步：提取其中的 t 份子水印，根据拉格朗日插值和反置乱进行水印的恢复。

通过上面的改进，可以实现盲检测功能，而且由于嵌入位是通过混沌来随机确定的，攻击者在不知道初始值和混沌映射的情况下增加了攻击难度，理论上是可以提高算法的鲁棒性。

（4）攻击测试基本思想：

攻击测试中提取水印图像的思想是这样的：对于剪切、椒盐噪声攻击鲁棒性测试中，直接通过水印提取算法就能恢复出水印信息；对于旋转、压缩、缩放、中值滤波的鲁棒性测试中，用攻击后的含水印图像的中心部分代替嵌入水印后图像的中心部分，通过这种方式合成的图像中有部分是攻击前的水印图像，一部分是攻击后的水印图像，然后再进行分块，通过检测算法提取出水印图像。

4.5 实验结果与分析

在本算法中，假设载体灰度图像 M，512×512 像素 256 级灰度图像，水印图像 I 为二值图像，大小为 64×64 像素。

在本论文中，我们采用了峰值信噪比（PSNR）和相似度（NC）两个值来进行测评。其中，峰值信噪比（PSNR）表示了嵌入水印前后图像质量的好坏，相似度（NC）表示提取出的水印与原始水印之间的相似程度。

$$PSNR = 10\log_{10}\left[\frac{255}{\sqrt{MSE}}\right] \tag{4.9}$$

$$MSE = \frac{1}{M \times N}\sum_{x=1}^{M-1}\sum_{y=1}^{N-1}(f(x,y) - f_r(x,y)) \tag{4.10}$$

其中，$f(x,y)$ 和 $f_r(x,y)$ 表示原始载体图像和嵌入水印后的载体图像的像素值。PSNR 的值越高，说明嵌入水印后对原始载体图像的影响就越小，水印的不可见性就越高，M,N 表示图像的大小。

另外我们还可以采用归一相关系数 NC 来比较原始水印和提取水印的相似性，用来评价提取出的水印质量的高低，归一相关系数 NC 为：

$$NC = \frac{\sum_{m,n} W_S(m,n)w(m,n)}{\sum_{m,n} w^2(m,n)} \tag{4.11}$$

其中，$w(m,n)$ 和 $W_S(m,n)$ 分别表示原始水印和提取水印的像素值。

（1）参数选择及 shamir 理论验证

在本算法中，取 n=9，t=3,即(3，9)门限方案，在该方案中，根据实验分析，当取不同的 q 时，提取的水印结果如图 10 所示,(a),(b),(c)分别表示取不同的素数 q 时恢复出的

水印图像。由以上结果分析可知，q越大越好，但是存在一定的问题，就是在模q运算后，,则在提取t份水印信息恢复原始数据时，q越大，影响的二进制数据的位数就越多，如果其中有一个错误就会导致最后结果的错误，因而在该算法中，所取的q应该尽可能的小，综合考虑，在本算法中，取q=257。

(a) q=11　　(b) q=255　　(c) q=257

图 10　取不同 q 时恢复出的水印图像

本测试是为了验证 shamir 理论是否可行，根据 shamir 理论(t,n)门限体制，基于 shamir 密钥分存技术可以在得到大于某个值的子密钥后完全恢复出密钥信息，而且在不知 shamir 参数的情况下是很难恢复出原始密钥信息。

（2）shamir 的理论进行验证：

图 11 中，(a)图是嵌入水印后的图像，(b)图是提取 1 份子图$(t=1)$恢复出的水印图像，(c)图是提取 2 份子图$(t=2)$恢复出的水印图像，(d)图是提取 3 份子图$(t=3)$恢复的水印图像。由(b)、(c)、(d)图可知提取少于 3 份子图就不能恢复出水印信息，正好验证了 shamir 理论中的(t,n)门限方案。

图 12 中，由(a)、(b)图可以看出，嵌入水印前后图像的差别并不大，经实验得出，嵌入前后图像的峰值信噪比和提取出的水印与原始水印的相似度分别为：

$$PSNR = 63.6691, NC = 1$$

可见该水印嵌入算法有很好的透明性和不可见性。

(a)原始水印图像　　(b) $t=1$　　(c)$t=2$　　(d)$t=3$

图 11　取出 t 份子图提取的水印图像

(a) 原始载体图像

(b) 嵌入水印后的图像

图 12 载体图像和嵌入水印图像

4.6 算法分析

4.6.1 容量分析

容量测试就是测试水印嵌入算法中最大嵌入水印信息量的测试，由于水印嵌入算法要满足的前提条件是嵌入后的图像与嵌入前的图像在人的肉眼下是分辨不出来，但是如果嵌入的水印信息量越多，这样鲁棒性强，但是载体图像的失真度就越大，这样就满足不了水印的不可见性的要求，达不到信息隐藏的目的和要求，所以容量测试是测试嵌入算法中所能隐藏的最大的水印信息量，是评判一个嵌入算法好坏的一个标准。

从图13上可以看到，随着嵌入容量的增加，峰值信噪比也会相应的降低，所以嵌入容量是有一定的限制。 在本算法中，采用替换法来嵌入水印，在嵌入水印之前，将水印图像的每一点像素值变小，即r=0.001，l(:,:) = l(:,:)*r，嵌入容量必须要综合考虑水印的透明性和水印的鲁棒性。

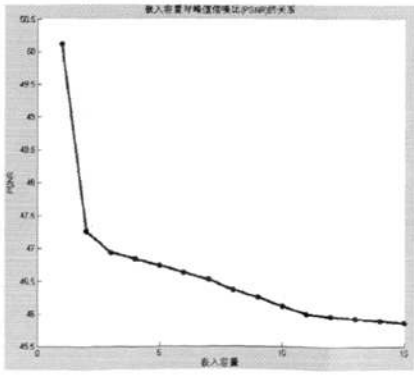


图 13 嵌入容量性能分析

4.6.2 嵌入子带分析

在前面的分析可知图像经小波变换后会得到不同层的小波系数，要实现盲检测水印方案，在进行水印嵌入时，选择系数是很重要的，低频系数比较少，那么嵌入的容量自然会少，而且低频系数对人眼敏感，高频系数是图像的细节部分，大幅度改变细节也会很容易被人眼察觉，而且图像会变得模糊。根据人类视觉特性（HVS）的要求，把信息嵌入到中频部分是比较合适的选择，下面给出了子带分析实验，在试验中，分别把低频，中频和高频子带用相同容量的水印来进行嵌入，然后再逆小波变换得到结果图 14，从图 14 中可以看到，如果水印全部嵌入在低频，那么得到的只有图像的轮廓；如果全部嵌入在高频部分，得到的图像变模糊，而且出现一些噪音；如果将水印信息全部嵌入在中频子带部分，则水印的不可见性较好，对载体图像的影响也较小，所以在本算法中，选择中频子带作为水印嵌入区域。

图 14　嵌入不同子带的水印图像

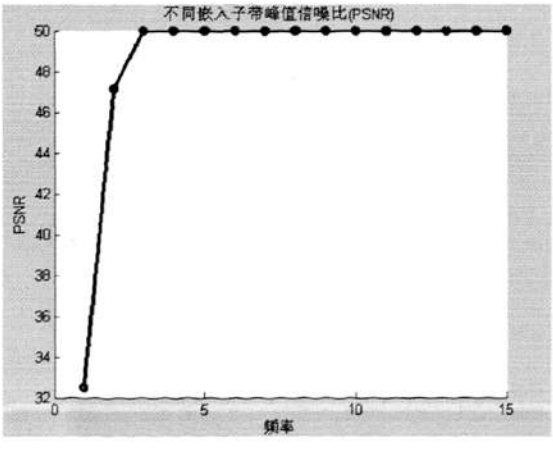


图 15　嵌入不同子带的性能分析图

4.7 鲁棒性测试

由于本算法采用盲检测方案，盲水印的鲁棒性不如非盲水印的鲁棒性，当嵌入水印后的

载体图像受到攻击之后，如果提取整幅受攻击的图像来进行水印的恢复和提取，实验证明：该方法所提取出的水印图像效果不是很好。因此在下面的的攻击测试中，除了裁剪攻击、噪声攻击测试之外，其它几种攻击测试中提取水印图像的思想是这样的：用攻击后的含水印图像的中心部分代替嵌入水印后图像的中心部分，通过这种方式合成的图像中有部分是攻击前的水印图像，一部分是攻击后的水印图像，然后再进行分块，通过检测算法提取出水印图像。通过该思想提取出的水印图像的优点如下：

（1）通过这种合成的方式提取出来的水印图像的效果比直接通过提取算法得到的检测效果要好。

（2）在没有原始载体图像的基础上，通过该思想能够确定该数字作品在传播过程中是否受到攻击。

4.7.1 裁剪攻击测试

裁剪攻击是对嵌入水印后的图像进行裁剪，以图破坏水印信息，使得提取水印信息失败来达到攻击的目的.表 1 给出了嵌入后水印受到不同程度的裁剪后再重新提取水印的分析数据，图 17 给出了峰值信噪比(PSNR)和相似度(NC)的曲线图。

在本攻击测试结果中，PSNR 表示裁剪攻击后的图像和相对应原始载体图像的峰值信噪比，即载体图像在大小选择上和裁剪后的图像大小相同。NC 表示提取出的水印和原始水印的相似程度。

图 16　不同裁剪强度下的图像

从测试结果来看，表 1 给出了不同裁剪强度下的峰值信噪比(PSNR)和相似度(NC)，图 17 为裁剪测试的性能分析结果，这些结果表明，裁剪强度越大，峰值信噪比越低，但是提取出来的水印图像效果较好，从理论上讲，根据 shamir 理论的门限方案，只要取出其中 3 块就可以会恢复出水印，也就是说只要剪切后的图像(I_J)和剪切前图像(I)的大小满足关系 $size(I_J) \geq \frac{1}{3} size(I)$ 就能很好的恢复出原始水印图像，证明该算法对抗剪切攻击具有很好的鲁棒性。

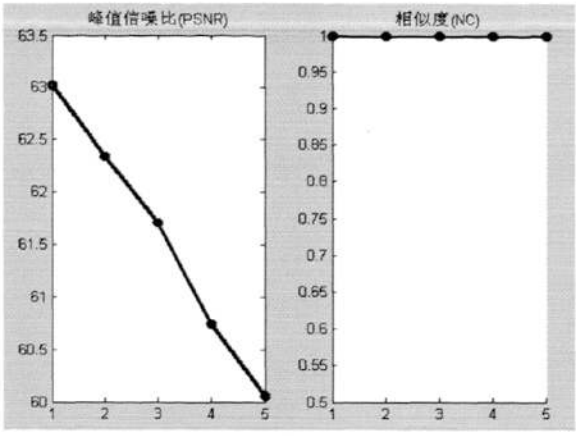


图 17　不同裁剪强度攻击测试性能分析

表 1　裁剪攻击测试结果

裁剪强度	裁剪攻击		
	相似度（NC）	峰值信噪比（PSNR）	提取水印图像
0.39	1	62.7544	水印信息
0.45	1	62.0851	水印信息
0.51	1	61.3902	水印信息
0.58	1	60.4216	水印信息
0.63	1	59.7316	水印信息

4.7.2　旋转攻击测试

对嵌入水印后的图像进行不同角度的旋转旋转攻击，在做旋转攻击测试时，将攻击后的水印图像反向旋转同样的角度，由于此时图像的尺寸变大，要对图像进行裁剪，裁剪的要求是尽可能地保留中心点附近的像素，并且图像被裁去部分还要进行填充处理。

表 2 给出了嵌入水印后的图像受到不同程度的旋转攻击后再重新提取水印的分析数据，图 19 给出了旋转攻击测试中峰值信噪比(PSNR)和相似度(NC)分析结果。

在本攻击测试结果中，PSNR 表示旋转攻击之后的图像和原始载体图像的峰值信噪

比，NC 表示提取出的水印图像和原始水印图像之间的相似程度。

从表 2 和图 18 所得到的测试结果上看，旋转的角度越大，含水印图像的峰值信噪比越低，检测出来的水印的相似度越低。而且从图 19 可以看出，旋转角度超过 10 度，图像峰值信噪比和提取的的水印的相似度下降较快，从某种程度上看，该算法对旋转攻击有一定的鲁棒性，但效果没有期望的好。

表 2　旋转攻击测试结果

旋转角度	旋转攻击		
	相似度（NC）	峰值信噪比（PSNR）	提取水印图像
3	1	37.7361	
5	1	36.4095	
10	1	34.9236	
15	0.9548	34.3518	
20	0.8616	34.0846	

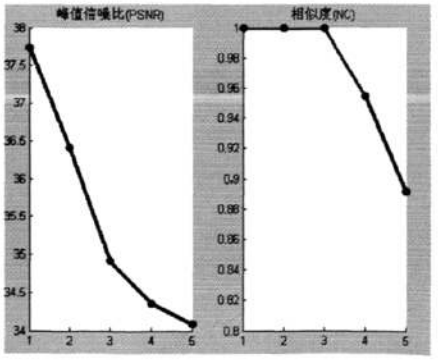


图 18 不同旋转角度攻击测试性能分析

图 19　旋转攻击后的含水印图像

4.7.3　缩放攻击测试

对含水印图像进行不同程度的缩放变换，然后进行检测。在检测时，将缩放后的图像反向缩放同样的系数。表 3 给出了嵌入后水印受到不同程度的缩放后再重新提取水印的分析数据，图 20 给出了峰值信噪比(PSNR)和相似度(NC)的曲线图。

在以下测试结果中，PSNR 表示进行反缩放后的含水印图像和原始图像之间的峰值信噪比，NC 表示提取出的水印图像和原始水印图像的相关性。

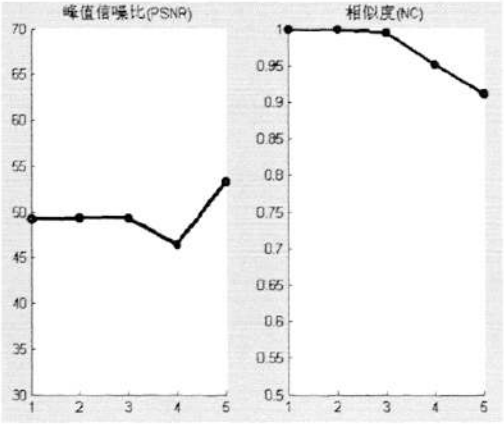
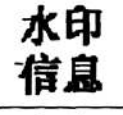


图 21　缩放攻击测试性能分析

表 3　缩放攻击测试结果

缩放系数	缩放攻击		
	相似度（NC）	峰值信噪比（PSNR）	提取水印图像
0.9	1	49.2972	
0.8	1	49.3098	
0.7	0.9942	49.3118	

0.6	0.9510	46.4834	
0.5	0.9109	53.2969	

由图 21 可知，反缩放后的图像和原始载体图像的峰值信噪比较高，从表 3 所得到的测试结果上看，该算法对图像的缩放攻击具有很好的鲁棒性.

图 20 不同缩放比例下的含水印图像

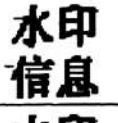
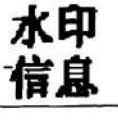
4.7.4 中值滤波攻击测试

中值滤波可以有效地去除脉冲型噪音，对图像的边缘有很好的保护，对图像来说主要是破坏细节部分。 表 4 给出了嵌入后水印受到不同程度的中值滤波后再重新提取水印的分析数据，图给出了峰值信噪比(PSNR)和相似度(NC)的曲线图。

其中：PSNR 表示中值滤波后的图像和原始载体图像的峰值信噪比，NC 表示提取出的水印图像和原始水印图像的相似程度。在测试过程中，攻击后的含水印图像的中心部分的选取与中值滤波窗口大小有关。

通过不同的窗口对含水印图像进行中值滤波攻击，从表 4 和图 23 给出的测量数据来看，选择的窗口越大，进行中值滤波后含水印图像的 PSNR 越小，提取水印图像的相似度越低，而且窗口越大，提取出的水印图像的 NC 下降越快。总体上看，该算法对中值滤波具有很好的鲁棒性。

表 4 不同窗口中值滤波后的测试结果

滤波窗口	中值滤波攻击		
	相似度（NC）	峰值信噪比（PSNR）	提取水印图像
3×3	1	53.8053	
5×5	1	50.7357	

7×7	0.9926	48.9675	
9×9	0.9586	47.8174	
11×11	0.9295	46.9543	

图 22　不同窗口中值滤波后的图像

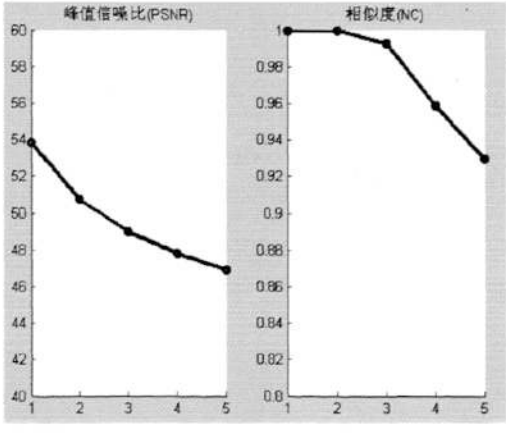


图 23　不同窗口中值滤波后的性能分析

4.7.5　JPEG 压缩攻击测试

JPEG 是压缩图像的标准，JPEG 是有损压缩，通过 JPEG 压缩后的图像再恢复时，眼睛察觉不出损失的变化，所以 JPEG 压缩攻击会对图像的中频部分有影响。 表 5 给出了嵌入后水印受到不同程度的旋转后再重新提取水印的分析数据，图 25 给出了峰值信噪比(PSNR)和相似度(NC)的曲线图。

其中：PSNR 表示压缩攻击后的水印图像和原始载体图像的峰值信噪比，NC 表示提取出的水印和原始水印的相似程度。

图 24　不同有损压缩后的含水印图像

表 5　不同 JPEG 有损压缩测试结果

压缩质量	JPEG 压缩攻击		
	相似度（NC）	峰值信噪比（PSNR）	提取水印图像
98	0.9811	55.4879	
80	0.9804	52.8490	
60	0.9791	51.6405	
40	0.9824	50.8417	
20	0.9807	49.4148	

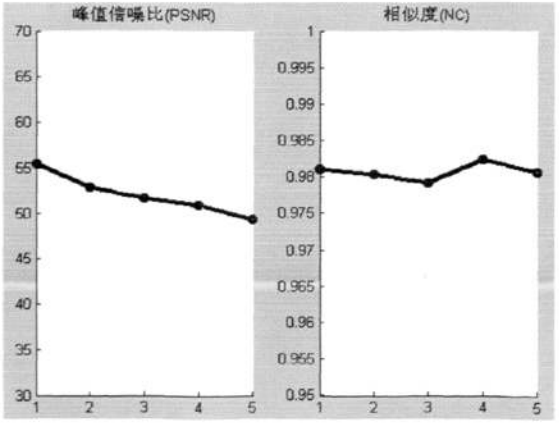


图 25　JPEG 有损压缩测试分析

由表 5 可知，选择不同的压缩因子对含水印图像进行 JPEG 压缩攻击，通过攻击

测试结果图 25 和表 5 给出的测试分析曲线可知，随着压缩因子的不断减小，提取出的水印图像和原始水印图像的相似度较高，而且相似度的变化也不大，说明本算法对 JPEG 压缩攻击具有很好的鲁棒性。

4.7.6 加椒盐噪声攻击测试

噪声攻击就是通过对嵌入水印后的图像进行噪音叠加，通过对嵌入图像加入噪音后，嵌入图像会发生明显的变化，人眼可以觉察出来，而且也会破坏水印信息，噪音攻击是水印攻击的一种方式，不过有时噪音攻击是无意的攻击，在传输过程中会发生这种情况。 表 6 给出了嵌入后水印受到不同程度的椒盐噪声攻击后再重新提取水印的分析数据，图 27 给出了峰值信噪比(PSNR)和相似度(NC)的曲线图。

由表 6 可知，该算法对噪声攻击具有一定的鲁棒性，由图 27 可知，所加的椒盐噪声系数越大，嵌入水印后的图像的质量有所下降，提取的水印图像的质量影响更大一点，但是只要椒盐噪声系数在一定的范围内，该算法还是能很好的抵抗椒盐噪声攻击，实验表明本算法对椒盐噪声攻击具有一定的鲁棒性。

图 26 加不同噪声系数的椒盐噪声后的含水印图像

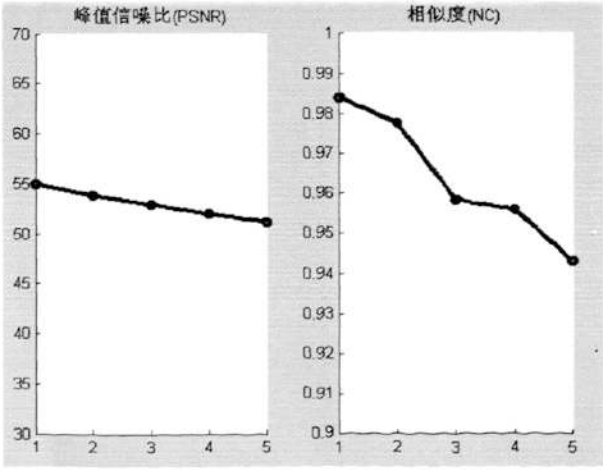


图 27 椒盐噪声攻击测试分析图

表 6 椒盐噪声攻击测试

噪声系数	椒盐噪声		
	相似度（NC）	峰值信噪比（PSNR）	提取水印图像
0.004	0.9842	54.9813	
0.008	0.9776	53.7662	
0.012	0.9583	52.8147	
0.016	0.9561	51.9805	
0.02	0.9431	51.1656	

4.8 本章小结

本章结合 shamir 理论和小波变换原理，提出了基于 shamir 理论门限方案的小波域数字图像水印算法，主要完成了以下工作：

（1）介绍了 shamir 理论秘密分存的思想和具体的分存方案，结合 DWT 变换设计了基于门限方案的水印算法。

（2）在设计内容上，对嵌入子带的选择和嵌入容量的选择做了定量的分析研究，在选择合适的嵌入容量的前提下选择在中频子带上嵌入水印。

（3）给出了水印的非盲检测和盲检测方案，并对盲检测进行了分析研究，通过混沌映射选择嵌入点，由于嵌入点是随机的，因而加强了信息的安全性。在文中给出了具体的算法，并对该算法进行了实验验证和定性分析，对压缩、缩放、旋转、中值滤波攻击后的图像在提取水印的过程中，还必须对该攻击后的含水印图像和嵌入水印后的图像进行特殊的处理才能提取出所隐藏的水印图像。实验表明，该算法对常见的压缩、缩放、加噪声、裁剪、中值滤波攻击有很好的鲁棒性，但是对旋转攻击的鲁棒性一般。

（4）本算法不足之处：在旋转、缩放、压缩、中值滤波攻击后提取时需要嵌入水印后的图像和攻击后的图像进行合成才能提取出较好效果的水印图像，如何将该算法进行

改进，使得在攻击提取时不需要原始载体图像和嵌入水印后的图像就能提取出效果较好的水印图像是下一步研究的方向。

第五章 基于 shamir 理论的 DWT 和 SVD 数字水印算法

5.1 奇异值分解

奇异值分解是最有效分析矩阵的数值分析工具，它是将矩阵对角化的数值算法。任意一幅数字图像，都可以表征为一个由许多非负标量所组成的矩阵，在矩阵的各个元素上，如果利用奇异值分解(SVD)将图像矩阵进行分解，就能够把图像信息集中到奇异阵的少数奇异值上。图像的奇异值具有很好的稳定性，即使图像被施加小的扰动，奇异值也不会有很大的变换。另一方面，奇异值对应于图像的亮度特征，其向量表征了图像的几何特征，奇异值所表现的是图像的内蕴特性而非视觉特性，反应的是图像矩阵元素之间的关系。图像的奇异值对于几何失真具有不变性，因而在数字图像的奇异值中嵌入水印信息几何失真具有很好的鲁棒性。正是由于 SVD 具有这样的一些特点，使得奇异值分解在数字水印领域应用广泛。

小波变换具有良好的分辨率特性和良好的能量压缩特性，奇异值分解很好的稳定性，正是由于 DWT 和 SVD 的这样一些性质，在水印嵌入过程中，可以兼顾水印的不可见性和良好的鲁棒性，同时还能提高水印的嵌入容量，在数字水印算法中，将小波变换和奇异值分解相结合的数字水印算法性能更加优越[40]。

对于任意一个 $M \times N$ 的图像矩阵 $A \in R^{M \times N}$ 可以分解为三个矩阵之积，形如：

$$A = U \sum V^T \tag{5.1}$$

其中，$U \in R^{M \times N}$ 和 $V \in R^{M \times N}$ 都是正交矩阵，V^T 表示矩阵 V 的转置，S 表示元素为非负的对角矩阵：

$$\sum = \begin{bmatrix} \lambda_1 & & & & & \\ & \lambda_2 & & & & \\ & & \cdots & & & \\ & & & \lambda_r & & \\ & & & & \lambda_{r+1} & \\ & & & & & \lambda_m \end{bmatrix} \tag{5.2}$$

其中：r 是 A 的秩，且 $\lambda_1 \geq \lambda_2 \geq \lambda_3 \ldots \geq \lambda_r \geq \lambda_{r+1} \geq \lambda_m = 0$，$\lambda_r$ 是由该分解唯一确定的，λ_r 叫做矩阵 A 的奇异值。$A = U \sum V^T$ 叫做 A 的奇异值分解。

5.2 算法的基本思想

第四章介绍了基于 shamir 理论门限方案的水印算法，采用了盲检测的方案来完成，实验证明该算法具有良好的透明性和不可见性，对于常见的攻击的鲁棒性较强，但是抗旋转攻击的鲁棒性较差，本章算法的目标是设计一种既能有效抗几何攻击，又具有很好的水印的不可见性的数字水印算法。

数字水印一般以版权保护为应用目的，因而要求对水印的鲁棒性较高。针对这一要求，在设计过程中，首先要考虑水印类型的选择，为了提高水印对抗攻击的能力，对水印信息如何加密处理是要考虑的问题；另一方面，选择在哪一种变换域上设计水印算法，选择好变换域后，还要选择水印的嵌入位置，还要考虑抗攻击测试的能力。因此算法主要从这几个方面来考虑和设计。

5.3 算法设计步骤

5.3.1 水印预处理

第一步：读入原始载体图像 I 和水印图像 M ,假设水印 M 图像大小为 $M \times N$ 。

第二步：设置初始值,u_0, μ ，根据 Logistc 映射产生混沌序列 $K \in \{k_1, k_2, ...k_{M \times N}\}$ 。

$$u_{k+1} = \mu u_k (1-u_k), u_k \in (0,1) \tag{5.3}$$

第三步：利用混沌序列 K 对水印图像 M 按照式（5.3）采用异或方法进行置乱，置乱后的水印图像为 M_L 。

即 $M_L = K \oplus M$

经混沌加密后的水印图像如图 28（b）所示:

(a)原始水印图像　　(b)加密后的水印图像

图 28　原始水印和加密水印

5.3.2 水印分存：

根据 shamir 理论中的(t,n)门限体制构造多项式如式(5.4)所示：

$$f(t)=(a_0+a_1t+a_2t^2+...)\bmod q \tag{5.4}$$

由该多项式生成影子图像$M_{Li}(i=1,2,3,...n)$，生成影子图像的方式如图 29 所示：本算法中影子图像的分存方式和上一章中在分存方法上略有不同。在本算法中，每次选取置乱后的水印图像中的 2 个像素，作为式(5.4)中的系数a_0,a_1，如果要把水印图像分成 4 个影子图像，则表达式（5.4）中的t取不同的四个数，这样就得到了 4 个不同的$f(t_i)$,其中$t=1,2,3,4$,将这 4 个不同的值存放在 4 幅影子图像的相应位置，这样就实现了水印图像的分存处理。

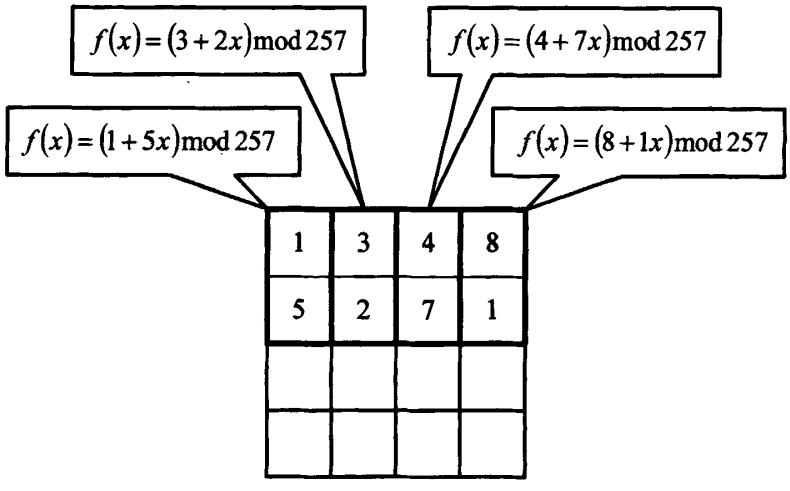


图 29 原始图像分块

这里假设分为 4 份影子图像，如图 30 所示：

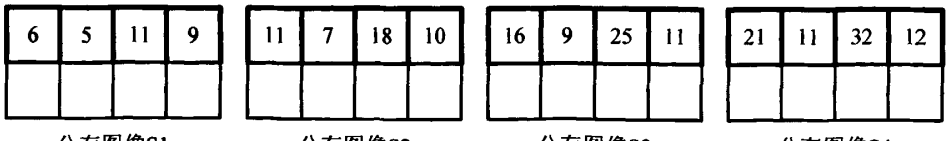


图 30 分存图像 s1, s2, s3, s4

假设置乱后的水印图像为大小64×64像素，按照上述分存方式进行水印分块处理，如果要分存为 4 块，这样分存后的影子图像大小为64×32，分存后的影子图像为图 31 所示:

(a) (b) (c) (d)

图 31 分存后的影子图像

5.3.3 水印嵌入

第一步：将载体图像 I 采用 haar 小波进行一级小波变换，即 $I_W = DWT(I)$，得到低频子带图像 LL，水平细节子带图像 HL，垂直细节子带图像 LH，和斜向细节子带图像 HH。

第二步：选择低频子带 LL 进行奇异值分解；$LL \rightarrow USV^T$，可以得到正交矩阵 U,V 和对角矩阵 S。

第三步：将分存后的 n 幅子水印图像 M_{Li} 拼接成一幅水印图像 $M_L^{'}$，要求 $size(M_L^{'}) \le size(LL)$,如果 $size(M_L^{'}) < size(LL)$，则对 $M_L^{'}$ 做填充补零处理，要求 $size(M_L^{'}) = size(LL)$。

第四步：将水印信号 $M_L^{'}$ 嵌入到载体图像中，选择经小波变换后的低频子带进行嵌入，在低频分量的对角矩阵 S 上嵌入水印,即

$$S^{'} = S + \alpha M_L^{'},$$

其中，α 为嵌入强度,$S^{'}$ 为嵌入水印后的对角矩阵。

第五步：对嵌入水印后的对角矩阵 $S^{'}$ 进行奇异值分解，即

$$S^{'} \rightarrow U_1 S_1 V_1^T$$

第六步：由 U, S_1, V^T 获得嵌入水印后的水印图像 $LL^{'}$，即

$$LL^{'} = US_1V^T$$

嵌入水印后的 LL 子带图像如图 32 所示：

第七步：将得到的 $I_W^{'}$ 进行小波逆变换,这样就得到了嵌入水印后的图像 $I^{'}$。

$$I^{'} = IDWT(I_W^{'})$$

嵌入水印后的LL子带图像

图 32 嵌入水印后的 LL 子带图像

5.3.4 数字水印提取

水印提取算法大致是嵌入算法的逆过程

第一步：对嵌入水印后的图像 $I^{'}$ 都进行一级 *haar* 小波变换，分别得到不同分辨率下的低频子带图像 $LL^{'}$，水平细节子带图像 $HL^{'}$，垂直细节子带图像 $LH^{'}$，和斜向细节子带图像 $HH^{'}$。

第二步：对低频子带 $LL^{'}$ 进行奇异值分解，$LL^{'}=U_2S_2V_2$,得到正交矩阵和对角矩阵。

第三步：根据嵌入算法中的第五步，进行运算，可以得到 $D=U_1S_2V_1^T$。

第四步：根据水印嵌入算法中的第四步种的 S,α,可以得到置乱后的子水印图像，

$$W^{'}=\frac{1}{\alpha}(D-S)$$

第五步：从 $W^{'}$ 中抽取两块子图恢复出水印图像。具体方法可以参照 4.2 节所介绍的有限域拉格朗日插值方法进行水印的提取。具体可以描述如下：以图 33 的分存结果为例，介绍提取水印的过程。

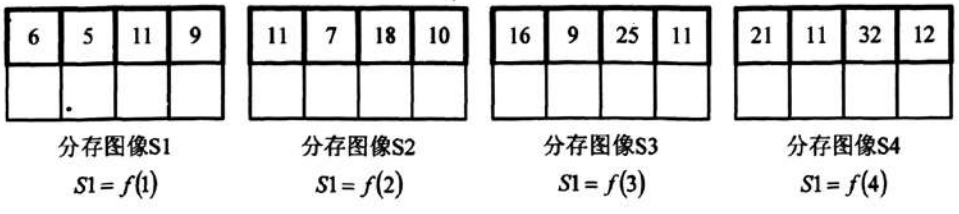


图 33 分存的影子图像

假设我们在提取的时候选取两个影子图像来进行水印的恢复和提取，在这里我们可以提取分存图像S_2, S_3来进行秘密水印图像的恢复：

根据分存原理：$\begin{matrix}(a_0+2a_1)\bmod 257=11\\(a_0+3a_1)\bmod 257=16\end{matrix}$，

解该方程组可得$\begin{cases}a_0=1\\a_1=5\end{cases}$，所以由分存图像$S_2$和$S_3$中的第一个元素就能恢复出原始水印图像中的第一块子水印信息，依此类推，分别取S_2和S_3中的第2、3、4个元素第按照同样的算法进行计算就可以恢复出原始水印图像中的第2、3、4块子水印信息。所以只要提取t份子水印就能实现秘密信息的恢复和提取。

5.4 实验结果与分析

本算法中，原始载体图像I大小为512×512的256级灰度图像，水印图像M大小为64*64的二值图像，门限方案为(2,4)门限方案，即$t=2, n=4$，至少取出其中2份水印就能恢复出原始水印；门限素数经实验验证取$q=257$。本算法选取嵌入强度$\alpha=0.15$，所得到的嵌入水印后的图像和提取水印后的图像如图34所示：

(a)原始载体图像

(c) 嵌入水印后的图像

(b)原始水印图像

（d）提取出的水印图像（NC=0.9832）

图34 原始载体图像和嵌入水印效果图

从图 34 可以看出，嵌入水印后对原始载体图像的影响较小，通过该算法提出的水印图像效果较好。

5.4.1 剪切攻击测试

（b） 剪切右上角

（b）剪切左下角

（c）剪切右下角

图 35 剪切攻击后的水印图像和提取出的水印图像

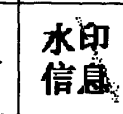
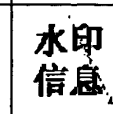
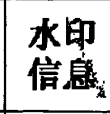
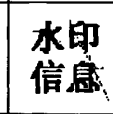
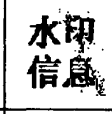
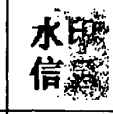
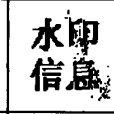
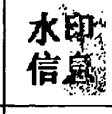
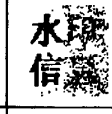
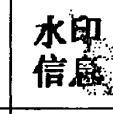
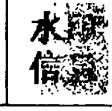
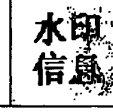
从不同的角度对嵌入水印后的图像进行剪切攻击测试，从图 35 可以看出，该算法

对于剪切攻击有一定鲁棒性。

5.4.2 抗噪声攻击测试

对嵌入水印后的图像分别加以高斯噪声、乘积性噪声、椒盐噪声，其噪声系数分别为 0.001，0.0015，0.01，0.015，0.02，得到的结果见表 7 所示:

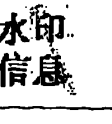
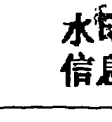
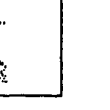
表 7 抗噪声攻击测试结果

噪声系数	椒盐噪声			高斯噪声			乘积性噪声		
	NC	PSNR	提取图像	NC	PSNR	提取图像	NC	PSNR	提取图像
0.001	0.9572	34.3133		0.9437	29.6454		0.9633	36.7735	
0.005	0.9431	33.2014		0.9153	27.8737		0.9621	35.0183	
0.01	0.8917	24.7120		0.7064	19.8292		0.9002	26.7862	
0.015	0.8194	23.1082		0.6736	18.1708		0.8810	25.0492	
0.02	0.7853	21.6677		0.6185	17.0208		0.8383	23.7952	

由表 7 可知，采用本算法对原始载体图像嵌入水印后，对嵌入水印后的含水印图像分别加以椒盐噪声、高斯噪声和乘积性噪声后，提取出的水印图像效果良好，由此可见，该算法对抗噪声攻击具有良好的鲁棒性。

5.4.3 旋转攻击测试

表 8 旋转攻击测试结果

旋转角度	20	40	50	70
相似度（NC）	0.8972	0.8869	0.8947	0.8884
提取出的水印图像				

(a)含水印图像旋转 20 度

(b)旋转 20 度提取出的水印图像

(c)含水印图像旋转 45 度

(d)旋转 45 度后提取出的水印图像

(e)含水印图像旋转 60

(f)旋转 60 度后提取出的水印图像

图 36 旋转攻击测试

对含水印图像分别旋转 20 度，40 度，60 度,80 度后提取出来的水印图像和原水印图像的相似度如表 8 所示：由图 36 和表 8 的旋转攻击测试结果看，该算法对旋转攻击具有很好的鲁棒性。

5.4.4 图像增强攻击测试

对嵌入水印后的图像分别进行图像增亮，图像变暗、图像增加对比度、图像降低对比度，图像直方图均衡化攻击后，所得到的嵌入水印后的图像和提取出的水印图像如图37、38、39、40、41所示：


图37 图像变亮后的含水印图像和恢复出的水印图像


图38 图像变暗后的含水印图像和提取出的水印图像


图39 直方图均衡化后的含水印图像和提取出的水印图像

图 40 增加对比度后的含水印图像和提取出水印图像

图 41 降低对比度后的含水印图像和提取出的水印图像

表 9 图像增强攻击测试结果

攻击类型	图像增亮	图像变暗	增加对比度	降低对比度	直方图均衡化
攻击后图像 PSNR	11.3718	25.2124	13.7026	20.2233	16.2307
提取水印图像 NC	0.6377	0.9537	0.6147	0.6419	0.5785

5.4.5 中值滤波攻击测试

对嵌入水印后的图像在3×3的邻域窗中进行中值滤波，所得到的图像如图 42 所示。

经实验验证，经中值滤波后，载体图像的峰值信噪比 (*PSNR*) 为 41.0693，水印图像的相似度 (*NC*) 为 0.9441。由此可见该算法对中值滤波的攻击具有良好的鲁棒性。

图 42　中值滤波后的图像和提取出的水印图像

5.4.6 JPEG 压缩攻击测试

对嵌入水印后的图像进行 JPEG 有损压缩实验，对压缩后的水印图像进行水印检测。图 43 是在压缩因子为 0.8 的时的含水印图像和根据本算法提取出来的水印图像。

图 43　压缩质量因子=0.8

在不同的压缩比下，对嵌入水印后的图像进行 JPEG 有损压缩，所提取出来的水印图像和原始水印图像的相似度见表 10 所示：

表 10　JPEG 有损压缩攻击测试结果

压缩因子	0.9	0.8	0.7	0.6
相似度（NC）	0.9750	0.9714	0.9710	0.9689

由以上实验结果可知，提取出来的水印和原始水印有很高的相似度，足以证明该算法对 JPEG 压缩攻击有很好的鲁棒性。

5.5 本章小结

本章结合 shamir 理论门限方案，针对第四章提出的算法对旋转攻击的不足，设计了基于小波域和奇异值分解的数字水印算法。

（1）采用混沌序列对原始水印图像加密处理，采用 Logistic 混沌映射对水印图像置乱出来。

（2）根据 shamir 理论的门限体制，对水印图像进行了分存处理，分存的方法和第四章中的分存方法略有不同，构成（2，4）门限方案。

（3）在 DWT 域结合奇异值分解进行水印嵌入算法的设计，并由 shamir 理论中的拉格朗日插值实现了水印的提取，实验表明：该嵌入算法具有很好的透明性和不可见性，另一方面，在提取 $s(t \le s \le n)$ 份子水印的情况下就能恢复出原始水印信息。

（4）对该算法进行了攻击测试，攻击测试结果表明：该算法对剪切、加噪、旋转、压缩等攻击具有很好的鲁棒性，是一种可行的数字图像水印算法。

总结与展望

随着网络技术和计算机信息技术的飞速发展，人类社会已经进入个一个全新的数字信息化时代。以数字媒介为载体的作品由于其获取容易、复制简单和传播迅速等优点，极大的丰富了人类的生活。但是利用网络的开放性和共享性所进行的一些恶意的行为，比如侵犯版权，信息篡改等，严重的损害了数字作品的创作者和使用者的利益，因此，对多媒体数字信息合法持有人的权益保护问题就成了当今数字技术的一个重要研究课题。

1、本文主要研究工作

本文主要对静态图像的水印技术进行了研究，主要工作如下：

（1）分析了 shamir 理论的及其门限方案。提出了基于 shamir 理论的小波域数字水印算法，利用秘密共享信息分存的思想将秘密信息嵌入载体图像中。在该算法的基础上上，改进了以往采用非盲检测的图像水印方案，通过混沌置乱来选择水印嵌入点，将分存的水印信息嵌入到相应的嵌入点，采用盲检测实现水印提取和恢复。实验证明：该算法对数字图像水印不仅具有较好的不可见性，在进行攻击测试时，需要将攻击前后的图像进行特殊处理才能提取出水印图像，而且对图像的噪声，压缩，剪切具有较好的鲁棒性。

（2）为了提高对旋转攻击的鲁棒性，提出了基于 shamir 理论的 DWT 和 SVD 的水印方案，实验证明，该算法嵌入和提取效果都比较理想具有很好的鲁棒性。

（3）本文采用两种方案来实现水印的算法，一种方案是盲检测方案，一种是非盲检测方案，相同点就是应用了 shamir 理论的信息分存思想，前者在对抗攻击时需要对攻击前后的图像进行特殊处理才能检测出水印信息，通过实验验证，该检测方案的鲁棒性效果良好；后者在对抗常见的攻击时不需要对攻击前后的图像进行特殊处理，通过提取算法就能直接提取出水印信息，该算法的鲁棒性较好。

2、展望

尽管数字水印技术的发展日新月异，各种算法层出不穷，但是仍然还有很多的工作有待进一步的努力，来不断的完善这一领域。本文提出的算法再有些方面存在不足，今后应该在这几个方面不断加以改进：

（1）针对本文中提出的盲水印方案，由于本身盲水印的鲁棒性比较弱，因而根据本文算法，嵌入水印后的图像不受到任何攻击的时候，水印提取效果很好；但是一旦受

到攻击，采用原来的直接检测的方案，水印信息提取出来效果非常不好，因而在检测之前必对攻击前后的水印图像进行了处理。在以后的研究工作中，尽可能的找到一种算法，该算法对攻击后的水印提取不需要原始载体图像和嵌入水印后的载体图像，实现真正的盲检测，这是以后需要研究的问题。

（2）在本文所提出的算法中，水印的嵌入强度都是确定的，在以后的研究工作中，应该根据载体图像不同的特性，根据载体图像的灰度值或者是小波变换后的系数的不同，嵌入不同强度的水印信息，使得嵌入的数字水印的强度可以根据载体图像进行必要的自适应。

（3）将 shamir 理论的秘密共享信息分存的思想应用到彩色图像领域也是需要考虑的问题。

（4）找出传统的 shamir 门限方案的图像分存算法的不足，然后进行改进，从而使得算法更具有安全性。

参考文献

[1]孙圣和，陆哲明，刘夏木等著. 数字水印技术及应用[M]. 北京：科学出版社，2004

[2]黄继开，谭铁牛. 图像隐性水印综述[J]. 通信学报，2000，26(5)：643-653.

[3]刘瑞祯，谭铁牛. 数字图像水印研究综述[J]. 通信学报，2000，21(8)：39-48.

[4]Mauro Barni, Franco Bartolini, Teddy Furon. A general framework for robust watermarking security [J]. Signal Processing, 2003,35(6): 2069-2084

[5]Ingemar J.cox, Matt L.Miller. The first 50 years of electronic watermarking[J]. EURASIP Journal on Applied Signal Processing, 2002,12(10): 126-132

[6]Bellovin S M, Cheswick B, Keromytis A D. Worm Propagation Strategies in an IPv6 Internet [EB]. Login: Magazine. 2006,31(1):70-76.

[7]Wolfgang R B and Delp E J. A watermark for digital images[A]. Proc IEEE Int. Conference on Image processing[C], Lausanne, Switzerland,2006:219-222

[8]Yang C C, Chang T Y, Hwang M S. A(t,n) multisecret sharing scheme[J]. Applied Mathematics and Computations,2004,151(2):483-490

[9]Miller M L, Cox I J, dBloom J A. Informed embedding: Exploiting image and detector information during watermark insertion[A]. IEEE International Conference on Image Processing[C], 2000.201-203

[10]Niu X M,Sun S H. Digital watermarking of still images with gray-level digital watermarks[J]. IEEE Transactions on Computer Electronics, 2000,46(1): 137-145

[11]Tao B and Dickinson B,Adaptive watermarking in the DCT domain[J]. Proc. IEEE International Conference on Image Processing, Lansanne, Switzerland, September 1996:51(1): 25-28

[12]Mauro Barni,Franco Bartolini, Alessandro Piva. Improved wavelet based watermarking Through Pixel wise Masking[J]. IEEE transactions on image processing 2001, 5(10):783-791

[13]Cox I J,Killian J,Leighton F T,etal.Secure spread spectrum watermarking for multimedia[J].IEEE Transactions on Image Processing,1997,6(1): 1673-1687.

[14]Koch E,Zhao J. Embedding robust labels into images for copyrity protection[A].

In:Proceedings of the knowtight'95 conference on intellectual property rights and new technologies[C]. Vienna,Austria, 1995: 241-251

[15]Naoki, Masud, Kazuyuki, Aihara.Crytosystems With Discretized Chaotic Maps[J].IEEE trans Circuit and Systems,2002,49(1):28-40

[16]Podilchuk C I, Zeng W. Image-adaptive watermarking using visual models. IEEE Journal on selected areas in communiction, 1998, 16(4):525-539

[17]Jian Zhao，Qin Zhao， Mingquan Zhou，Jianshou Pan,A Novel Wavelet Watermark Algorithm Based on Neural Network Image Scramble[J]. Lecture Notes in Computer Science, 2005(8), 346-350

[18]Hernandez J, Amado M and Perez-Gonzalez F. DCT-domain watermarking technique for still images:Detector performance analysis and a new structure[J]. IEEE Trans . on Image Processing,2000,9(1):53-68

[19]赵健，周欣，周明全,非线性技术数字水印研究发展现状与展望[J], 北京邮电大学学报.2005(28)：112-114

[20] Jian Zhao，Mingquan Zhou，Nonlinear Watermark Techniques Application In Digital Librarie[J]，Journal of Electronics.2005. 22(5)：524-527

[21]赵健，周明全， DCT 变换数字水印改进算法软件实现[J].计算机应用与软件.2006.23(8)：52-53

[22]牛少彰，扭心忻，杨义先. 基于拉格朗日插值公式的数字水印分存算法[J].北邮电大学学报. 2003.9(3): 143-245

[23]李笑平. 硕士学位论文：基于小波变换的数字水印技术研究[D]. 华中科技大学.2006.5

[24]刘九芬，黄达人，胡军全.数字水印中的正交小波基[J]. 电子与信息学报，2003.25(4)：453-459

[25]牛少彰，扭心忻，杨义先. 基于 Shamir 秘密共享方案的数字水印算法[J]. 中国图像图形学报..2003.8(10).1178-1182

[26]Kundur D and Hatzinakos D. A robust digital image watermarking method using wavelet based fusion[A]. IEEE International Conference on Image Processing[C], Santa Barbara, CA, 2002:544-547

[27]Kundur D and Hatzinakos D. Digital watermarking using multiresolutions wavelet decomposition[A]. IEEE International Conference on Acoustic, Speech and Signal Processing[C], Seattle, Washington, USA, 2003,56(9):2969-2972

[28]Kundur D. Multiresolution digital watermarking:algorithms and implications for multimedia signals[R]. Ph. D. Thesis. Dept. of Electrical &Computer Engineering, University of Toronto,August 1999

[29]赵健，俞卞章，彭进业，许家栋.秘密共享方案的小波混沌数字水印算法[J]. 系统仿真学报,2007,19(22): 5347-5350

[30]Jian Zhao， Bianzhang Yu， Research and Development on Image Processing of Wavelet and Fractal Based, Dynamics of Continuous, Discrete and Impulsive Systems [J]: Applications and Algorithms.13: 987-991 Part 3 Suppl. S, DEC 2006, 987-991

[31]赵健，周明全. 改进的小波域混沌数字水印算法实现[J]. 光子学报. 2004. 33(10): 1236-1238

[32]Jian Zhao, Mingquan Zhou, Hongmei Xie, Jinye Peng, Xin Zhou. A Novel Wavelet Image: Watermarking scheme Combined with Chaos Sequence and Neuran Network[A]. Lecture Notes in Computer Science. 2004,vol 3174: 663-668

[33]周欣 基于 Shamir 理论的小波域数字水印技术研究[D].西北大学.2006,5

[34]石润华，仲红，黄刘生. 动态的多重秘密共享方案[J]. 计算机工程.2008 12(8):23-25

[35]胡志川. 基于小波域的图像数字水印研究[D]. 山东师范大学. 2007,5

[36]袁源，丁莹，李炳发. 数字水印的确定性攻击方法及其解决方案[J]. 计算机应用研究，2005.12(3)：143-146

[37]王慧琴，李人厚，曹毓秀等. 一种数字水印技术反攻击系统研究[J]. 计算机应用研究，2004.8：105-106

[38] 钟桦，张小华，焦李成. 数字水印与图像认证——算法及应用[M]. 西安：西安电子科技大学出版社.2006：3-177

[39]胡春强. 图像分存算法的研究与实现[D]. 重庆大学.2009,3

[40]方旺盛. 赖晓芳.基于 shamir 秘密共享的整数小波联合数字水印算法[J]. 江西理工大学学报，2009.30(4):29-32

[42]林瑞娟. 小波域图像数字水印算法研究[D]. 山东师范大学，2007,5

攻读硕士学位期间取得的科研成果

1、 林晓圆，赵健，谢瑜，余秋菊. 图像拟仿射变换的 DWT 水印算法. 计算机工程与应用（已录用）

2、于 2008~2009 参与了陕西省科技厅自然科学基金项目，项目名称：基于分形理论的图像理解研究，项目编号：2007F38，立项单位：西北大学，立项时间：2007~2009，我参与该项目时间：2008~2009，主持人：郭秀梅（导师赵健排第二）

致谢

光阴似箭，三年紧张而又充实的研究生生活即将结束，在硕士论文完成之际，我向所有支持、关心、和帮助过我的人表示诚挚的谢意。

感谢我的导师赵健副教授三年来的谆谆教诲。在我的学习生活中，赵老师自始自终给予我细致的指导和严格的要求，他是我的良师益友。赵老师严谨的治学态度、兢兢业业的工作精神、待人真诚的为人品质是我今生学习的榜样。赵老师在我学习期间不仅传授了做学问的方法，还 授予了做人的准则，这些都将使我终身受益。无论是在理论学习期间，还是在论文的选题、查阅资料、开题、研究和撰写的每一个环节，都得到了导师的悉心指导和帮助，才使得论文得以完成。在此，瑾向导师致以最诚挚的谢意。

同时还要感谢共同学习、讨论和生活的同学林晓园、刘媛及 2008 级的师弟师妹们在学习讨论中的同理合作，也感谢她们在长期的学习生活中给予的支持、理解和帮助！

最后，我要感谢我的父母和家人，多年来他们的默默支持、他们的理解和信任、他们的关怀和疼爱、他们的殷切期盼，一直都是我前行的最大动力、没有他们，就没有我现在的一切。

在此，我再最后一次衷心的感谢所有关心、支持和帮助过我的亲人、老师、同学和朋友！

路慢慢其修远兮，吾将上下而求索。

最后以一句诗词结束本文：书山有路勤为径，学海无涯苦作舟。