分类号：TP13 学号：016096236

西北工业大学

硕士学位论文

（学位研究生）

题目 基于图像的信息掩密技术

作者 姚辉灿

指导教师 慕德俊 专业技术职务 教授

学科（专业） 控制理论与控制工程

西北工业大学自动化学院

2004 年 3 月 14 日

摘要

信息隐藏技术可以被广泛地应用于保密通信、版权保护、数字票据防伪等领域，对信息隐藏技术的研究具有重要的实用价值。

目前大部分的研究工作集中于数字水印技术，而用于秘密通信的掩密术则较少有人涉及。本文对信息隐藏领域的另一个重要方向——掩密技术进行了研究，着重讨论了其在数字图像中的应用。

首先，介绍了信息隐藏的相关基本知识。然后，分别在空间域和 DCT 域对于以静止图像为载体的信息隐藏技术进行了探讨。

在空间域内，利用人的视觉特性，我们提出了基于图象方差、图象平坦测度、模糊分类的隐藏算法，同时提出了基于差值矩阵的信息隐藏，。

在频率域内，研究了基于 DCT 变换的信息隐藏技术，提出了改进的 DCT 自适应隐藏算法、DCT 域奇偶性嵌入方法和改进的融合算法，同时提出了差值矩阵的 DCT 域的隐藏算法，给出了这些算法的信息嵌入与恢复过程，并对频率域内的这些隐藏算法的鲁棒性进行了分析。

关键字：信息隐藏　　掩密术　　数字图像　　数字水印

Abstract

Information hiding techniques can be used in the fields of covert communication, copyright protection, digital receipt anti-counterfeiting, and so on. It's of great value to study them.

At present time, most of the studies focus on digital watermarking techniques, and few are done on steganography, one of the most important directions in the field of information hiding,. This thesis concerns the steganography. We also place emphasis on its applications in digital images.

Firstly, the relative basic knowledge of information hiding are presented, and then the techniques of digital images based information hiding in the domain of spatial and DCT (Discrete Cosine Transform) respectively.

In spatial domain, according to the characteristics of HVS (Human Visual System), we introduce several approachs based on images' deviation, images' flatness measurement, fuzzy classification, and an approach based on difference matrix as well.

In frequency domain, we research DCT based information hiding techniques, and then give an adaptive technique, and a parity based approach in the DCT domain, and an approach based on improved integration algorithm. We also propose an approach based on difference matrix in DCT domain, and show all the approachs to embed/detect the secret messages, and their robust analysises.

Key words: information hiding, steganography, digital image，digital watermarking

目录

第一章 绪论

§1.1 引言

Internet 是一个开放系统，以方便、广泛、快捷的信息交流为目的，必须为普通用户提供便捷的访问方式，网络在给人们带来便利的同时也暴露出越来越严重的安全问题。例如，多媒体作品的版权侵犯、软件或文档的非法复制、电子商务中的非法盗用和篡改、网络中信息的非法截取和查看、甚至是黑客攻击等等。毫无疑问，网络中的信息安全问题是现在乃至未来相当长时期内的研究热点之一。

多年以来，已有的安全体制主要建立在密码技术之上。密码技术可以分为私钥和公钥两种加密体制。私钥加密体制因其密钥量大而难以大面积使用，因此目前的网络中广泛采用的是公钥加密体制。后者利用了“ 计算安全性 ”原理，一旦计算机的性能大幅度提高则会对其构成威胁[1]。因为加密通信容易引起对手的猜疑及感知“ 机密信息 ”的存在，这种通信方法在敌对环境下，很容易导致强大的对手动用各种手段破密，即使在短时间内不能破密，也已经使通信双方的位置或身份信息基本暴露，从而导致此后的通信处于对手的监控之下，此时就意味着通信的安全已经受到损害。

可喜的是，近年来国际信息技术研究领域出现一个新的研究方向——信息隐藏技术——将会给网络化多媒体信息的安全保存和传送开辟了一条全新的途径。该技术与密码技术的不同点在于：密码技术隐藏信息的“ 内容 ”而信息隐藏技术则隐藏信息的“ 存在性 ”。信息隐藏技术可以隐藏“ 机密信息 ”的存在，确保通信双方在交换信息时不受对手猜疑。信息隐藏比信息加密更为安全，因为它不容易引起攻击者的注意。信息隐藏是把机密信息隐藏在其它无关紧要的信息中形成隐秘信道，除通信双方以外的任何第三方并不知道秘密通信这个事实的存在，信息加密从“ 看不懂 ”变为“ 看不见 ”，转移了攻击者的目标。如果两种方法综合使用，先把重要信息加密，再将之隐藏，则是保证信息安全的更好方法。

§1.2 信息隐藏的学科分支

信息隐藏现在已经成为一门新兴的、拥有许多分支的学科。信息隐藏，对应的英文术语是 Information Hiding，是利用人类感觉器官的不敏感(感觉冗余)，以及多媒体数字信号本身存在的冗余(数据特征冗余)，将信息隐藏于一个载体信号(掩护体)中，不被觉察到或不易被注意到，而且不影响载体信号的感觉效果和使用价值。

参考[2]，信息隐藏的主要学科分支包括：掩蔽信道、匿名技术、掩密术、数字水印技术。

- 信息隐藏
  - 掩蔽信道
  - 掩密术
    - 语言掩密
    - 技术掩密
  - 匿名
  - 数字水印
    - 鲁棒水印
    - 易损水印

掩蔽信道(Covert channel)，可理解为“隐蔽的信道”，是指这些通道一般被运用于不可信程序，当对别的程序执行操作时，将有关信息泄露给不可信程序的拥有者。掩蔽信道一般存在于多级保密系统的背景之中。

匿名(Anonymity)，就是设法隐藏消息的来源，即隐藏消息的发送者和接受者。

掩密术(Steganography)，Steganography 源于希腊文，字面意思是“隐写(covered writing)”，该技术侧重于用掩护体去掩盖秘密信息。掩密术是信息隐藏的一个重要学科分支。密码术从事秘密信息内容的保护，而掩密术从事秘密信息存在的隐蔽。

数字水印(Digital Watermarking)，是用来证明一个数字产品的拥有权、真实性，成为分辨真伪的一种手段。数字水印一般隐藏于数字化产品(图片、音频、视频、文本等)之中，人们不易感知，只能通过数据处理来识别、读取。

本文主要就掩密术及数字水印进行研究。本文以后章节如非特别声明，信息隐藏均指掩密术及数字水印。信息隐藏是一门跨学科跨专业的研究领域。

(1) 从它的研究方法来看，它与数学、生理学、电子学、计算机科学等

许多学科可以相互借鉴；

(2) 从它的研究范围来看，它与模式识别、计算机视觉、计算机图形学、密码学等多个专业又互相交叉。

如今信息隐藏学作为隐蔽通信和知识产权保护等的主要手段，正得到广泛的研究与应用。

§1.3 信息隐藏技术简介

信息媒体的数字化为信息的存取提供了极大的便利性，同时也显著地提高了信息表达的效率和准确性。特别是随着计算机网络通讯技术的发展，数据的交换和传输变成了一个相对简单的过程。人们借助于计算机、数字扫描仪、打印机等电子设备可以方便、迅速地将数字信息传达到世界各地。随之而来的副作用是通过网络传输数据文件或作品使有恶意的个人或团体有可能对一些机密的文件进行窃取、攻击或破坏，因此如何在网络环境中实施有效的信息安全手段成为一个迫在眉睫的现实问题。人们常常认为通信安全的实现可以通过加密来完成。即首先将数据文件加密成密文后发布，使得网络传递过程中出现的非法攻击者无法从密文获得机密信息，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。因为信息经过加密后容易引起攻击者的好奇和注意，容易遭到攻击和破坏。密码学一直被认为是在通信研究领域中主要的信息安全手段并受到极大重视，但是加密方法有一个很大的缺点，那就是它明确地提示攻击者哪些是重要信息，容易引起攻击者的好奇和注意，并有被破解的可能性，而且一旦加密文件经过破解后，其内容就完全透明了。或者，攻击者可以在破译失败的情况下将信息破坏，使得即使是合法的接收者也无法阅读信息内容。

直到最近几年人们才对信息隐藏有了更深刻的认识，并把加密和隐藏这两种手段结合起来，即先把信息加密后再把它隐藏起来。将秘密信息隐藏于普通文件(载体文件)中传递出去，以保证秘密信息不容易被窃取和破坏，这称为信息隐藏。秘密信息的数字载体可以是普通的图像、声音、文本或其他任何数字化表示的代码或媒介。隐藏的消息可以是明文、密文或其他可表示为位流的数据。传统的以密码学为核心技术的信息安全和伪装式信息安全技术不是互相矛盾、互相竞争的技术，而是互补的。由于信息隐藏过程不破坏原载体的外观特

性，这就使得有恶意的个人或团体无法知道载体文件中是否含有机密信息，这就增强了信息传输的安全性。

信息隐藏技术是一种特殊的信息加密技术，其主要内容是将秘密信息隐藏于另一载体信号之中，其形式可以是任何一种数字媒体，如图像、声音、视频等等。信息隐藏技术不同于传统的加密技术，加密技术仅仅隐藏了信息的内容，而信息隐藏技术不但隐藏了信息的内容而且隐藏了信息的存在。常见的信息隐藏技术多半是利用声音、图像和视频本身具有不易觉察的可失真的特性来实现。

目前，信息隐藏技术的研究方向及应用的主要领域有两个：掩密术领域和数字水印领域。

- 掩密术保护的是秘密信息；数字水印保护的是载体信号。
- 掩密术强调如何使隐藏在多媒体信息中的信息不被他人发现，即信息存在性的隐密；数字水印则关心隐藏的信息是否被盗版者修改或移去，而它们的反向问题是发现和破坏方法的研究。
- 掩密术主要用于信息的安全通道，如用于军事目的的秘密信息传送，个人隐私的保护等；水印技术应用于版权保护、违反者追踪、电子商务中的网页保护和票据防伪等领域。

尽管信息隐藏技术的各个应用领域的侧重点有所不同，但是有一点它们是相同的：都是利用人类的感觉冗余，以及多媒体数据特性存在的冗余即数据特性冗余将信息(掩密术中的秘密信息或数字水印技术中的版权信息等)隐藏在掩护体(掩密术中的掩护信息或数字水印技术中的被保护信息)之中，对外表现的只是掩护体的外部特征，而且不改变掩护体的基本特征和使用价值。实际上，所有的数字水印技术都可以用于掩密术，进行数据隐藏。

本文主要研究以静止图像为载体的信息隐藏技术。

§1.4 信息隐藏的要求

一般说来，信息隐藏应满足如下几个要求：

(1) 隐蔽性：不影响对载体信息的理解，也就是说人的生理感官辨别和计算机检测都无法发现载体信息内包含了其它信息。

(2) 鲁棒性：要尽量保证隐藏了信息之后的载体数据在经历可能的处理(如

信号处理、有损压缩、滤波、调制等)、恶意攻击(如非法攻击、篡改、删除等)或者信道中随机噪声的影响后，还可以提取出原始的隐藏信息。

(3) 安全性：信息隐藏系统的安全性与密码系统的安全性非常类似，信息嵌入的算法是公开的，安全性是建立在密钥管理的基础上的，只有拥有密钥才能提取信息。

(4) 容量：容量是载体媒体可嵌入的最大信息量。一般来说，嵌入的信息量越大，信息隐藏系统不可检测性和稳健性越差。

(5) 信息隐藏系统是盲的：即在信息提取过程中不使用载体信号。在大多数情况下载体信号是不可得到的。

(6) 效率：信息的嵌入和提取的时空开销代价是否可以接受。

以上要求并不是每一个信息隐藏系统都必须满足，实际上也不可能全部满足，许多要求是自相矛盾的，实际的系统只能根据具体应用的不同来进行折衷。

§1.5 信息隐藏技术分类及常用方法

§1.5.1 信息隐藏技术的分类

信息隐藏技术是一种新兴的知识领域，尽管还处在发展研究阶段，可以也已经具有了自己意义和内涵。现在可以将其作如下分类：

(1) 按密钥分类：

若嵌入和提取采用相同密钥，则称其为对称隐藏算法，否则称为公钥隐藏算法。

(2)按载体类型分类

载体包括基于文本、图像、视频和声音等数字媒体的信息隐藏技术。

(3)按嵌入域分类

主要可分为空域(或时域)方法和变换域(或频域)方法。一般说来，变换域又可以分为 DCT 域和 DWT 域。限于篇幅，本文没有涉及到 DWT 域的信息隐藏技术。

(4)按提取要求分类

若在提取隐藏信息时不需要利用原始载体，则称为盲隐藏；否则称为非盲隐藏。显然使用原始的载体数据更便于检测和提取信息。但是，在数据监控和跟踪等场合，我们并不能获得原始的载体。对于其他的一些应用，如视频水印，即使可获得原始载体，但由于数据量巨大，要使用原始载体也是不现实的。隐秘目前主要采用的是盲隐藏技术。

(5)按保护对象分类

主要可分为掩密术和水印技术。掩密术主要用于保密通信，它所要保护的是隐藏的信息；水印技术主要用于版权保护及真伪鉴别等目的，它最终所要保护的是载体。例如可将数字、序列号、文字、图像标志等版权信息嵌入到多媒体数据中，以起到版权保护的作用。对于数字水印，我们又可以进行以下分类。所有的数字水印技术都可以用于掩密术。

- 数字水印
  - 按隐秘性分
    - 可感知水印
    - 不可感知水印
  - 按嵌入域分
    - 时空域水印
    - 变换域水印
  - 按提取是否需要原作品分
    - 盲提取水印
    - 非盲提取水印
  - 按稳健性分
    - 稳健水印
    - 脆弱（易损）水印

§1.5.2 信息隐藏技术的常用方法

现行的信息隐藏典型算法按嵌入域的不同，分为空域隐藏算法和变换域隐藏算法。

1. 空域隐藏算法

空域法是直接改变图像元素的值，一般是在图像元素的亮度或色度中加入隐藏的内容。如 LSB 算法，它通过调整伪装载体某些像素数据的最低 1—2 位有效位来隐藏信息，致使所隐藏的信息靠视觉很难被发现。空域类算法的特点是只需对隐秘载体进行很小的、不易察觉的改变就能隐藏很大的信息量，计算速度较快。但从基本原理上看，该算法所隐藏的信息是极为脆弱的，其鲁棒性较差。若载体图像有微小的改变或者对载体的较小的扰动，如有损压缩，都有

可能导致整个信息的丢失。

2. 变换域隐藏算法

变换域隐藏算法是利用某种数学变换，将图像用变换域(如频域)表示，通过更改图像的某些变换域系数加入待隐藏信息，然后再利用反变换来生成隐藏有其他信息的图像。常见的变换域算法有：基于 DCT 的变换域算法、基于 DWT 的变换域算法。

与空域方法相比，变换域方法的优点如下。

· 在变换域中嵌入的信号能量可以分布到空域的所有像素上。

· 在变换域中，人的感知系统的某些隐蔽特性可以更方便地结合到编码过程中。

· 变换域方法对传输过程中的图像压缩、滤波以及噪声均有一定的抵抗力。

· 变换域方法对诸如压缩，修建和某些图像处理等的攻击的鲁棒性更强。

· 变换域方法可与数据压缩标准兼容(如 JPEG、MPEG 等)，常用的变换包括离散余弦变换(DCT)和小波变换(DWT)。

因此，目前的多数信息隐藏方法采用变换域技术，即把待隐藏的信息嵌入到载体的一个变换空间(如频域)中。

§1.6 信息隐藏检测技术简介

信息掩密术的目标是避免传送秘密信息时引起怀疑，从而使秘密信息不可检测。信息隐藏的检测分析技术则是发现隐藏的消息并使这些消息无效的一种技术。若信息在传送时引起了他人的怀疑，并进而破坏信息，那么说明隐藏失败。在网络上，有不少非法者利用隐藏技术，通过开放的网络将不可告人的信息或计划发送给同伙，共同图谋非法活动，危及到民众和国家的安全。这时，就要尽量在他们进行信息传递时，截取并破坏他们的秘密信息，使它们不能准确到达目的地址。由此需要大力发展针对信息隐藏的检测技术。

对传统的信息加密系统的攻击是为了恢复或篡改消息。而对信息隐藏系统的攻击和分析可能有几种形式，即检测、提取、混肴(攻击者在存在的隐藏信息上进行伪造或覆盖)及使隐藏信息无效。不管是否存在嵌入消息，在不改变载体外观的情况下，都可以对任何载体作处理以破坏某些可能隐藏的信息或使之无

效。检测隐藏信息的存在性仅需要处理包含隐藏信息的载体，这样比使隐藏信息无效更简便。

总体说来，目前常用的信息隐藏检测方法为：

- 在不改变图像外观的情况下，对图像做处理变换，如另存为其他图像格式，滤波，做有损压缩等等，对有调色板的图像变换其调色板的索引值。
- 利用位分析法，对图像的最低位进行处理，然后分析是否改变图像的原始特性，或提取到可疑的信息。
- 分析图像的统计特征，并进而确定一个合理的统计量，计算其值，判断是否符合普通图像的特点。

当然，针对不同的隐藏方法最好采用不同的攻击方法，但是由于网络上图像格式的多种多样，而且隐藏技术也是层出不穷，因此也不可能用一种方法来检测全部的隐藏技术，只能从检测效率和运行时间上进行综合选择。

§1.7 信息隐藏技术的研究动态和发展现状[3]

在 1994 年的 IEEE 国际图像处理会议(ICIP'94)，R. G. Schyndel 等人[4]第一次明确提出了"数字水印"的概念，从此掀起了现代信息隐藏技术研究的高潮。仅仅过了两年，在 ICIP'96 上，已经出现了以信息隐藏领域中的水印技术、版权保护(Copyright Protection)和多媒体服务的存取控制(Access Control of Multimedia Services)为主要内容的研讨专题。同年在英国剑桥召开了第一届信息隐藏国际研讨会(First International Workshop on Information Hiding)，内容涉及数据隐藏、保密通信、密码学等相关学科领域。在美国，许多著名大学和大公司的研究机构，如麻省理工学院的媒体实验室、明尼苏达大学、普林斯顿大学、南加州大学等，以及 NEC 公司、IBM 公司等，都一直在致力于信息隐藏技术方面的研究，并已取得了大量研究成果。目前，应用于数字图像的水印技术已被考虑写于 JPEG 2000 标准[5]，这必将进一步推动信息隐藏技术的发展。

以数字水印为代表的信息隐藏技术也引起了我国科研人员的浓厚兴趣。为了促进国内信息隐藏技术的研究和应用，我国信息安全领域的三位院士与有关应用研究单位联合发起了我国的信息隐藏学术研讨会，并于 1999 年 12 月组织召开了第一届会议，至今，已经成功举办了四届。国家 863 计划智能计算机专家组也于 2000 年 1 月举办了"数字水印技术学术研讨会"。此次研讨会由中科院

自动化所模式识别国家重点实验室和北京邮电大学信息安全中心承办，与会者就数字水印技术的发展动态和趋势进行了全面、深入的探讨。从这次会议反应的情况上看，我国相关学术领域的研究与世界水平相差不远，而且有自己独特的研究思路。

当前网络上有各种能够实现掩密的软件，下表是目前实现基于图像的信息隐藏和提取功能的常见工具。

名称	载体文件	隐藏文件	生成文件	加密	运行环境
4t HIT Mail Privacy LITE	BMP,JPG,GIF, PNG,TIF,WMF ,EPS	Message	有	128-bit 算法	Windows
BlindSide	24bit BMP	TXT 文件	BMP	是	Dos
Secrets	BMP,GIF,JPG,I CON,Metafiles	任意	BMP	是	Windows
Contrabands	24bit BMP	任意	BMP		Windows
Courier	BMP	Message	24bitBMP		Windows
Data Privacy Tool(DPT)	24bit BMP			是	Windows
Digital Picture Envelope (DPE)	24bit BMP , (>63x63,<513x 513)	Message	24bitBMP	是	Windows
EzStego	GIF	TXT 文件	GIF	改变调色板	Windows
Ghosthost	任意种图片格式	任意文件	任意图片		Windows
Gif-it-Up	GIF	任意文件	GIF	是	Windows
GifShuffle	GIF	文件	GIF	CFB	Dos
Hide4PGP	BMP	TXT 文件	BMP	是	Dos
Hide and Seek	GIF	文本文件	GIF	是	Dos
Hide in Picture	24bit/8bit BMP	任意文件	BMP	随机数	Windows
In the Picture	24bit BMP	任意文件	BMP	是	Windows
Invisible Secrets	BMP,JPG,PNG	任意文件	BMP,PEG, PNG	Blowfish Twofish, RC4/TM	Windows
JPHS	JPG	任意文件	JPG	Blowfish	Windows
JSteg	GIF,JPG	文件	JPG	无	Dos
Mandelsteg	GIF	TXT,DAT	GIF	PGP	Dos
Permeate	BMP	任意文件	BMP	密码	Windows
Pretty Good Envelope (PGE)	GIF,JPG	TXT	JPG	密码	Dos
Stash-it	JPG,BMP,PCX, PNG,TIFF	任意文件	BMP,PCX, GIF	stash	Windows
Steganos	BMP	任意文件	BMP	Stealth/PGP	Windows

S-Tools	BMP,GIF	任意文件	BMP	IDEA	Windows
Webstego	BMP	任意文件	BMP	是	Windows
Z-file	BMP	任意文件	BMP	密码	Windows

表 1 常见信息隐藏工具[6,7]

§1.8 课题来源及本论文所做的主要工作

信息隐藏作为一种新的秘密通信方法，已经成为网络安全研究中一个十分活跃的领域。它与信息安全、信息隐藏、数据加密等均有密切的关系。因此，信息掩密技术的研究具有很大的现实意义。本课题来源于国家信息安全产品测评认证中心所委托的 863 计划项目“网络环境下隐藏信息的检测与分析技术研究”中的子课题“图像信息隐藏检测系统”的研究。

本论文的主要工作是：

- 搜集网络上多种伪装工具，对其归类总结。
- 空域的信息隐藏。介绍了空间域中常见的信息隐藏方法——LSB 替换算法、奇偶性方法、调色板方法等，并结合人类视觉系统特点，提出基于图像方差、平坦度、模糊隶属度等隐藏技术，还对基于差值矩阵的隐藏进行了实验。
- DCT 域的信息隐藏。研究了基于 DCT 变换和融合的信息隐藏技术，并给出了改进的算法，同时提出了 DCT 域自适应、DCT 域奇偶性两种信息隐藏算法，以及差值矩阵的频域隐藏算法。

下面是本论文的内容安排：

◆第一章绪论，简要介绍信息隐藏技术的相关概念、研究现状

◆第二章介绍信息隐藏技术的相关的理论知识，为后面章节的提到的算法和进行的实验提供知识基础。

◆第三章阐述图像空间域的信息隐藏技术的常用算法，并对典型算法进行试验，讨论试验结果。

◆第四章阐述图像 DCT 变换域的信息隐藏技术的常用算法，并对典型算法进行试验，讨论试验结果。

◆第五章总结本文所做的工作，并对以后工作的展望。

第二章 信息隐藏技术

§2.1 信息隐藏的模型

§2.1.1 掩密术的通信模型

掩密术的目的是在通信双方间建立一条秘密通道[1]，这样中间的其他任何人不能检测到通信过程的存在，也不会从伪装的介质当中提取到任何有意义的信息。“经典”的秘密通信模型是由Simmons[8]于1983年提出的所谓“囚犯问题”。如图2.1所示：Alice和Bob因犯罪被逮捕并关押在不同的牢房内。他们想策划逃跑，不幸的是两人之间的所有通信都要在看守Wendy的监督下进行。Wendy不允许他们进行加密通信，如果发觉任何可疑的通信就会把他俩都送入单独的牢房，并禁止任何信息交换。因此，他们不能采用常规的密码通信技术，因为一条经过加密后的消息虽然可能不会导致逃跑计划的泄露，但是它可作为双方进行协商逃跑的证据，双方必须以秘密的方式进行通信，以免引起Wendy的疑心。为此，他们不得不建立一个隐藏通道，这就是通常所说的阈下信道。一个实用的办法是将有用的信息隐藏在某种看似普通的信息中。例如，Bob可以画一幅画，描绘一头蓝色的奶牛躺在绿色的草地上，用各对象的颜色传递信息，然后把这幅现代画发送给Alice，当然Wendy不知道其中机窍。

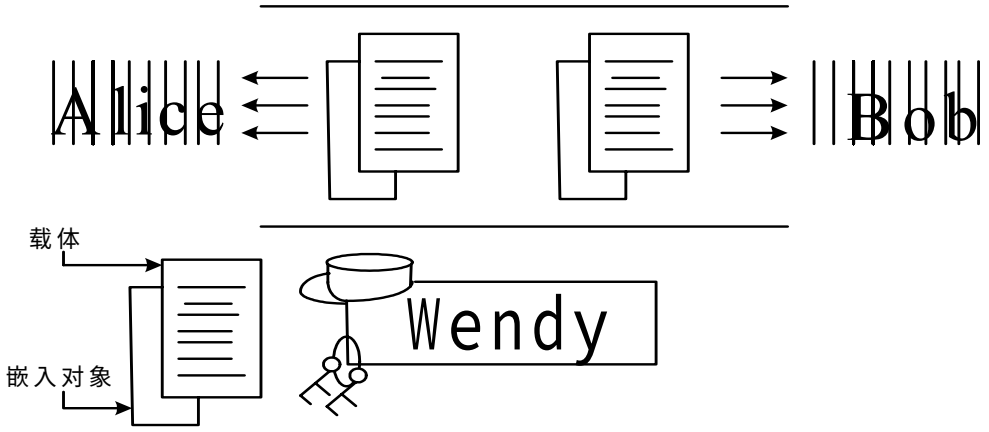


图2.1 囚犯问题模型

信息加密技术隐藏了信息的内容，掩密术更进一步的隐藏了通信过程本身的存在性。发送方和接收方可以秘密地交换秘密信息。在一般情况下，我们可以对监狱看守Wendy进行分类，如果它可以修改Alice和Bob间的信息流，则Wendy称为主动看守，如果她只能检查Alice和Bob间的信息流，则Wendy称为被动看守。在通信过程中，双方都要考虑到被动的、主动的或者是恶意的攻击者。

掩密术的大多数应用都可以用如图2.2所示的框图来描述，大量的研究工作都是基于这个模型。

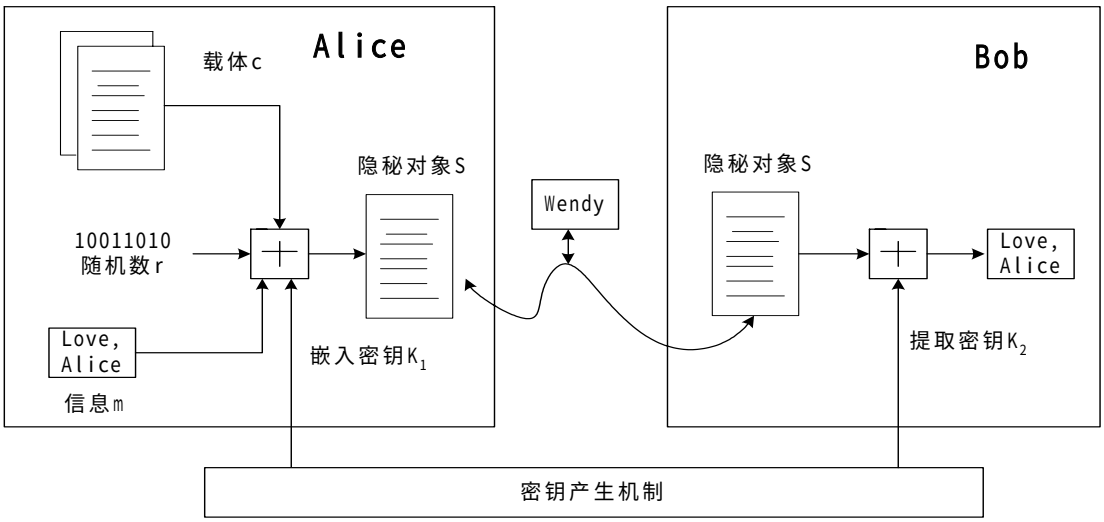


图2.2 典型的隐秘系统模型

Alice想把秘密信息M送给Bob,首先随机地选取一个载体信息C，理论上讲它可以是任何计算机可以读取的数据，如数字图象文件、数字音频文件或文本文件等，它可以不被怀疑的传送给Bob。然后在C中嵌入秘密信息，有时会使用嵌入密钥K_1。由此Alice将隐秘载体C改变成为隐秘对象S。

Alice在公开信道上将S传送给Bob,希望Wendy不会注意到所嵌入的数据。因为Bob知道Alice所采用的数据嵌入方法和提取过程中所使用的提取密钥K_2，所以他能重建或恢复出消息M，而且这个恢复过程在没有原始载体C的情况下也能进行。监视通信的Wendy应当不能决定Alice发送出的载体中是否含有秘密消息，即使她知道也不能确定在所发送的$S\{s_1,s_2,\ldots,s_n\}$集合中，哪个S_i中含有秘密信息。隐秘通信系统的安全性主要取决于第三方不能区分隐秘载体和隐秘对象间的差别上。

在实际运用中，并非所有的数据文件都可以用作秘密通信中的隐秘载体。

这是因为要保证让未曾参与通信过程的第三方不能发现数据嵌入过程中所做的修改。这就要求隐秘载体中含有足够的冗余以便它能够被秘密信息所替换。在同一次通信过程中，同一隐秘载体一般不应当被使用超过两次。因为如果攻击者得到同一个隐秘载体的两个不同版本，就能很容易地检测到并且可能恢复出秘密信息。为了避免意外的重复使用，发送方和接收方都应当销毁已经在信息传送中使用过的隐秘载体。

§2.1.2 数字水印的一般模型

数字水印是指嵌入数字产品中的数字信号，可以是图像、文字、符号、数字等一切可以作为标记、标识的信息，它能够证明产品版权的所有者。一般的说，水印系统都要包括两个基本模块：水印嵌入模块和水印提取模块。水印信号嵌入(或水印编码)模块，其功能是完成将水印信号加入原始数据中；水印信号检测(或是水印恢复和解码)模块是用来判断某一数据块中是否含有特定的水印信号。

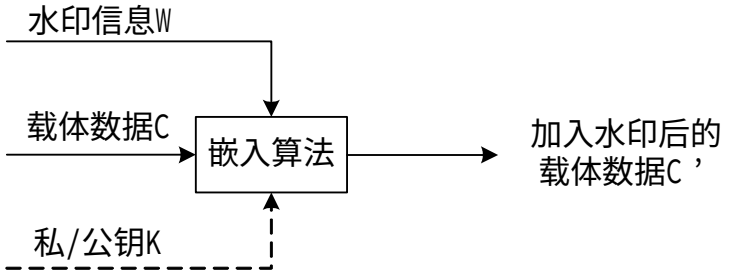


图2.3 水印信号的嵌入模型

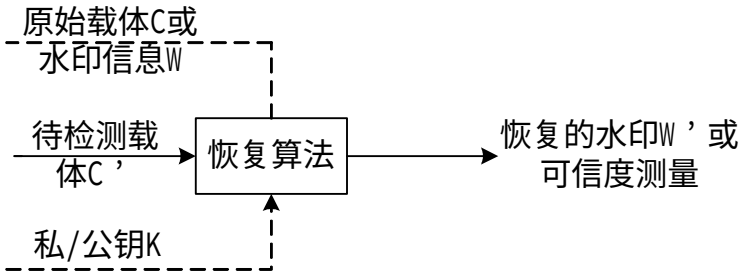


图2.4 水印信号的恢复模型

图2.3为水印信号的嵌入模型，输入信号为水印信息W，载体数据C，私钥或公钥K用来增强算法的安全性，避免未授权方恢复和修改水印，它可有可无，

这要依据具体的应用不同，如果水印为不可见，一般来说，是具有合法密钥的用户才能正确的恢复出所嵌入的信息，实际系统中通常是一个或几个密钥的组合。水印信息W可以为序列号、图象，文本等任何形式的数据，载体数据C可以为音频、视频、图象或文本等，经过嵌入算法的处理，相应的水印信息就被嵌入到载体中去，得到的是嵌入水印信息后的载体数据C ’。

水印信息的恢复模型如图2.4所示，待检测的载体信号C ’可能是受过恶意攻击处理的，在进行水印信息的恢复时，可以根据所采用嵌入的具体方法不同，应用或不应用原始载体C或原始水印信息W来对嵌入的水印信号进行恢复。其中恢复的数据可与原始的水印信号进行相似度或可信度测量，以此来判定水印信息的存在。

§2.1.3 改进的信息隐藏模型以及图像置乱

信息隐藏是充分利用通信过程中冗余信息的存在来工作的。数字图像或音频信号天然地包含噪声形式的冗余。如果能够对秘密信息进行某种方式的编码，使得它与真正的随机噪声不可区分，则攻击者将没有机会检测到秘密信息。为了使隐藏信息更具随机性，经常在嵌入消息之前对消息进行预处理，如文本文件的加密，数字图像的置乱等。

引入了预处理后的信息隐藏模型如图 2.5 所示：

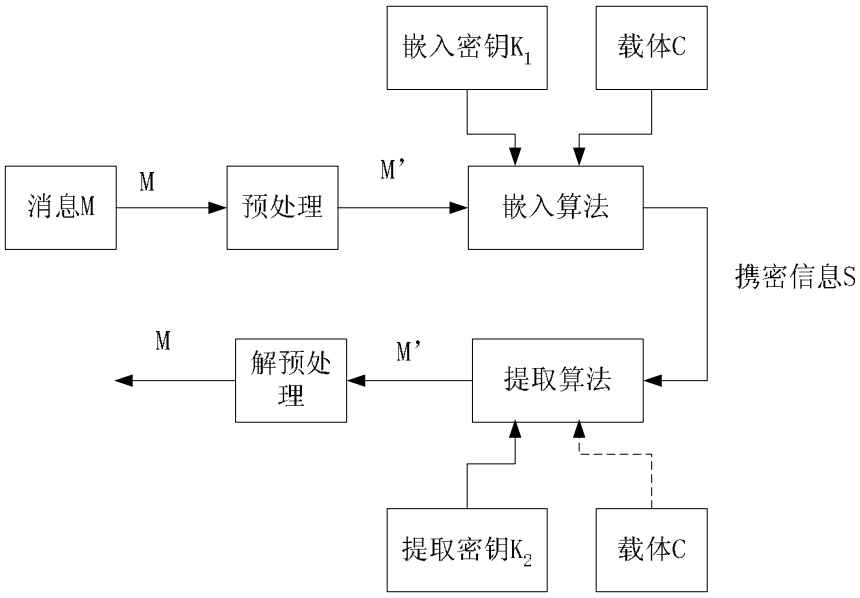


图2.5 信息的隐藏和提取系统模型

对于图像置乱，“置乱 ”，顾名思义就是通过把要传输的信息次序打乱，

削弱了像素间的相关性，增强了信息隐藏的不可感知性，使其变得难以辨认。数字图像置乱和信息加密思想类似，它是对图像进行处理，使图像成为看起来杂乱无章的图像，隐藏真实的图像信息。图象置乱可以达到两个目的：

- 第一个目的是加密处理，就象不知道加密密钥对加密过的信息进行解密一样，如果不知道置乱所采用的算法，同样难以恢复原始图像的信息；
- 第二个目的是图像被置乱后是一个无法读取的杂乱信息，可被抽象成一些随机的信息，没有任何明显可统计的特征如形状，纹理色彩等，在隐藏到另一幅图象中时不会出现容易识别的形状或交叠现象，因而可做到不可察觉，增加信息隐藏的安全性。

下面介绍两种简单的图像置乱算法：

方法一[9]：步骤如下

（1） 对原图像取一个固定模框，模框中像素位置排列如图 2.6 所示

（2） 建立一个宽度与原图像模框不同的置乱模框(见图 2.7)，在置乱模框中把原图模框中的像素位置信息按横向次序填入

（3） 将置乱模框中的像素位置信息按纵向次序读取，填回原图像中就得到信息次序的混乱，见图 2.8

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

图2.6 原图像

1	2	3
4	5	6
7	8	9
10	11	12
13	14	15
16		

图2.7 置乱模框

1	4	7	10
13	16	2	5
8	11	14	3
6	9	12	15

图2.8 置乱结果

其中置乱模框的宽度是密钥的特征参数之一。其长度则随原图像模框中像素的多少而变换。置乱模框也可以选取其他的形状，如菱形、星形、三角形等。图像经过多次上述的“ 置乱 ”(取不同的特征参数)后可以取得较好置乱效果。以256×256Lena图进行实验，效果如下：

图2.9 256×256Lena原图

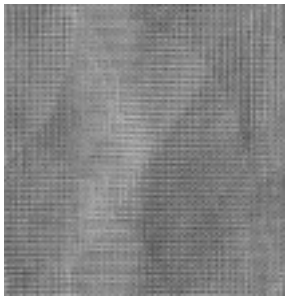


图2.10 以2096×64为置乱模框的置乱

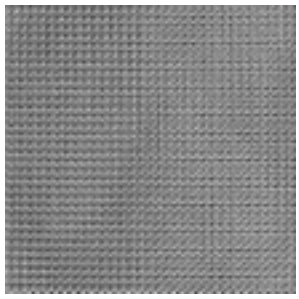


图2.11 对图2.10进行512×128为置乱模框置乱

方法二[10]：随机序列置乱法。步骤如下：

(1) 产生0到$M_1 \times M_2 - 1$的随机数作为原始水印的每个像素点的标号，其中M_1、M_2为原图像的大小。

(2) 利用桶分类排序算法将这些随机标号按由小到大排序，随机标号的顺序排序使得标号所标识的原图像点随机分布。

置乱算法示意图如下：

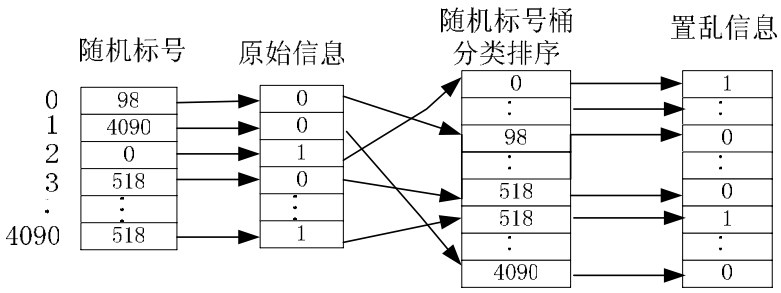


图 2.12 随机序列置乱法示意图

将256×256Lena图进行实验，结果如图2.13，可以看出，置乱效果较好。

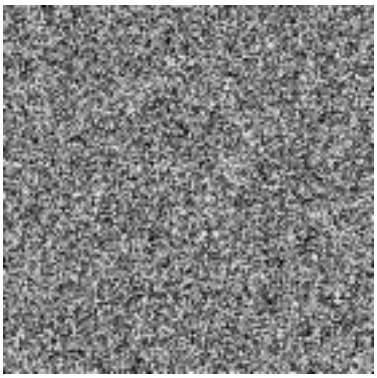


图 2.13 Lena 图的随机序列置乱

此外，人们提出了很多图像置乱的方法，如基于密码学、Arnold变换、幻方、Gray码变换、正交拉丁方[11-13]等方法。

§2.2 人类视觉特性

信息隐藏方法的隐藏原理就是基于人的视觉特性，利用人的视觉冗余来嵌入信息，因此在进行信息隐藏算法的讨论之前，有必要对人类的视觉系统作一介绍。

§2.2.1 人类视觉系统介绍

人的视觉系统是一个非线性系统。根据韦伯定律，人眼对光强变化的响应成反比，即人眼在低光强时有较高的灵敏度，在高光强下具有较低的灵敏度。再者，人的视觉对空间频率有的依赖性，随着频率的增大，人眼的分辨率会迅速降低，并且人眼对不同角度的空间频率视觉信号的响应也不大相同，在垂直方向与水平方向的频率具有较强的视觉响应，在对角线的方向，响应就显著下降。人的视觉特性还受外界条件的影响，在不同照度下，人眼对相同图像数据有不同的视觉感受。不同的环境、底色和背景会产生不同的视觉感受，一个图像数据完全相同的色块在不同的背景不同的陪衬下会有不同的视觉效果，因此人眼对图像的视觉不是对图像每个像素逐一产生响应，每个像素的视觉感受，受到周围像素的影响，每个局部的视觉响应不但取决于这个局部的图像数据，还和这个局部周围的图像数据整幅图像的数据有关，人眼视觉是对一幅图像产生的总体感受。

§2.2.2 与信息隐藏有关的一些特性[14]

就目前来看，在信息隐藏技术上，主要运用的人眼视觉特性有三个方面，分别为频率敏感特性(Frequency Sensitivity)，对比度掩蔽特性(Contrast Sensitivity)和亮度掩蔽特性(Luminance Masking)。

(1) 频率敏感性 频率敏感性描述人眼视觉在不同的频率下，对正统光栅增益的敏感程度，通常可以借助对比敏感性函数 CSF(Constrast Sensitivity Function)或调制传递函数 MTF(Modulation Transfer Functon)来加以描述。调制函数曲线如图 2.14 所示，该函数曲线反映了人眼视觉对低频部分的变化敏感性而对高频部分的变化不敏感特性。利用该模型，可以在假设最小的观察距离是固定的情况下，对每一个频率带，确定其静态的与图像内容无关的 JND(Just Noticeable

Difference)数值是可能的。但该模型在低分辨率显示和近距离观测等等条件下具有缺陷。频率敏感性提供了一个基本的视觉模型，它仅仅依赖于观察条件而不依赖于图像内容。

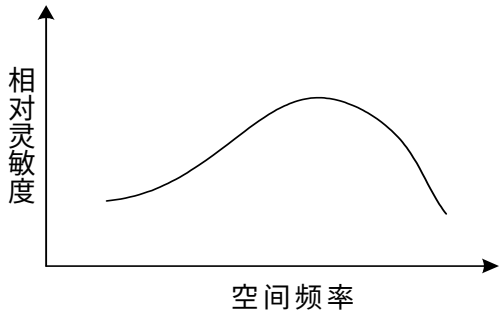


图 2.14 调制函数曲线

(2) 亮度敏感性 亮度敏感性描述在一个不变的固定亮度背景下，测量噪声可察觉门限的效果，这一特性取决于背景平均亮度和噪声亮度水平。一般认为，低亮度可视性高于高亮度，其描述函数通常是由图像局部特性构成的非线性函数。但是，亮度敏感性对视觉掩蔽的描写很不充分，它不能描述由于调频细节或图像纹理引起的掩蔽现象。对于人类视觉系统，它是一个非线性函数并且依赖于局部的图像特性。

(3) 对比度掩蔽特性 对比度掩蔽特性反映了在存在背景信号前提下人眼视觉对一个信号的感知掩蔽特性。也就是说一个信号在另一个信号存在的情况下的可检测性，尤其当这两个信号具有相同的空间频率、取向和位置时，掩蔽特性最强。一般掩蔽特性可大致分为自对比掩蔽(self-contrast masking)和邻域掩蔽(neighborhood masking)两类。前者是指具有相同空间频率、取向和位置的信号的掩蔽效益；后者是指则由空间相邻系数导致的掩盖效应，其反映出人眼视觉对平坦区失真敏感性强于复杂纹理区域的特性。对比度掩码允许 JND 门限的更灵活的控制。

人眼的这些视觉掩蔽特性是一种局部效应，受背景亮度、纹理复杂性和信号频率的影响。具有不同局部特性的区域，在其不被人眼察觉的前提下，允许改变的信号强度不同。

第三章 基于空间域的图像信息隐藏

§3.1 LSB 替换算法

最低有效位 (Least Significant Bit，LSB)方法是最基本的空间域图像信息隐藏算法，许多其它的空域算法都是从它的基本原理进行扩展的。

(1) 隐藏原理

在我们针对信息隐藏所采用的介质中，我们主要是图像为载体，而图像又按照颜色不同划分为 24 位真彩色图像，8 位彩色图像，8 位灰度图像，16 色位图和单色位图。一般来说在进行信息隐藏时， 24 位真彩色图像和 8 位灰度图像的应用较广泛。

LSB 方法是通过改变图像像素值的最低有效位来实现数据的嵌入，这样保证了信息嵌入的不可见性。显然，LSB 隐藏算法最低位被改变的概率是 50%，它在原始图像里面引入了极小的噪声，在视觉上是不可见的。实际上，对于真彩色图像，我们在其最低两位甚至三位来隐藏信息使视觉上仍然是不可见的，对于灰度图像，改变其最低两位也能取得较好的效果。位平面图如下，可以看出随着位平面的降低，随机性越来越强，第 0、1、2 甚至 3 位平面都具有很大的随机性。

图 3.1 128×128 Lena 图

图 3.2 Lena 图的第 7、6、5、4、3、2、1、0 位平面

另外，在 LSB 方法中，我们也可以不采用直接嵌入的方法，根据异或的可逆准则，采用替换的准则来实现信息的隐藏。异或的简单原理如下：(a⊕b)⊕b=a。因此我们在嵌入数据位时，嵌入的是数据位与 1 或者 0 的异或值。基于异或的运算也有许多改进的算法，在嵌入的过程中，首先计算每个像素灰度值的每一位的异或值，并把所得到的结果与要嵌入的信息进行异或运算，然后，把像素灰度值的最低位全部清零或置为 1，再根据异或运算结果的值来改变最低位的信息，实际上，这相当于对信息进行了一层加密处理，嵌入的不再是原始信息，而是原始信息的另外一种表达形式，不知道密钥的攻击者很难从中提取出信息。

(2)数据隐藏率

对于 24 位图像，LSB 隐藏算法是 3 数据位/像素，每个像素又是由 24 位来表示，可以隐藏的信息率采用如下方式计算：

3[隐藏位/像素]/24[数据位/像素]＝1/8

如果是改变每个字节的最低两位，可以隐藏信息率为 2/8 ，同理，改变三位的话，信息隐藏率变为 3/8 。

我们也可以计算出在 8 位灰度图像中进行信息隐藏时的数据隐藏率，8 位灰度图像的是每个像素隐藏一个信息位，每个像素是由 8 位来表示，它的 LSB 信息隐藏率为：1[隐藏位/像素]/8[数据位/像素]＝1/8，可能看出它的结果与 24 位图像相同，同样改变两位或三位也与 24 位图像相同。

(3)实验结果

图 3.3 为 256×256×8 的 Lena 灰度图，图 3.4 为 LSB 直接替换第 0 位平面后的 Lena 图，我们看不出两个图片间的区别，隐秘性相当好。

图 3.3 Lena 原图

图 3.4 LSB 嵌入后的 Lena 图

(4)鲁棒性分析

LSB 算法具有非常小的鲁棒性。对于许多变换，即使是有益的，也都是很脆弱的。

- 有损压缩 典型的有损压缩如 JPEG，就很有可能彻底破坏隐藏的信息。问题是 LSB 算法试图利用人类视觉系统的漏洞，而有损压缩算法所依赖的，是对附加噪声的不敏感性，正是利用它来减少数据量的。
- 几何变换 移动像素尤其是改变像素在原栅格中的位置都有可能破坏嵌入的消息。
- 任何其它的图像变换如模糊，滤波等，通常都会破坏隐藏的数据。

(5)问题及解决方案

LSB 对信息隐藏学来说是比较好的，因为它具有较大的信息隐藏率。我们可以对它的主要缺点之一：提取的容易性进行改进。我们不想让攻击者能够读取我们所发送的任何信息，通常采用如下两种补充的方法来达到这个目的：

- 采用较强加密算法对待隐藏的信息进行加密，提取者只有能够解密时才能读取信息。
- 采用密码随机函数对信息隐藏的位置进行随机放置，如果不知道随机种子的话，重建消息也几乎是不可能的。

这样信息采用两种不同的密钥进行保护，比直接嵌入获得了较好的机密性，也保护了信息的完整性，伪造信息几乎是不可能的。

然而对于信息隐藏理论来说，密码学只是信息隐藏的辅助工具，我们不想

我们的消息是加密的混乱的消息，我们必须想办法来提高信息隐藏算法的安全性，即使是直接嵌入也很难检测出被隐藏的信息。

与这个问题相关的两个最重要的问题是：

- **图像内容的选择**
- **图像大小、格式的选择**

第一个问题，要求作为隐藏载体的图像首先必须看起来比较自然，必须选择使它在发送者和接收者之间来交换这个图像是有理由的；其次它必须有多种变化的颜色，也就是嘈杂的，以便加入的噪声能够被已经存在的覆盖。较宽的纯色区域，即使加入很小的噪声变化也是非常大的，这容易引起人的视觉上的警觉。

第二个问题就是文件的大小。这涉及到图像格式的选择，通常双方之间大的图像文件交换容易引起怀疑。看看图像的尺寸，24 位无压缩的图像大小是很不正常的，这是因为发送方对它没有压缩是很奇怪的，通常用的压缩算法并不会降低图像质量。

我们需要较小的图像文件尺寸，我们应当采用 8 位图像，因为他们的大小看起来更象是正常的。

256 彩色图像的问题是它利用一个索引的调色板，由于这些颜色的变化并不是按照一定的规律递进的，改变一个 LSB 位就是我们改变一个像素到邻近的位置，如果在调色板中近邻的颜色对比度较大，这样图像中的像素会突然改变它的颜色，隐藏的消息将会变得可见。

为了解决这个问题，不同的方法得到了研究，如重新排列调色板，以便邻近的颜色对比度不会太强烈，或者甚至减少调色板到一个较小的颜色数，在相邻的位置重复颜色表中的入口，以便嵌入消息后的差别变得根本不可见。而且对于大多数图像来说，颜色数的减少，如从 256 减到 32 几乎不可见。

大多数专家建议采用 8 位灰度图像，他们调色板比彩色的变化要少，因此 LSB 信息隐藏人眼是很难觉察到的。

§3.2 奇偶性方法

(1)隐藏原理

奇偶性方法也是在空域内直接对像素的灰度值进行更改，但是它并不是直接嵌入要隐藏的信息，而是根据要隐藏的信息位来改变灰度值。

奇偶性方法可以按照两种不同的规则来实现信息的隐藏：

规则 1：如果要隐藏的信息位为 1，则改变图像的数据使它为奇数，如果隐藏的信息位为 0，则改变图像的数据使它为偶数。或者采用相反的情况，数据为奇数时表示隐藏的是 0，偶数时表示隐藏的是 1。在对数据位进行改变时，可以采用加 1 或减 1 的方法来实现数据奇偶性的改变。

我们可以举个简单的例子如下：

如字母 Z 为要隐藏的消息，我们用奇数来表示隐藏的是 1，偶数表示隐藏的是 0，奇偶数的改变规则采用加 1 的方法来实现，对于边界值 255，我们则采用减去 1 的方法。一个图像数据部份其编码前后的结果如下，带下划线的表示图像数据发生了更改。

编码前： *71 90 48 120 135 171 254 255*

Z ： *01011010*

编码后： *72 91 48 121 135 172 255 254*

规则 2：我们也可以按照计算数据位中的 0 或者 1 的个数的奇偶性这样一个规则来实现信息的嵌入。如果要隐藏的信息位为 1，则改变图像数据最低位的值使 1 的个数为偶数；信息位如果为 0，则改变数据的最低位使 1 的个数为奇数。或者采用相反的情况，如果 1 的个数为偶数，表示隐藏的信息位是 0，相反则是 1。

例如字母 Z 为要隐藏的消息，采用 1 的个数为奇数表示隐藏的信息位是 0，偶数表示隐藏的信息位为 1 的方法，一个图像数据部分其编码前后的结果分别如下，带下划线的字符表示被更改的数据位。

编码前 ：00100111 11101001 11001000 00100111 11001000 11101001 11001000 00100111

Z： *01011010*

编码后 ：0010011**0** 1110100**0** 11001000 00100111 1100100**1** 11101001 1100100**1** 0010011**0**

(2)数据隐藏率

奇偶性方法的数据隐藏率与 LSB 方法相同，不管是真彩色图像还是灰度图像，它们的每一个图像数据信息只能隐藏一位的信息，隐藏效率仍然是 1/8。

(3)鲁棒性分析

奇偶性方法对于一些图像处理方法的攻击也是很脆弱的。常用的有损压缩，滤波以及比例变换都会破坏所隐藏的信息。一般而言，空域算法的鲁棒性都是很脆弱的。

(4)问题及解决方法

奇偶性方法提取信息的容易性，对它的安全性也是一种挑战。攻击者只要知道嵌入算法的先验知识也能正确的提取出信息。我们仍然可以采用 LSB 所补充的方法：对隐藏的信息进行加密以及对信息存放的位置进行随机的产生。

奇偶性方法另外一个缺点是它的不确定性较差，数据不是表示 0 就是 1，这在很大程度上给攻击者提供了便利的条件。和上述加密方法类似，一个改进的嵌入机制是采用查表的方式来实现信息的嵌入。

我们可以针对灰度图像来举个简单的例子。因为灰度图像的颜色种类只有 256 种，查表的方式是把所有的可能的值用来表示 1 或 0，在嵌入数据时，改变图像数据到最近的图像数据。

…	77	78	79	80	…	234	235	236	…
…	1	0	0	1	…	1	1	0	…

图像数据的映射表

对于灰度图像，我们可以根据上述的映射表来隐藏数据，它的前提条件是通信双方必须同时拥有这个映射表，以便接受方能够正确恢复出所隐藏的信息。同时这个映射表也必须是秘密的，它的丢失会造成信息的泄露。

对于彩色图像，0,1 间隔的区间不能太长，否则会引起图像色彩变化剧烈，容易造成失真，视觉上引起人的怀疑。

规则 2 的改进方法则相对简单，它是和 LSB 方法的改进类似，我们计算 0 或者 1 的个数时，改变的不是数据位的最低位的值，而是选择次低位，或者第三位来实现信息的隐藏。

§3.3 基于统计的信息隐藏

基于统计的信息隐藏技术也是空域算法的重要分支，它对图像的一些特征进行统计来表示要隐藏的信息。我们只给出一些简单的统计隐藏方法。

信息隐藏在变化较平缓的区域容易引起失真，故在图像变化较平稳的区域尽量少隐藏或不隐藏信息，应当在变化较复杂的地方多隐藏信息。这是因为，根据人的视觉特性，一些纹理区域的灰度值的改变对人的视觉系统不是很敏感，轻微的改变某些像素的灰度值，人的眼睛是觉察不到的，而对于平坦区域的噪声，人的视觉系统是非常敏感的。那么如何判断某些区域变化的复杂度？这就是下面我们所要解决的问题。

§3.3.1 基于中值滤波形式的信息隐藏

(1) 隐藏原理

中值滤波就是用一个窗口 W 在图像上扫描，把窗口内包含的图像像素按灰度值升(或降)序进行排列，取灰度值居中的像素灰度值作为窗口中心像素的灰度，这样就完成了中值滤波。用公式表示即

$$g(m,n)=\text{Median}\{f(m-k,\ n-l),\ (k,\ l)\in W\}$$

通常窗口内的像素数为奇数，以便有个中间像素。

常用的窗有线形、方形、十字形、圆形和环形等，如图 3.5 所示。

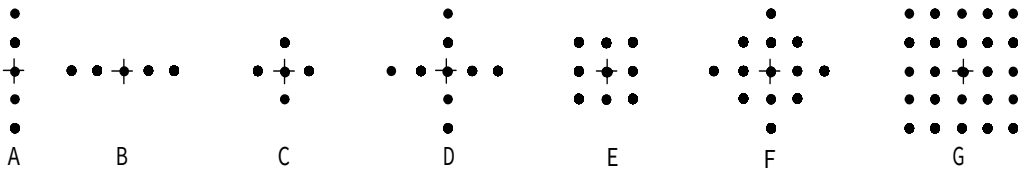


图 3.5 中值滤波常用窗形状

一个较简单的统计隐藏方法是源于中值滤波的思想。中值滤波是由许多不同的窗口组成，最简单的是线性的，也就是说，只有三个像素的线性窗口。在隐藏的时候，可以有两种不同的方式来实现信息的隐藏：一种是比较中间像素的灰度值与两边像素灰度值的关系，如果中间像素的灰度值位于两边像素灰度值之间，则认为我们在里面嵌入的信息位是 1，否则是 0，也可以采用相反的情况来实现隐藏，如果两边像素灰度值相差不大或者相等，我们可以轻微改变他

们的值，使中间像素的灰度值位于它们之间或之外，这种改变的技巧可以灵活掌握。另外一种隐藏方式是计算两边像素灰度值的平均值，当我们所要隐藏的信息位为 1 的时候，我们就改变中间像素的灰度值，让它等于两边像素灰度值的平均值。否则我们认为隐藏的信息位是 0，同样的道理我们也可以采用相反的情况来实现信息的隐藏。

举个简单的例子如下，我们采用线性的三个像素窗口，中间值如果位于两边灰度值之间，表示隐藏的位为 1，否则为 0。下面是一部分图像数据在信息位编码前后的结果。

编码前：*60 75 55 84 91 121 150 154 150 254 250 255*

信息位：*1011*

编码后：*60 58 55 84 80 121 160 154 150 254 250 245*

提取的时候则相对简单，只要对数据信息分成三个一组，对中间的像素值进行判断，如果它位于前后两个像素值的范围内，则认为所隐藏的数据位是 1，否则认为是 0。对于中间像素的灰度值的改变，我们依据的是尽量使灰度值的改变量较小的原则，如果隐藏的消息位是 0，就让中间像素的灰度值改变为两边灰度值较小的减去 4。如果隐藏的信息位是 1，为了避免两边灰度值相等的情况，我们把中间像素的灰度值等于较小的灰度值加 4，或者把较大的灰度值进行减 4 处理。

(2)隐藏效率

数据隐藏效率是按照窗口的大小来进行的，在一个只有三个像素的线性窗口内隐藏信息时，每三个像素才能隐藏一位的信息。它的隐藏效率也只有 1/24。

l[隐藏位/像素]/8[信息位/像素]=1/24

(3) 实验结果及分析

我们仍旧采用先前所采用的文本文件，在 Lena 图像中隐藏了 633 字节的信息，原始图像如图 3.6 所示，隐藏后的图像如图 3.7 所示，恢复出的信息如图 3.8 所示。但是从实验的结果中可以看到，隐藏后的介质图像在一些边缘的地方加入了噪声，这是因为在对中间像素的灰度值进行改变时，一些边缘的地方灰度值提前或滞后一个像素发生了突变，但是这种方法仍然具有较好的视觉效果。

图 3.6 原始图像

图 3.7 隐藏后的图像

```
Northwestern Polytechnical University (NPU) is situated in Xi'an, a world-famous ancient
capital city. NPU is one of the 15 key universities in China, and during the"Seventh
Five-year Plan"and the"Eighth Five-year Plan", NPU had been one of the universities of state
capital construction. At the beginning of the"Ninth Five-year Plan", NPU was approved by the
state to be in the first group of universities funded by"Project 211", and at the later
stage of the"Ninth Five-year Plan", NPU was selected as one of the 21 universities of the
state capital construction.
```

图 3.8 恢复出的信息

(4)一些改进方法

我们也可以对上述方法进行改进和推广，其基本思想是类似的。在隐藏信息时，仍然取三个像素值一组进行信息隐藏。在对中间值进行改变时，如果隐藏的信息位是 1，就改变中间像素的灰度值，使它与另外两个像素灰度值的平均值相等；隐藏的信息位如果是 0，就改变中间像素的灰度值使它与两边两个像素的平均值不相等，如在平均值的基础上加上或减去一个数。与上述的方法相比，这种情况下的中间像素的灰度值的改变没有上一个方法的改变量大，隐蔽性更好。

在采用 Matlab 进行仿真时，由于图像数据是以无符号数据表示的，因此在计算是必须把它转化成双精度类型，而且在比较相等时，必须指定一个比较小的范围，差值在这个范围内才能认为两个值是相等的，这样才可能完整的恢复出所隐藏的信息。采用这种方法隐藏后的图像如图 3.9 所示，由于这个方法是上述方法的改进，因此隐藏的信息量是相等的，所恢复出的信息与前面的相同。

图 3.9 隐藏后的图像

```
Northwestern Polytechnical University (NPU) is situated in Xi'an, a world-famous ancient
capital city. NPU is one of the 15 key universities in China, and during the"Seventh
Five-year Plan"and the"Eighth Five-year Plan", NPU had been one of the universities of state
capital construction. At the beginning of the"Ninth Five-year Plan", NPU was approved by the
state to be in the first group of universities funded by"Project 211", and at the later
stage of the"Ninth Five-year Plan", NPU was selected as one of the 21 universities of the
state capital construction.
```

图 3.10 恢复出的信息

同样可以把这种方法推广到图像块中去，选择图像的某块区域，利用所选择图像某块区域内部像素间的关系来隐藏信息。同样我们选择 3×3 的区域来作为信息隐藏的分块，我们首先计算周围 8 个像素灰度值的平均值，通过改变中心像素灰度值与平均值之间的关系来隐藏信息，当中心像素的灰度值大于平均值时，我们认为隐藏的消息位是 1，否则我们认为隐藏的消息位是 0。通过改变中心像素的灰度值，我们就可以在一个 3×3 的区域内隐藏一位的信息。采用上述的隐藏方法，我们在 Lena 图像中隐藏了 220 个字节的信息，隐藏后的图像和提取的信息分别如图所示

图 3.11 隐藏后的图像

```
Northwestern Polytechnical University (NPU) is situated in Xi'an, a
world-famous ancient capital city. The president of NPU is appointed directly
by the State Council. NPU is one of the 15 key univers
```

图 3.11 恢复出的信息

可以看到，这个改进的方法同样也达到了较好的隐藏效果，隐藏后的图像几乎与原始图像是一致的，因为对它的改变不是每个像素都发生了变化，而是根据隐藏信息的需要，改动某块区域中心像素的灰度值，同时，它还具有在恢复信息的时候不需要原始图像的优点，用户只要根据所选择块区域的大小，以及周围像素的平均值与中心像素的灰度值之间的关系就可以正确恢复出所隐藏的信息。它的缺点除了鲁棒性不高外，它所隐藏的信息量也是较小的，因为它在每个用户所选择区域内只能隐藏一位的信息，需要 8 个区域块才能达到隐藏一个字节的目的。而前面所采用的方法，几乎在一个区域内就隐藏了一个字节的信息。因此，这个方法的隐藏容量几乎是前一个方法的八分之一。

另外可作的改进的方法是线性窗口大小的调整，在实际的操作过程中，我们不一定非要采用 3 个像素的线性窗口，我们还可以采用十字的窗口，3×3 的窗口或者更大的窗口。

§3.3.2 基于图像方差的隐藏技术

1 隐藏原理

根据人的视觉特性，对高频信息(如复杂的区域)的敏感度低于对低频信息(如平滑区域)的敏感度，因此信息嵌入到频率越高的区域，对原始图像的影响越小，信息隐藏的透明性越好。 因此在图像内进行信息嵌入时，图像的选择尤其重要，图像变化太平坦，不利于信息的隐藏，而且如果嵌入的信息量过大，容易引起图像的失真。为此，我们采用了一种较常用的统计的方法就是计算图像块的方差，用来区分平坦区域和变化较复杂的区域，反映图像的平滑程度，在较平滑的区域，嵌入的信息量应该较小，而在变化较复杂的区域，则嵌入较多的信息。

我们可以把图像中某块区域内部的元素看成是一系列的随机数，这些随机数的数学期望是描述这块区域的平均值，而方差则描述了这些随机变量对平均值的偏离程度，方差越大，表明偏离程度越大。对于图像的某块区域，它的方差可以近似描述为它的平滑程度，方差越大，表明图像中的区域内部变化较大，也就是说，所选中的图像区域可能是图像内容的边缘或纹理区域，这样我们就可以利用人的视觉特征在这块区域内进行信息隐藏，而且隐藏后的图像与原始图像不会有任何明显的差别，不易被人眼所觉察，对图像造成的失真也较小。

假设 X_1，X_2…，X_n，是图像中的某块区域的灰度值，且 $X_i \in (0,255)$，那么它们的数学期望可表示为：

$$\overline{X} = \frac{1}{n}\sum_{i=1}^{n} X_i$$

它们的方差表示为：

$$S_n^2 = \frac{1}{n-1}\sum_{i=1}^{n}(X_i - \overline{X})^2$$

2 实验结果及讨论

在实验中，我们仍采用 Lena 图像来作为要隐藏的信息载体，在进行分块隐藏时，所采用块的大小是 3×3，对每个 3×3 的块，计算其方差，并对要隐藏信息的块的方差作专门的要求。我们首先确定一个阈值，如果某个区域的方差大于这个值，那么我们就认为这个块处于图像的边缘或者纹理区域，我们就可以在这个块中隐藏信息，否则，我们不对它作任何处理。根据图像的不同，阈值的选择又有所不同，我们在隐藏的过程中，所采用的阈值是 90，对于方差大于 90 的区域，我们对它隐藏一个字节的信息，中心像素的灰度值不发生任何改变，所隐藏的 8 个位的信息分别放在周围 8 个像素灰度值的次不重要位(LSB 左边的一位)而不是最不重要位。其实为了提高提取信息的精确性，我们还可以对信息进行重复隐藏，同时把信息隐藏到最不重要位或者在不同的区域隐藏相同的信息。

隐藏前后的 Lena 图像分别如图 3.12、3.13 所示，可以看到，图像在隐藏前后在亮度上有轻微的变化，基本上没有发生太多的改变，具有较好的视觉效果。隐藏的文本信息如图 3.14 所示，图 3.15 是从隐藏后的图像中提取的信息。考虑到图像的信息隐藏容量，在隐藏的时候，我们只隐藏了图示信息的前面 633 个字节的信息。

图 3.12 原始图像

图 3.13 信息隐藏后图像

```
Northwestern Polytechnical University (NPU) is situated in Xi'an, a world-famous ancient
capital city. NPU is one of the 15 key universities in China, and during the"Seventh
Five-year Plan"and the"Eighth Five-year Plan", NPU had been one of the universities of state
capital construction. At the beginning of the"Ninth Five-year Plan", NPU was approved by the
state to be in the first group of universities funded by"Project 211", and at the later
stage of the"Ninth Five-year Plan", NPU was selected as one of the 21 universities of the
state capital construction.
```

图 3.14 原始文本信息

```
Northwestern Polytechnical University (NPU) is situated in Xi'an, a world-famous ancient
capital city. NPU is one of the 15 key universities in China, and during the"Seventh
Five-year Plan"and the"Eighth Five-year Plan", NPU had been one of the universities of state
capital construction. At the beginning of the"Ninth Five-year Plan", NPU was approved by the
state to be in the first group of universities funded by"Project 211", and at the later
stage of the"Ninth Five-year Plan", NPU was selected as one of the 21 universities of the
state capital construction.
```

图 3.15 从隐藏图像中恢复的信息

(2)数据隐藏率

可以看到采用上述的隐藏方法具有较高的信息隐藏容量，它几乎相当于每个像素点隐藏了一位信息。它的主要缺点是鲁棒性不高，这是所有与 LSB 类似的隐藏方法的缺点[15]，因为它们都在空域内直接对像素的灰度值进行操作，相应的如果灰度值的信息受到损失，则不太容易恢复出所隐藏的信息。

(4)检测算法

上述所采用的隐藏方法在恢复所隐藏的信息时，必须拥有正确的原始介质图像，否则不可能正确恢复出信息来。这是因为如果要恢复出隐藏的信息，同样需要计算所分成块的方差，但是我们在嵌入信息后，图像的像素值发生了改变，我们不能利用隐藏后的图像的方差来判断某个块是否隐藏了信息，还必须借助于原始图像进行。

阈值的选择并没有固定的公式可言，还是以人的主观感觉为标准，这是一个很难确定的问题，下一节中，我们给出了近似的进行区域选择的方法。

用方差来描述图像的区域平滑程度只是一种近似，是一种比较粗糙的测量方法，而且计算量比较大，对于图像来说，一般它都具有一定的连续性，我们可以采取抽样的方法来计算如隔行采样，隔列采样等。

§3.3.3 基于平坦测度的隐藏方法

陈默等[16]提出了图像块平坦测试的概念，它的目的是为了在帧间进行编码时，对扫描方式进行选择的优化策略，现在我们把它运用到信息隐藏过程中去，同样取得了较好的隐藏效果。

1 图像的平坦度函数

块的平坦测度(Flatness measurement)指块的像素在水平和垂直两个方向上的综合分布特点。假定块的大小为8×8大小。块的平坦测度定义如下：

$$F = aF_v + bF_h$$

其中F_v和F_h分别是块的垂直和水平平坦测度，a、b 是比例因子，它们的作用是调节水平和垂直平坦测度以获得子块的综合平坦测度。一般$a = b = 1$, F_v和F_h

分别定义如下：

$$F_v = \sum_{i=0}^{7} F_v(i)$$

$$F_h = \sum_{i=0}^{7} F_h(i)$$

其中：$F_v(\ )$和$F_h(\ )$定义如下：

$$F_v(j) = \sum_{i=0}^{6} FM(l_{i+1,j} - l_{i,j}).j = 0,1,\Lambda\ ,7$$

$$F_h(j) = \sum_{i=0}^{6} FM(l_{j,i+1} - l_{j,i}).j = 0,1,\Lambda\ ,7$$

其中 FM()为相邻像素平坦测度函数，定义如下：

$$FM(x) = \begin{cases} 1, x \geq T \\ 0, x < T \end{cases}$$

T 是控制阈值，控制阈值的确定由人类视觉系统对于像素亮度变化的敏感度决定。一般而言，阈值可以由实验得出。控制阈值 T 的选择依赖于图像块本身的起伏特性,图像的起伏特性可以由图像像素的方差表征。如果图像的像素的方差较大，则阈值也要较大，否则，方差较小，阈值也小。方差的计算可以由下式完成：

$$\sigma^2 = \sum (x-m)^2 p_x(x)$$

其中：

$$m = \sum x_i p_{x_i}$$

在实际计算时我们可以简化为：

$$m = \frac{1}{64} \sum_{i=0}^{7} \sum_{j=0}^{7} l_{i,j}$$

$$\sigma^2 = \frac{1}{64} \sum_{i=0}^{7} \sum_{j=0}^{7} \left(l_{i,j} - m\right)^2$$

得到方差后就可以用实验的方法获得控制阈值 T，仍然利用陈默[16]在实验中所得到的经验公式：

$$T = \sigma^2 / 30 + 1$$

另外控制阈值与量化参数也有一定的关系，直观的分析表明，控制阈值大，子块的平坦度小，控制阈值小，子块的平坦度大，因为控制阈值与图像的方差为线性关系。通过对 HVS(Human Visual System)的分析，HVS 对平坦区域的噪声比对非平坦区域的更加敏感，因此如果一个块的平坦测度较大，就要采用精细量化，反之则采用粗糙量化。通过平坦度和控制阈值的关系我们可以调整量化参数，从而有效地分配码位，达到较好的图像质量。这是把平坦测度矩阵运用到图像编码中去，同样的道理，我们也可以把它运用到信息隐藏中去，我们通过分析图像的平坦测度矩阵来进行信息嵌入区域的选择。如查某块的图像平坦测度较大，则证明这个块位于图像变化比较平坦的区域，我们在这些区域内应该尽量少隐藏或者不隐藏信息，如果它的平坦度较小，则证明它的变化不是很平稳，可能就处于图像变化较强的区域，根据人的视觉特性，在这些区域内进行信息隐藏，不会给图像造成失真，具有较好的不可察觉性。

图 3.16 Lena 图像

图 3.17 隐藏后的图像

我们首先把 Lena 图像进行 8×8 的分块，分块后计算 128×128 的 Lena 图像的平坦度矩阵如下：

5	0	3	4	5	5	6	6	3	3	0	2	0	0	7	0
2	1	4	5	6	4	5	1	0	4	2	3	5	2	0	4
0	1	4	5	5	4	6	4	1	0	1	2	6	0	0	1
1	1	6	5	1	7	4	4	4	2	0	2	0	0	4	0
3	1	4	1	0	3	3	5	2	3	2	0	2	0	0	4
4	2	5	0	1	4	3	0	2	2	5	0	0	1	2	4
3	2	6	1	1	2	2	3	0	8	0	0	0	0	3	4
3	2	3	5	1	2	3	0	1	2	0	1	5	1	3	2
1	3	5	0	2	0	1	0	0	3	0	1	1	3	0	3
2	2	4	2	4	1	0	1	2	1	0	1	0	4	3	5
3	2	2	3	1	0	1	2	5	0	0	1	0	6	1	4
0	3	3	1	1	0	3	0	7	0	0	1	5	2	1	2
0	3	0	2	2	2	7	4	1	1	0	1	2	2	0	0
0	2	0	2	1	0	6	1	6	3	4	0	5	1	0	4
0	1	0	4	2	0	1	1	3	3	1	0	0	2	0	1
1	1	4	3	1	2	1	4	5	6	2	1	8	0	7	4

图 3.18 Lena 图像的平坦测度矩阵

2 实验结果及结论

从图像的平坦度矩阵可以看到，在图像的变化比较平滑的区域它的平坦度较大，在图像变化比较复杂的地方，平坦度较小。根据实验结果，我们认为如果平坦度大于 3 就认为比较平坦，如果小于 3 就可用来隐藏一定量的信息。图是我们在图像的平坦度小于等于 3 的区域的每个像素的低三位用文本信息所替换，隐藏了 3792 个字节的信息，所恢复的信息由于它的信息容量较大，我们没有将其列出。从隐藏前后图像的比较可以看到，隐藏后的图像与原始图像并没有太明显的改变，满足了信息隐藏视觉上不可感知性的要求，取得了较好的视觉效果。

§3.3.4 基于模糊隶属度的隐藏算法

1．图像的模糊分类及隐藏原理[17]

在图像层和宏块层进行 H.263 的码率控制时，提出在宏块层采用前向控制的方法，根据视觉掩蔽特性设计模糊分类器，确定人眼对每个宏块的敏感程度和相应的量化步长因子。能在视频输出码率恒定的条件下，保持图像质量的稳定，取得了较好的视觉效果。

我们采用模糊感觉分类法，分别计算亮度掩蔽特性、空间掩蔽特性和时间掩蔽特性的隶属度，然后对计算出的结果进行加权平均来确定高敏感度、一般敏感度和低敏感度的隶属度，然后选取这几个隶属中的较大者来确定这个宏块的敏感度类型。亮度掩蔽特性是指在背景亮度较亮或较暗时，人眼对亮度不敏感的特性。空间掩蔽特性是指随着空间变化频率的提高，人眼对细节分辨能力下降的特性。时间掩蔽特性是指随着时间变化频率的提高，人眼对细节分辨能力下降的特性。实验表明，当灰度值小于 55 时，绝大多数观察者的感觉为黑或非常暗；当灰度值大于 220 时，感觉为非常亮，经过实验，所得到的亮度隶属度曲线如图所示：

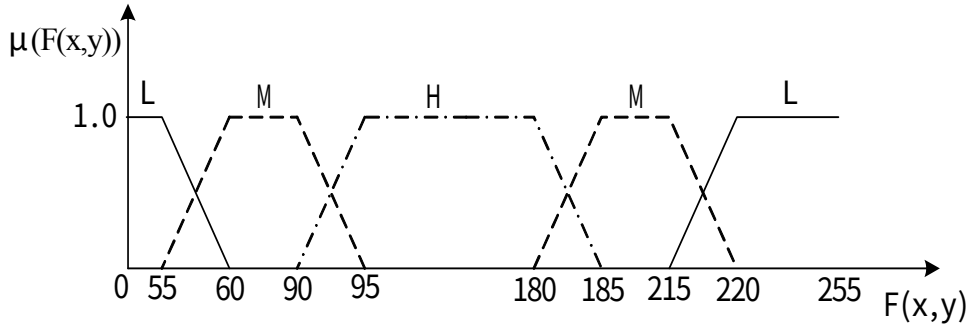


图 3.19 像素的隶属度分类

其中横坐标表示图像的灰度值，纵坐标表示的是亮度的隶属度，H 表示高度敏感类，M 表示中度敏感类，L 表示低敏感类。从图中可以看出人类视觉系统对亮度的敏感特性是从灰度值为 140 左右的值开始，呈对称分布，由中心向两边逐渐下降的。也就是说，人眼对中等的灰度值的变化较敏感，而对最亮或最暗的区域的灰度值的变化不是很敏感,向低灰度和高灰度两个方向非线性下降。

同样我们也可以利用这种特性来进行数据隐藏，我们只需把所要隐藏的消息嵌入在灰度值属于不敏感的像素中就不会引起人的察觉。隐藏的原理如下：首先我们对图像在空间域内进行分块，每个块的大小为 3×3，计算每个块的亮度均值 μ，如果这个值隶属于低敏感类，我们就先把整个块的最低三位清零，然后相应的信息位，否则我们只改变像素的 LSB 位。

2 实验结果及讨论

在实验过程中我们发现，如果灰度值的均值接近于 0，这时采用改变每个块的低三位是不明智的，这会给图像在某些较暗的地方造成光斑，引起图像的失真。我们在嵌入信息的过程中，对嵌入的标准进行改进。由隶属度曲线我们可以看出，在平均灰度值小于 60 或大于 215 的块，就可以认为是低敏感类，我们就要在这类块中嵌入信息。考虑到信息隐藏的不可见性，我们选择对每个块的均值 μ，30< μ <60 及 215< μ <245 之间的块内进行信息隐藏，这是因为我们通过实验发现，在低敏感类的块中如果改变其像素值的大小在 30 范围内，人眼还是不能察觉到的。信息嵌入的方法是采用信息位来替换每个块的低三位。信息隐藏的载体仍然采用 Lena 图像，隐藏后的图像如图所示，所恢复出来的文本如图所示，我们在载体中嵌入了 502 字节的信息。从图中可以看到，经过信息嵌入后的载体仍然很难从肉眼分辨出与原始图像的区别，也没有给原始图像造成任何失真，具有较好的不可见性。

图 3.20 隐藏后的图像

```
Northwestern Polytechnical University (NPU) is situated in Xi'an, a world-famous ancient
capital city. NPU is one of the 15 key universities in China, and during the"Seventh
Five-year Plan"and the"Eighth Five-year Plan", NPU had been one of the universities of state
capital construction. At the beginning of the"Ninth Five-year Plan", NPU was approved by the
state to be in the first group of universities funded by"Project 211", and at the later
stage of the"Ninth Five-year Plan", NPU was selected as one of the 21 universities of the
state capital construction.
```

图 3.21 所恢复的内容

§3.4 调色板方法

(1)技术要点

为了节省图像的储存空间，将图像中最具有代表性的颜色提取出来，利用三个位元组记录每个的 RGB 值，将它放在文件的头部，这就是调色板。然后针对图像中每个像素的 RGB 颜色值，在调色板中查找相应的颜色，并记录其索引值。因此，在调色板中隐藏信息必须选择具有调色板的图像，一般是 8 位灰度或彩色图像。

最早的利用调色板来隐藏信息的方法是：改变调色板中的排列次序来代表被嵌入的信息。由于它不会改变像素的颜色，因此嵌入信息后的图像与原始图像是相同的。而采用 LSB，奇偶性方法或其它在图像的调色板中实现信息的隐藏信息方法则不同，它是通过改变图像的颜色来实现信息的嵌入。对于灰度图像，这种改变还是可以容忍的，对于彩色图像，就必须认真的加以考虑，这是因为彩色图像调色板中相邻的索引颜色值并不是相近的，有可能差别很大，如果轻微的改变索引就有可能造成图像颜色的巨大变化,引起视觉上的严重失真。

(2)隐藏效率

根据不同的信息隐藏方法，信息隐藏效率也是不同的，但是有一个致命的弱点是调色板隐藏的信息量不会太大。这是因为调色板的颜色种类是固定的，8 位灰度或彩色的都是 256，嵌入容量小是这个技术的主要缺点之一。针对这个问题，张哲峰等[18]提出一种隐藏算法，可以有效地提高嵌入的数据量。

(3)鲁棒性分析

在调色板内隐藏信息的鲁棒性是较差的，有一些图像处理软件在打开图像时，就可能对图像的调色板进行了修改，在另存时就会破坏掉已经嵌入的信息。

(4)检测算法

调色板的检测算法是与嵌入算法相关的，一般提取时都比较容易。

(5)一些问题

图像的调色板是图像的一个较特殊的组成部分，实际上它是不太适合于嵌入信息的，在少量信息传递还是可以采用的。它的主要优点是在图像受到攻击时如加入噪声、剪切处理等，仍然能够恢复出所隐藏的信息，它的缺点也是很明显，就是传递的信息量完全依赖于调色板的大小。

§3.5 基于差值运算的图像隐藏技术

1. 隐藏算法的原理

在利用像素差值进行信息隐藏时，首先计算每个图像的差值矩阵，差值矩阵的计算方法如下：

1）对于每一行，计算它的每个灰度值与前一个像素的灰度值的差；

2）对于第一列，坐标为(1,1)的像素的灰度值保持不变，第一列其它的像素值都减去坐标为(1,1)点像素的灰度值。

像素差值的图像隐藏技术是利用相邻像素具有相似的灰度值的特性来隐藏信息，只有在边界的地方才有灰度值的突变。直接把所得到的秘密图像的差值矩阵与介质图像的每个像素的灰度值进行叠加，它要求通信双方必须拥有介质图像才能正确提取出隐藏的图像信息。由于差值矩阵与介质图像叠加后很可能出现边界溢出的情况，因此必须对隐藏前的差值矩阵进行量化处理，接收方在收到隐藏后的介质时只要进行相应的逆量化就可以恢复出隐藏的信息。由于我们所针对的是灰度图像，因此所得到的差值范围也位于-255-255 之间，

量化时采用奇数代表负数，偶数代表正数。首先对 0-255 的灰度值进行量化处理，每个图像像素值除以 5，再把所得到的结果分成不同的区间，每个区间代表不同的数据，用奇数表示差值矩阵的正值，负数则用偶数表示，差值矩阵量化表如 3. 1 所示。接收方在收到图像后只要对图像进行减法操作就可得到秘密图像经过量化后的差值矩阵，在恢复原图像的差值矩阵时，我们把所得到的量化矩阵进行反量化处理，均以所处区间的中间值来代替，这样所得到的矩阵会与原始的差值矩阵有误差，最大的值为 25，这在灰度图像中，较难分辨出

这种差异。

信息嵌入步骤描述：

(1) 把所得差值矩阵中的所有值量化，都除以 5，0-255 的数值范围除以 5 后变为 0-51，由于差值矩阵也会出现负值的情况，因此正确的范围应该是 -51~51。

	6-10	11-15	16-20	21-25	26-30	31-35	36-40	41-45	46-51
1	3	5	7	9	11	13	15	17	19
-1~ -5	-6~ -10	-11~ -15	-16~ -20	-21~ -25	-26~ -30	-31~ -35	-36~ -40	-41~ -45	-46~ -51
2	4	6	8	10	12	14	16	18	20

表 3.1

(2) 在进行反量化处理时，假如所得到的值为-10，绝对 10，为偶数我们则认为它所处的区间为-21—25，这时取值时以-23 为量化差值，-23*5 即为差值矩阵的值。

(3) 假如在对图像进行叠加操作时会出现边界溢出的情况，这时我们采用减法处理，使得到的结果仍然处于所在的区间不过是符号相反。我们举例如下：假如介质图像的灰度值是 240，要加入的值是 20, 240+20 显然超出了 255，这时我们用 240-20 来代替。在提取隐藏的数据时，介质图像的灰度值是 240，隐藏后的图像是 220，220-240=－20，取其绝对值为 20，查表得量化值为-48。

信息恢复时的步骤简述：

(1) 首先我们根据原始介质图像计算它与所得到的隐藏后的图像二者之间的差值，并对其取绝对值运算。

(2) 对所得到的结果按照表 3.1 来求出量化后的差值矩阵，并对所得的结果反量化得到秘密图像的差值矩阵。

(3) 根据秘密图像的某个像素的灰度值(也可以认为是密钥)来计算原始的秘密图像的灰度值，这样就可以恢复出原始的秘密图像。

2. 实验结果及讨论

图 3.22 是原始的介质图像，要传输的秘密图像如图 3.23 所示，我们计算图

3.23 差值矩阵，对它进行量化处理后叠加到图 3.21，所得到的结果如图 3.24 所示。可以看到，隐藏后的图像在亮度上有所改变。由于是灰度值的叠加，在亮度上是有所增加的，但是在没有原始介质的图像的情况下，不太容易确定图像的内容是否发生了改变，满足了信息隐藏的不易察觉性的要求。但是这种方法由于在量化时引入了量化误差，因此所恢复出的图像信息在亮度上有所偏暗，我们在对恢复出的图像进行灰度值的修正，所得到图像几乎与原始的秘密的图像没有区别，取得了理想的信息隐藏效果。恢复的图像和经过灰度修正的图像分别如图 3.25 和 3.26 所示。

这种方法的密钥就是秘密图像的任意一点的灰度值，因为如果知道图像中任意一点的灰度值就可根据这个点的灰度值计算出其它点的像素灰度值。这种方法的优点是在传输过程中，传输的是像素差值矩阵，而不是原始的图像数据，即使传输的数据被截获，如果不知道正确的密钥，也很难恢复出原始图像的数据信息。它的主要缺点是在提取隐藏的信息时必须拥有正确的原始介质图像。

图 3.22 原图

图 3.23 秘密图像

图 3.24 掩密图像

图 3.25 恢复的图像

图 3.26 经过修正的图像

从以上各种空间域隐藏方法可以看出，空间域的信息隐藏一般具有容量大的特点，但是鲁棒性都不太好。

第四章 基于 DCT 的信息隐藏技术

§4.1 基于离散余弦变换的信息隐藏技术

DCT 变换的全称是离散余弦变换(Discrete Cosine Transform)，是指将一组光强数据转换成频率数据，以便得知强度变化的情形。根据人类视觉系统模型，若对高频的数据做些某些修改或处理，再重新转换成为原来的形式时，虽然与原始的数据有些差异，但是人类的眼睛却是不容易分辨出来。DCT 变换是 JPEG，MPEG 压缩编码的核心，它较好的利用了人类视觉系统的特点，在保持图像质量的前提下，较好的实现了对图像的压缩，下面我们简要介绍一下 JPEG 压缩的流程。

§4.1.1 JPEG 压缩原理介绍[19]

JPEG 压缩一般要经过四个步骤：颜色模式转换及采样、离散余弦变换(DCT，Discrete Cosine Transform) 变换、量化、编码，压缩的具体流程如图 4.1 所示：

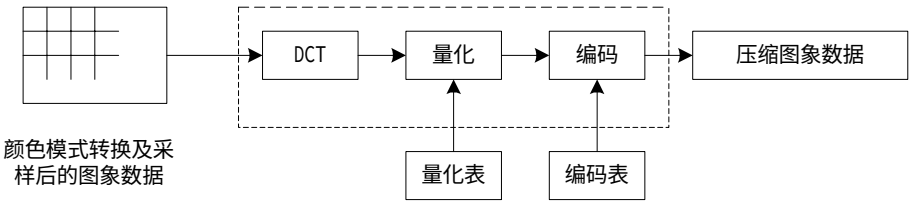


图 4.1 DCT 压缩编码步骤

1．颜色模式转换及采样

RGB 色彩系统是我们最常用的表示颜色的方式。JPEG 采用的是 YCbCr 系统。要用 JPEG 基本压缩方法处理真彩色图像，首先要把 RGB 颜色模式图像数据转换为 YCbCr 颜色模式的数据，Y 表示亮度，Cb、Cr 分别表示色度和饱和度，它们的计算公式分别如下：

Y ＝0.2990R+0.5870G+0.1140B

Cb = − 0.1687R − 0.3313G+0.5000B+128

Cr = − 0.5000R − 0.4187G − 0.0813B+128

人类的眼睛对低频数据比对高频的数据具有较高的敏感度，事实上，人类眼睛对亮度的改变也比对色彩的改变要敏感得多，也就是说 Y 成分的数据是比较重要的。由于 Cb 和 Cr 成份的数据相对不是太重要，就可以只取部分数据来处理来增加压缩的比例。JPEG 通常有采样方式：YUV 4：1：1 和 YUV 4：2： 2，分别代表 Y，Cb 和 Cr 三个数据成份的采样比例。

2. DCT 变换

JPEG 将整个亮度矩阵与色度 Cb 矩阵，饱和度 Cr 矩阵，视为一个基本单元称作 MCU。每个 MCU 所包括的矩阵数量不得超过 10 个。例如，行和列采样的比例皆为 4：2：2，则每个 MCU 将包括四个亮度矩阵，一个色度矩阵及一个饱和度矩阵。当图像数据分成一个 8×8 矩阵后，因为 DCT 转换公式所接受的数字范围是在 - 128 和+127 之间，还必须将每个数值减去 128，然后一一代入 DCT 变换公式中，即可达到 DCT 变换的目的。

JPEG 压缩时首先将原始图像数据分成 8×8 的数据块，作为二维 DCT 变换的输入，DCT 变换的公式如下所示：

$$F(u,v)=\frac{1}{4}C(u)C(v)\left[\sum_{i=0}^{7}\sum_{j=0}^{7}f(i,j)\cos\frac{(2i+1)u\pi}{16}\cos\frac{(2j+1)v\pi}{16}\right]$$

它的逆变换的公式如下：

$$f(i,j)=\frac{1}{4}C(u)C(v)\left[\sum_{u=0}^{7}\sum_{v=0}^{7}F(u,v)\cos\frac{(2i+1)u\pi}{16}\cos\frac{(2j+1)v\pi}{16}\right]$$

其中，

i,j 代表图像数据矩阵内某个数值的坐标位置。

f(i,j) 代表图像数据矩阵内的某个数据。

u,v 代表 DCT 变换一矩阵内某个数值的坐标位置。

F(u,v) 代表 DCT 变换后矩阵内的某个数值。

c(u)c(v)=1/1.414 当 u=0，v=0。

c(u)c(v)=1 其它。

经过 DCT 变换后的矩阵数据自然数为频率系数，这些系数以 F(0，0)的值

最大，称为 DC 直流系数，其余的 63 个频率系数则多半是一些接近于 0 的正负浮点数，我们把它们统称为 AC(交流)系数。经过 DCT 变换后，图像的大部分能量被集中在 DC 系数和一些低中频 AC 系数上，而其它的 AC 系数的绝对值都较小，大部分高频系数都变成了 0。

3. 量化

图像数据转换为频率系数后，还要接受一项量化程序，才能进入编码阶段。量化是对经过 DCT 变换后的频率系数进行量化。量化的目的是减小非“ 0”系数的幅度以及增加 “ 0”值系数的数目，同时也是为了实现压缩的目的。经过量化阶段后，所有数据只保留整数近似值，也就再度损失了一些数据内容，量化是图像质量下降的最主要原因，但是它并不影响图像给人的视觉效果，只是一些对人的视觉冗余的数据被丢弃。

量化阶段需要两个 8×8 矩阵数据，这是因为人眼对亮度信号比对色差信号更敏感，因此使用了两种量化表，一个是专门处理亮度的频率系数，另一个则是针对色度的频率系数，将频率系数除以量化矩阵的值，取得与商数最近的整数，即完成了量化。

当频率系数经过量化后，将频率系数由浮点数转变为了整数，这有利于于执行最后的编码。JPEG 标准所提供的参考量化表分别如下：

16	11	10	16	24	40	51	61
12	12	14	19	26	58	60	55
14	13	16	24	40	57	59	56
14	17	22	29	51	87	80	62
18	22	37	56	68	109	103	77
24	35	55	64	81	104	113	92
49	64	78	87	103	121	120	101
72	92	95	98	112	100	103	99

表 4. 1　亮度量化矩阵表

17	18	24	47	99	99	99	99
18	21	26	66	99	99	99	99
24	46	56	99	99	99	99	99

47	66	99	99	99	99	99	99
99	99	99	99	99	99	99	99
99	99	99	99	99	99	99	99
99	99	99	99	99	99	99	99
99	99	99	99	99	99	99	99

表 4.2 色度量化矩阵表

4. 编码

接着就是对量化后的数据进行编码压缩。由于相信直流系数间的相关性，对于直流系数，JPEG 标准采用的是 DPCM(差分编码)方法，而其它的 AC 系数则采用的是游程编码方法，从左上角开始沿对角线方向，以 Z 字形(Zig-Zag)进行扫描直至结束。量化后的 AC 系数通常会有许多零值，以 Z(Zig-Zag)字形路径进行游程编码有效地增加了连续出现的零值个数。编码过程是无损的，具体过程不在赘述。

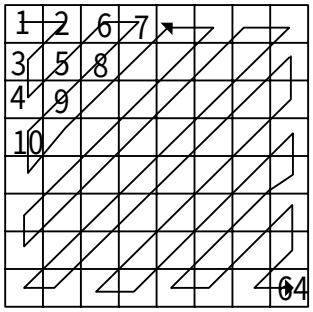


图 4.2 Zig-Zag 扫描途径

§4.1.2 基于离散余弦变换的水印嵌入

经过 DCT 变换后的系数被分成如图 4.2 所示的直流(DC)系数和交流(AC)系数，直流系数是标号为 1 的系数，其余的系数则是交流系数。直流系数基本上代表了图象块的平均值,交流系数则是从标号为 2 系数开始到标号为 64 的系数，依次从低频到高频过渡。考虑到人的视觉特性，低频是对人的视觉最重要的部分，对于 DCT 的低频系数要尽量给予保留，而高频系数在 JPEG 压缩流程的量化过程中容易被丢弃，信息最好也不要嵌入到高频系数中去，一般最好的选择是把信息嵌入到中低频系数当中去。就目前的文献[20-29]来看，大部分都是把水印嵌入在中低频区域。

1. 水印的嵌入方法

在 DCT 域进行信息编码的方法通常是通过调整一个图像块中的两个或多个 DCT 系数间的关系来实现信息的嵌入。在如图 4.2 所示的 Zig-Zag 形式的区域中，对于低频区域的描述，目前并没有统一的标准，不同的图像的低频区域也可能不尽相同，参考文献[11]，我们认为，通常情况下，按照 ZigZag 方向，从 2 到 10 的位置认为是低频区域，从 11 到对角线的区域是中频区域，其它的则认为是高频系数。频域内信息嵌入的方法通常都是在中频区域，且靠近低频区域的系数中进行信息的嵌入，这是因为越靠近低频区域，嵌入的信息经过各种各样的处理后保留的可能性就越大，反之则相反。

我们假设介质图像为 C(x,y),其中 C(x,y)∈{0,255}, x=0, 1, 2, …, M-1, y = 0, 1, 2, … N-1, M,N 分别为图像的高度和宽度。要嵌入的水印图像为 W(x,y),其中 W(x,y) ∈{0,1}, x=0,1,2,…,WW-1,y=0,1,2,…WH-1,WW,WH 分别表示二值图像水印的宽度和高度。一般来说要求 M，N 较 WW，WH 大，具体的规则应该由要嵌入的水印的大小以及可供嵌入的系数的多少来确定。

在水印图像 W(x, y)被嵌入之前，要对它进行预处理，采用置乱算法进行加密处理，这样做的目的是防止在水印嵌入后，介质图像产生出嵌入水印图像的轮廓。假设被置乱后的 W(x,y)为 W‘ (x，y)。介质图像 C(x,y)经过 DCT 变换后为 C(u,v)。在 DCT 域进行信息嵌入时，有许多种方法，可以利用 DCT 系数间的关系来进行隐藏，也可以进行加性的直接嵌入，采用加性的的方法是必须需要原始的介质图像才能正确的恢复出所隐藏的信息，而利用系数间关系的方法则不需要这种限制。我们采用系数间关系的方法来进行信息的嵌入，它的原理如下：

采用系数间关系的隐藏方法是在图像的 DCT 系数中，选取一对或多对 DCT 系数，通过改变 DCT 系数间的大小关系来确定所隐藏的信息流是 1 还是 0。我们为了简单起见，在一个 8×8 图像块中，只隐藏了一位的信息，因此只要选择两个 DCT 系数即可，假设分别为 $C_i(u1,v1)$，$C_i(u2,v2)$。它的原理就是假如我们要隐藏的数据位为‘ 1 ’，我们就让 $C_i(u1,v1)>C_i(u2,v2)$，否则我们就认为所嵌入的数据位为‘ 0 ’。如果 DCT 系数与要隐藏的信息不匹配，我们就改变 DCT 系数的值，可以采用互换位置或者是另外一个系数加上或减去一个数值。

2. 水印嵌入位置

在进行信息嵌入前，还有一些工作必须预先做的，就是参与通信的双方要能够知道信息嵌入的位置，这样才能正确的提取出所隐藏的信息。在 DCT 变换域内嵌入信息时，嵌入位置的选择也很重要，通常要考虑如下因素：

(1) 低频系数集中了图像信号大部分能量，对图像较为重要，因此信息嵌入于此具有足够的鲁棒性。而且低频系数通常具有较大的值，信息嵌入后对图像的影响较小，有利于保证不可见性。

(2) 直流系数代表了块的平均亮度，对直流系数的改变容易导致块效应(block effects), 块效应是指图像损伤或失真严重时在图像子块的边缘部分会出现不连续的现象。块效应的出现对图像的主观质量会产生明显的影响。

(3) 根据人眼的频域特性，人眼对于图像上不同空间频率成分具有不同灵敏度，对中频响应较高，而对高低频响应较低。

嵌入的位置我们可以通过伪随机序列来选择要嵌入的块，这里的每个块都是 8×8 的矩阵。这个序列我们可以认为就是双方通信的秘密密钥 K，由它作为种子来产生随机序列，要求这样随机数是不能重复的。同时选择要改变的 DCT 系数时，也要依据一定的准则，我们在利用关系进行隐藏时，必须考虑到 JPEG 压缩，因为在量化时有一些信息会损失。比如在隐藏编码信息‘ 1 ’时，要求 $C_i(u1,v1) > C_i(u2,v2)$，但是｜$C_i(u1,v1) - C_i(u2,v2)$｜的绝对值必须大于某个整数 T，这个 T 的取值是越大越好，这样有利于恢复信息，但会给图像的质量带来负面影响。如果要求能够抵抗 JPEG 压缩的攻击， T 的取值一定要大于量化表中的量化值，T 的取值和人的视觉特性有关，我们在下面的章节中对 T 的取值有详细的论述。这是因为在量化后 $C_i(u1,v1)$与 $C_i(u2,v2)$的关系不一定是事先所改变的那样。而且所选择的 DCT 系数最好在量化表中具有相同的量化值，如(4,2)与(3,3)等，这样保证图像在经过 JPEG 压缩时，信息能够得到正确恢复，如果选择不同的量化值，改变 $C_i(u1,v1)$与 $C_i(u2,v2)$的关系时，差值不够大的话可能会提取出错误的信息，差值太大又会影响图像的质量，这在实际的操作中必须进行比较和折衷。

在信息嵌入后，再经过逆 DCT 变换就变成了具有水印信息的图像，接收方在收到图像后，对图像作 DCT 变换，通过比较相应的 DCT 系数就可以恢复出信息。设 L 为量化表中相应位的量化值，信息位的嵌入和恢复方法具体可描述如下：

DCT 域信息嵌入方法：

```
For i=1 To WW*WH
    If  W‘i(x,y)=’1’ 要隐藏的水印信息位
        改变两个系数间的大小关系
        Ci(u1,v1)= Ci(u1,v1)+ abs(Ci(u1,v1)- Ci(u2,v2))/2+L
        Ci(u2,v2)= Ci(u2,v2)-abs(Ci(u1,v1)- Ci(u2,v2))/2
    Else
        Ci(u1,v1)= Ci(u1,v1)- (Ci(u1,v1)- Ci(u2,v2))/2
        Ci(u2,v2)= Ci(u2,v2)+ (Ci(u1,v1)- Ci(u2,v2))/2+L
    End IF
End For
```

DCT 域信息提取过程

```
For i=1 To WW*WH
    If Ci(u1,v1)> Ci(u2,v2)
        Mi =1
    Else
        Mi =0
    End If
End For
```

从上面的信息嵌入及提取过程可以看出，采用这种方法更直接方便，提取信息的时候也相对简单。

§4.1.3 实验结果及讨论

NorthwesternPolytechnicalUniversity

图 4. 3 原始图像及隐藏的文本信息

图 4.4 隐藏后图像

NorthwesternPolytechnicalUnivers

图 4.5 质量因子为 5 的 JPEG 压缩

NorthwesternPolytechnicalUnivers

图 4.6 质量因子为 3 的 JPEG 压缩

NorthwesternP/lytech由calUnivers

图 4. 7　5%的均匀噪声及提取的信息

Nortxwe[lurN?l■teyhnican諮i鰊bs

图 4. 8　5%的高斯噪声及提取的信息

我们对 DCT 域的嵌入算法进行了仿真，仍旧采用 128×128 的 Lena 图像作为信息嵌入的介质，图 4.3 分别是原始图像和要嵌入的信息。图 4.4 是信息嵌入后的图像，我们可以看到，采用在 DCT 域的数据嵌入算法，具有较好的隐藏效果。图 4.5 和图 4.6 是分别对隐藏后图像进行质量因子为 5 和 3 的压缩后的图像和提取的信息，压缩的方法采用 Photoshop 来实现，从实验结果可以看出，基于离散余弦变换的信息嵌入技术对 JPEG 压缩具有较高的鲁棒性。之所以能够经受 JPEG 压缩，这是因为 JPEG 压缩同样采用的是 DCT 变换，在 DCT 域内的嵌入方法较好的利用了 JPEG 的压缩原理，使得两个 DCT 系数的关系是以量化值的大小为基础的，要隐藏信息的两个 DCT 系数间至少要相差一个量化值，这样保证在经过 JPEG 压缩后，这两个系数间的关系不会因为压缩而改变。图 4.7 是在隐藏后的图像中加入 5%的均匀噪声及恢复出的信息，图 4. 8 是在隐藏后的图像中加入 5%的高斯噪声及恢复出信息，可以看到采用 DCT 变换嵌入的方法对均匀噪声不敏感，而对高斯噪声则比较敏感。

§4.2 DCT 域自适应的信息隐藏

在实际的具体应用中，图像信息的嵌入必须满足鲁棒性要求，同时嵌入图

像后的载体不会破坏原始图像的质量。因此需要一种根据图像本身特征自适应地调整图像信息嵌入的方法[30]，这有利于扩大图像隐藏的应用范围和质量。我们提出了改进的根据 JND (Just Notice Difference)特征值来确定图像信息嵌入强度的方法，取得了较好的隐藏效果。

§4.2.1 可视察觉门限

JND 是在不会导致视觉感观上失真的情况下，用来衡量某个特征所能允许的最大形变或误差。根据人类视觉系统的模型，超过这个门限值，人的眼睛就能感受到隐藏后的介质图像与原始图像的差别。JND(Just Notice Difference)取决于背景亮度，在黑暗区域或特别亮的区域，JND 值比较高，一般趋近于一个常数；在灰暗区域或中等亮度区域，JND 值比较低，但不是恒定值，而且在此情况下，人眼的灵敏度急速下降。根据 JND 的性质，在不引起视觉质量失真的情况下，要尽可能的隐藏信息，应对每个不同强度的块采用不同的门限值。

JND 随频率变化的示意图如图 4.9 所示，它是通过大量的实验所获得的结果[31]：

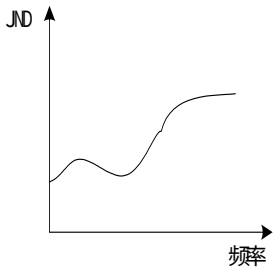


图 4.9 JND 随频率变化示意图

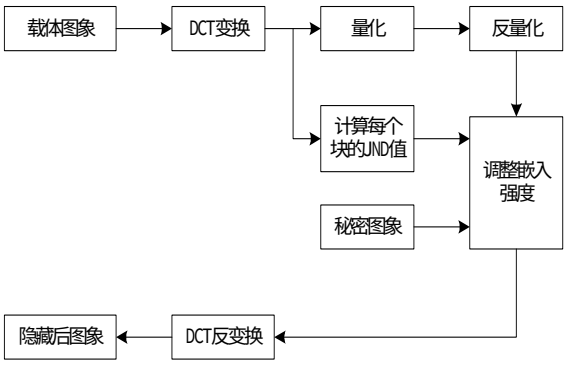


图 4.10 信息嵌入过程

水印信息嵌入在图像的 DCT 域，我们可以利用 Podilchuk[32]介绍的方法计算图像块的噪声敏感度大小：

首先我们将原始图像分成互不覆盖的块，块的大小为 8×8,记为：

$B_m = f_m(x,y)$，m=1,2,…，(M/8)*(N/8)

然后对每一图像块进行 DCT 变换，即：

$$B_m^{'} = DCT(B_m) = F_m(u,v)$$

我们在 DCT 域计算其对比度灵敏度

$$C(u,v) = 5.05e^{-0.178(u+v)}(e^{0.1(u+v)} - 1)$$

其中，u,v 为空间频率。利用对比度灵敏度矩阵 C(u,v)可以计算出一个8×8图像块对噪声的视觉敏感性，具体计算如下：

$$S_{DCT} = \sum_{\forall(u,v)} C(u,v)\left|F_{DCT(u,v)}\right|^2$$

其中，F_{DCT} 为图像块的离散余弦变换。S 值反映了人眼视觉对此图像块的视觉敏感性，S 值越大，人眼对图像中的噪声越不敏感，也就是说可以嵌入到此图像块的水印强度越高。

最后，我们利用 S_{DCT} 计算图像块的可视噪声阈值 JND [33]：

$$JND = \alpha \ln S_{DCT}$$

其中α是权值，用来调节噪声阈值的大小，其取值范围可由实验获得。在我们所做的实验中，α的值取为 3。

§4.2.2 改进的自适应信息隐藏方法

在 Podilchuk[32]所采用的水印嵌入算法中，是以如下的形式进行水印信息的嵌入：

$$V_k^{'} = \begin{cases} V_k + JND(b,r,s) * \beta & if V_k(b,r,s) > JND(b,r,s) \\ V_k & 其它 \end{cases}$$

其中 b 表示图像经过 DCT 变换后所分成的 8×8 块的块号，r，s 分别表示每个块中的行号与列号。Vk(b,r,s)表示经过 DCT 变换后的系数。β 是嵌入强度。

在 Podilchuk 所采用的方法中，水印是直接嵌入在图像的 DCT 系数中，但是这种方法并没有很好的利用图像数据的信息冗余及人的视觉冗余，信息嵌入量比较少。我们在此基础上对水印的嵌入方法进行改进，改进的方法的流程图如图 4.10 所示，它的步骤简述如下：

(1) 首先对图像进行分块 DCT 变换，获取图像的 DCT 系数 w(i,j)，同时计算每个块的 JND 值。

(2) 对得到的 DCT 系数按照亮度的量化表进行量化，得到量化后的图像整数值。

(3) 对第(2)步所得到的整数值进行反量化,得到反量化的 DCT 系数 w(i,j)。

(4) 在反量化所得到的 DCT 系数上进行图像信息的嵌入，对于灰度图像可采用不同的嵌入策略，选取不同的嵌入位置，以及不同的嵌入强度,嵌入的公式可采用如下的方法表示 w'(i,j)=w(i,j)+a*d(i,j)。其中，w(i,j)代表反量化后的 DCT 系数，d(i,j)代表所要嵌入的图像的灰度值。在信息进行嵌入时，要满足 a*d(i,j)的值要小于所计算出的每个块的 JND 值。

(5) 对第 4 步的结果进行逆 DCT 变换就得到了嵌入信息后的图像。

综合考虑上节所述的水印嵌入位置的因素，我们把图像信息嵌入在 DCT 域的中频系数位置，较好的保证了鲁棒性和不可见性的折衷。

信息在恢复时的步骤正好相反：在提取隐藏的信息时，需要原始的图像介质，这就要求通信双方在进行通信之前必须事先拥有介质图像，或者以一个较安全的方式来传输它，这是采用这种算法的主要缺点。采用这种方法的数字图像提取过程如下：

(1) 对载体图像进行分块 DCT 变换，获取图像的 DCT 系数。

(2) 按照亮度的量化表对得到的 DCT 系数进行量化，并对量化的结果的小数部分舍去，进行取整运算。

(3) 对第(2)步量化后的结果进行反量化。

(4) 对隐藏有信息的图像进行同样 DCT 变换，按照公式就可提取出所隐藏的信息，d(i,j)=(w ' (i,j)-w(i,j))/a。

我们之所以在反量化的 DCT 系数中进行信息隐藏是因为这样既考虑了图像的 JND 特性，也充分利用了图像的信息冗余，这也是我们对 Podilchuk 方法所改进的地方。我们首先来考虑 JPEG 压缩时采用量化的原因。量化的目的是在保持一定质量的前提下，丢弃图像中对视觉效果影响不大的信息，也就是一些高频信息，这是我们用来增加信息的嵌入量或嵌入强度的依据。JPEG 压缩

中的 DCT 变换实际上是空间域的低通滤波器，经过 DCT 变换后，低频分量集中在系数的左上角，它包含了图像的主要信息如(如亮度等)，相比之下，高频分量显得不那么重要，采用量化的方法去掉高频分量，从而达到压缩的目的。经过量化阶段后，所有数据只保留整数值，这是引起信息损失的根源，但是这并不影响人的视觉效果。

作者原先所采用的方法，信息是在图像还存在冗余的基础上进行叠加的，一方面它限制了信息嵌入量，另一方面也限制了信息嵌入的强度，这是因为强度过大会引起图像的失真。从作者所采用的方法可以看出，实际所嵌入的信息是 JND 值的 30%左右，而图像的冗余信息依然存在，在图像上再嵌入信息不可能不降低图像的视觉质量,实际上是在原来图像的基础上又叠加了多余的信息。信息隐藏的主要特点就是利用已存在图像的信息冗余数据，采用信息隐藏算法把信息嵌入到这些冗余数据中去，或者说是用要嵌入的信息来部分地替换冗余信息，达到视觉上不可见的目的。

§4.2.3 实验结果及讨论

所采用的介质图像和秘密图像如图 4.11 所示。在我们所做的实验中，首先计算图像的 JND 值，a 的值我们取 0.05, 这样保证所嵌入图像信息的值不会超过 JND 值，图 4.12 是采用 Podilchuk 方法隐藏后的图像和恢复的图像信息，图 4.13 是采用改进的算法所获得的隐藏图像和恢复的图像信息。可以看到，改进的方法具有较好的不可察觉性，取得了较好的隐藏效果。

在我们对 a 的值进行调整的过程中，如果 a 的值逐渐增大，是 Podilchuk 所采用的算法率先出现了图像失真，这与我们的理论分析是相符的。

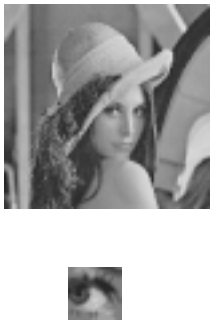


图 4.11

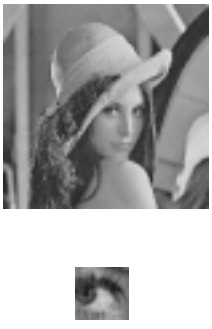


图 4.12

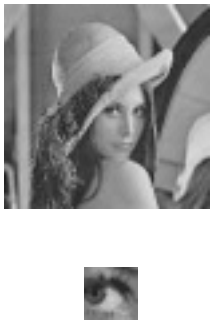


图 4.13

在考虑改进算法的鲁棒性时，我们对图 4.12 和图 4.13 隐藏后的结果进行了压缩，压缩的品质因数是分别为 90%和 75%，当压缩品质因数为 90%时两种算法所恢复出的图像信息分别如图 4.14 所示，图 4.15 分别是两种算法在压缩品质因数为 75%时所恢复的图像信息。从实验结果可以看到，在品质因数为 90%时，先前的嵌入方法已经出现了模糊，为 75%时已经不能看出原始图像的轮廓，而所改进的算法具有较好的抵抗 JPEG 压缩的能力，在压缩品质因数为 75%时基本上仍然能够分辨出原始图像的轮廓，这是与算法改进的初衷是相一致的。

图 4.14 品质因数为 90%

图 4.15 品质因数为 75%

本节提出了一种改进的自适应的数字图像信息隐藏算法，它充分利用图像所存在的冗余信息，结合人的视觉特性，在图像的 DCT 域内进行图像隐藏，取得了较好的视觉隐藏效果。它使隐藏后的图像对 JPEG 攻击具有较好的鲁棒性，计算简单，且容易实现。

§4.3 DCT 域的奇偶性嵌入算法

本节利用奇偶性的思想，提出了在 DCT 域内进行信息隐藏的方法，实验结果表明，该算法对 JPEG 压缩具有较好的鲁棒性。

§4.3.1 奇偶性隐藏原理

众所周知，DCT 变换后的高频系数经过量化后大部分都变成了零，这些高频系数的丢失对原始图像所要表达的信息并无大的妨碍，不影响图像的视觉效果，从零的个数奇偶性出发，我们提出了利用中高频系数中零的数目的奇偶性来进行信息的嵌入。这种方法通过改动 DCT 系数量化后 DCT 系数中零的个数的奇偶性来实现信息隐藏。假设我们设定 0 的个数为偶数时代表所隐藏的信息位为‘1’，奇数时表示信息位为‘0’。

信息嵌入的步骤如下：

(1) 对载体图像 C(x,y)进行 DCT 变换，获取 DCT 变换后的系数 $C_{DCT}(x,y)$。

(2) 按照 JPEG 亮度量化表对 DCT 系数进行量化 Cquant(x,y)。

(3) 计算量化后的中高频区域系数为 0 的个数。

(4) 根据所隐藏的信息位改变相应的系数。

(5) 逆 DCT 变换，得到嵌入信息后的图像 C'(x,y)。

信息的提取方法是信息嵌入的逆过程：

(1) 对 C'(x,y)进行 DCT 变换，得到频域系数。

(2) 对 DCT 系数按照 JPEG 亮度量化表进行量化。

(3) 计算量化后中高频区域 0 的个数，判断其奇偶性，如果为奇数则输出为 0，否则输出为 1。

(4) 每 8 位数据来组成一个二进制数据。

(5) 这些二进制数据就是所隐藏的代码，根据隐藏信息的类型，把这些代码转化为相应的格式如图像，声音，文本数据等，就得到所隐藏的信息。

对按照嵌入规则进行隐藏时，必须考虑如何来改变 DCT 系数，假如我们要隐藏的信息位为‘1’，如果中高频区域 0 的个数为奇数，这时我们改变靠近中频区域的系数，按照 Zig-Zag 的扫描方式，最好是改动 8×8 方块中对角线附近的中频系数。

对于载体 C(x,y),以及信息序列 $M_i \in \{1,2,\cdots,n\}$具体的嵌入规则如下:

```
For i=1 : n
    对于 C _quant(x,y)中数据块 Bi，假设 Bi(u,v)≠0
    If Mi=1
        IF   Bi 中高频区 0 的个数为奇数
             改动 Bi(u,v)使 Bi(u,v)＝0
        End If
    Else
        IF   Bi 中高频区 0 的个数为偶数
             改动 Bi(u,v)使 Bi(u,v)＝0
        End If
    End If
End
```

其实我们还可以对这种方法进行改进，因为我们没有必要来计算整个高频区域系数为 0 的个数，这是因为在经过量化后整个高频区域基本上全部为 0，我们可以选择靠近中频区域某一部分的系数的奇偶性进行信息隐藏。按照 Zig-Zag 的扫描方式及 8×8 块的排列方式，我们所选择要改动的系数主要集中在(6,1)，(5,2)，(4,3)这一对角线附近位置的系数。

§4.3.2 实验结果及讨论

NorthwesternPolytechnicalUniversity

图 4.16 原始图像及秘密的文本信息

图 4.17 嵌入后图像

NorthwesternPolytechnicalUnivers

图 4.18 压缩质量因子为 80%及提取的信息

NorthwesternPolytechnicalUnivers

图 4.19 压缩质量因子为 49%及提取的信息

NorthwesternPohytech.icalUnivers

图 4.20 2.03%的高斯噪声及恢复信息

NortnwestmvTolytEchnmcanEnm

图 4.21 5.41%的均匀噪声及提取信息

" @

图 4.22 图像中值滤波后恢复的信息

图 4.16 表示的是原始图像及待出入的秘密消息，图 4.17 表示的是嵌入秘密信息后的图像。可以看出，采用本算法隐藏前后的图像除了亮度有点偏暗外，并没有发生太大的改变，不会影响人的视觉效果，具有较好的视觉不可见性。

由于每个 8×8 块只能隐藏一位信息，因此在 128×128 的 Lena 图像里面我们只隐藏了 32 字节的信息。图 4.18 是对隐藏图像进行压缩后的图像，压缩质量因子为 80%，所恢复的信息在图 4.19 的下方。图 4.19 分别是压缩质量因子为 49%时的图像及恢复的信息。从实验结果中可以看到，算法对于 JPEG 压缩具有较强的鲁棒性，在质量因子为 80%及 49%时仍然能够正确恢复出嵌入的信息。图 4.20 是加入 2.03%的高斯噪声的隐藏图像及恢复的信息，图 4.21 是加入 5.41%的均匀噪声后的图像及所恢复的信息。从实验结果中可以看到，当加入 2.03%的高斯噪声时，已经有两位文本信息发生了错误，而加入 5.41%的噪声时则与原始信息发生了较大的出入。图 4.22 是图像经过 3×3 的中值滤波后所恢复的信息，可以看到，经过 3×3 的中值滤波后，几乎不能恢复任何原始信息，算法对滤波比较敏感。经过分析，我们认为，这是因为我们改变高频系数的奇偶性时，实际上是在原始图像上加入了高频信息，这些高频信息散步在图像上大部分很可能变成了一些孤立的噪声点，而中值滤波对于消除孤立的噪声点则是十分有效的。因此采用中值滤波后，代表所嵌入信息的像素点就可能发生了改变，不能正确的恢复出原始的信息。

§4.4 基于融合的信息隐藏技术

图像融合技术较早的应用是在遥感图像的处理，随着遥感技术的不断发展，已经使传感器空间分辨率、光谱分辨率得到大幅度提高，从而也使获得的数据呈海量的增加，同时也导致了数据源的多样性和复杂化，遥感影像融合是一种通过高级影像处理技术来复合多源遥感影像的技术，其目的是将单一传感器的多波段信息或不同类传感器所提供的信息加以综合，消除多传感器信息之间可能存在的冗余和矛盾，加以互补，降低其不确定性，减少模糊度，以增强影像中信息透明度，改善解译的精度、可靠性以及使用率，以形成对目标的完整一致的信息描述。

丁玮[34]等也提出了在空间域内进行图像融合的方法，我们结合他们的研究

成果提出了在 DCT 变换域内进行图像融合的方法。其基本的思想如图 4.23 所示。首先对原始介质图像和要传输的秘密图像分别进行 DCT 变换，然后按照一定的比例在频域内进行融合。

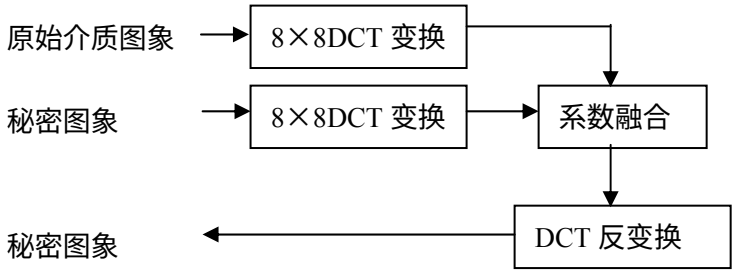


图 4.23 DCT 域图像融合方法

§4.4.1 图像融合隐藏原理

为了说明问题方便我们假设两幅图像具有相同大小，假设一幅介质图像为 C(x,y)，要隐藏的图像为 G(x,y)，其中 0≤x≤M，0≤y≤N。将两幅图像进行融合的方法为：

$F(x,y)=G(x,y)\times a+C(x,y)\times(1-a)$

其中 a 的值可位于 0 到 1 之间的数，它的取值直接影响到融合的效果。

恢复时采用 $G(x,y)=(F(x,y)-(1-a)\times C(x,y))/a$

我们所提出的方法是首先对介质图像和要隐藏的图像分别做 DCT 变换，对变换后的系数进行融合，融合后的系数再经过 DCT 反变换就达到了隐藏目的。其具体的步骤阐述如下：

(1) 对介质图象和要隐藏的图象分别做 DCT 变换，C2(u, v) = DCT (C(x, y))，G2(u, v)=DCT(C(x, y))，其中 0≤u≤M，0≤v≤N。

(2) 对变换后的 DCT 系数按如下公式进行融合。

$F(u,v)=C2(u,v)\times(1-a)+G2(u,v)\times a$。

(3) 对 F(u, v)进行逆 DCT 变换就得到了嵌入信息后的图象。

F2 (x, y)=IDCT(F(u, v))。

基于融合的图像隐藏技术在恢复时需要原始图像的信息才能正确恢复，恢复时的框图如图 4.24 所示，它的步骤可简述如下：

(1) 对介质图像和隐藏后的图像分别作 DCT 变换，C2(u,v)=DCT(C(x,y))，F3(u,v)=DCT(F2(x,y))。

(2) 由公式 G2(u,v)=(F3(u,v)－(1－a)×C2(u,v))/a 就可求出所隐藏图像信息的 DCT 系数。

(3) 对 G2(u,v)进行逆 DCT 变换就得到了所隐藏的图像信息。

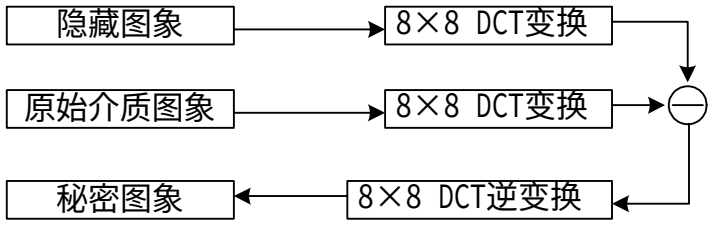


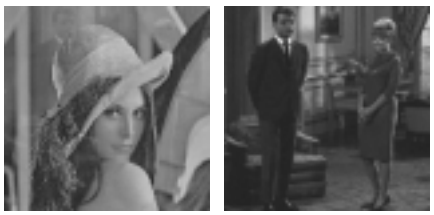
图 4.24 恢复信息框图

§4.4.2 实验结果及鲁棒性分析

图 4.25 是载体图像，图 4.26 是要传递的秘密图像，它们大小相同都是 128×128。

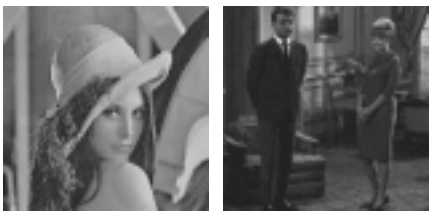
图 4.25 Lena

图 4.26 Couple



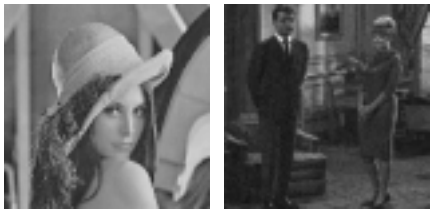
a=0.2 恢复的图像

图 4.27



a=0.1 恢复的图像

图 4.28



a=0.05 恢复出的图像

图 4.29

图 4.27，图 4.28 和图 4.29 分别是 a 取 0.2，0.1，0.05 时融合效果和恢复的图像。从实验结果我们可以看到，随着尺度 a 的不同，所取得的隐藏效果也是不同的，在 a=0.1 和 0.05 时都具有较好的不可见性，取得了较好的隐藏效果。由于 Couple 图像的整体灰度偏暗，因此在 a=0.1 时，整个图像的效果要较原始图像暗，但是它仍然具有较好的视觉效果。在 a=0.2 时，在隐藏后的图像上已经出现了被隐藏图像的轮廓，在实际进行图像信息隐藏时，为了尽可能的提高嵌入图像信息的不可见性，一般是首先对秘密图像进行置乱，一方面为秘密图像提供了另外一层的保护，另一方面也使图像自身的一些相关信息被打乱，使隐藏后的失真不会集中在某一区域上。

图 4.30 和图 4.31 分别是在 a=0.05，对融合后的图像进行 JPEG 压缩，质量因子分别为 95%和 80%时所恢复的图像。从实验结果中我们可以看到，所恢复的图像存在大量的噪声，在 95%时仍然能够反映出秘密图像的信息，在质量因子为 80%时基本上不能表达出原始图像的信息轮廓。

压缩质量因子为 95%时的恢复图像

图 4.30

压缩质量因子为 80%时的恢复图像

图 4.31

§4.5 基于差值矩阵的频域隐藏算法

§4.5.1 差值矩阵的计算及隐藏原理

对差值矩阵进行 DCT 变换，在 DCT 域内利用 DCT 系数间的关系来隐藏数据，由于所得到的矩阵是经过差值运算的，实际上相当于图像的边缘检测算子，因此在经过变换后的图像里面实现信息隐藏时所依赖的准则就与直接进行 DCT 变换再隐藏信息有所不同，而且所得到的隐藏效果也各不相同。

在进行 DCT 系数的选择时，根据人的视觉模型，人眼最敏感的部分是 DCT 变换的低频部分，所以我们要尽量保留低频系数。而在 JPEG 有损压缩会丢弃

高频部分，所以要隐藏的信息应该避免涉及高频系数。因此在隐藏信息时，应当使信息尽量嵌入在接近低频系数的中频系数位置，对中频系数进行调整来达到嵌入信息的目的。而在实际操作时，我们针对的 DCT 系数不再是图像的 DCT 变换的系数，而是它的差值矩阵，在实际的实验过程中，我们仍是选择隐藏信息在中频系数的位置，对这些系数进行选择时，是根据隐藏效果以及图像本身的特性来选择。选取不同的系数所得到的隐藏效果各不相同，对于变化较平缓的图像就要不断的实验来达到令人满意的效果，这是由于在进行隐藏时会引起图像的局部失真，而对较嘈杂的图像，也需要进行实验，只是它更容易达到较实际的隐藏效果。

由于我们针对的是差值矩阵的 DCT 系数，同样也存在高频和低频信息，可以很容易的分析，这些高频信息也正是图像变化较大的区域，也就是图像的边缘或纹理区域。我们仍然按照 DCT 域隐藏信息的准则，在差值矩阵的 DCT 系数内实现信息嵌入。

假设原始图像为 F(x，y){0≤x≤M，0≤y≤N}，M，N 分别为图像的宽度和高度。利用差值矩阵进行信息隐藏的步骤如下：

(1) 首先计算 F(x，y)的差值矩阵 G(x，y)；

(2) 对所得到的差值矩阵 G 进行分块的 8×8 的 DCT 变换；

(3) 选择适当的 DCT 系数来实现信息隐藏，这里我们利用两个系数间的关系来进行信息隐藏，隐藏的具体方法如在 DCT 域内进行隐藏的相同，不再赘述。

隐藏信息的提取步骤：

(4) 对于隐藏后的 DCT 系数进行逆 DCT 变换得到差值矩阵 G’；

(5) 利用差值矩阵 G’对原始图像进行重构，得到的就是隐藏后的图像，利用它就可进行信息传输了。

(6) 接收方在收到图像后，首先计算出图像的差值矩阵，然后对差值矩阵进行 DCT 变换，根据 DCT 系数间的关系就可提取出隐藏的信息。

§4.5.2 实验结果及鲁棒性分析

我们所选择的介质图像是 256×256 的 Bridge 灰度图像，要嵌入的图像

是一幅二值图像。首先我们计算出介质图像的差值矩阵，然后对差值矩阵进行 8×8 块的 DCT 变换，在所做的实验中，我们选择 8×8 方块中中频系数的对应位置为(4,4)，(3,5)，利用这两个系数之间的关系来隐藏信息。隐藏前后的图像分别如图 4.32 和 4.33 所示。从图像中我们可以看到，隐藏后的图像除了在亮度上有点偏暗外，基本上没有损失原始图像所要表达的信息，只传输其中的一幅图很难区分是否隐藏有信息，而且如果图像没有经过任何处理，仍然可以正确恢复出原始嵌入的图像信息。

我们把秘密图像信息按照顺序依次嵌入到介质图像中去，在对图像进行剪切处理操作时所恢复的水印分别如下各图所示：

为了测试算法的鲁棒性，我们用恢复出的图像与原始图像信号一致的元素在原始信号中所占有的比率来衡量原始信号与恢复信号之间的相似程度。

假设原始图像为 G(i，j)，恢复出的图像为 F(i，j)

$$\text{Sim}=\frac{\sum_{i=0}^{M-1}\sum_{j=0}^{N-1} S_{ij}}{M\times N}\times 100\%\text{，}\ S_{ij}=\begin{cases}0 & \text{如果} G(i,j)\neq F(i,j)\\ 1 & \text{如果} G(i,j)=F(i,j)\end{cases}$$

我们分别就图像受到左上角、右上角，左下角、右下角、中心裁剪以及不规则剪切攻击时，嵌入图像在没有经过预处理所提取到的图像信息进行了分析，所得到的结果分别如下各图(均为缩略图)所示。

原始图像

嵌入信息后的图像

原始秘密图像，32×32

Sim=100%

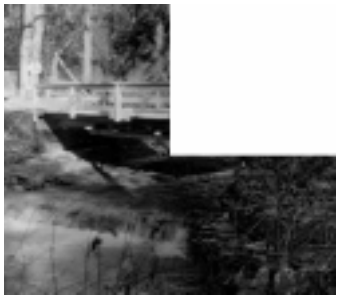
恢复图像

图 4.32

图 4.33

Sim=81.45%

图 4.34



Sim=79.10%

图 4.35

Sim=83.30%

图 4.36

Sim=79.00%

图 4.37

Sim=84.67%

图 4.38

Sim=92.58%

图 4.39

可以看到，原始秘密图像没有经过预处理，受到剪切处理所恢复的信息，在某种程度上也反映了隐藏后的图像所受到的攻击位置，也就是说，可以看到针对隐藏后的图像的操作实际上相对于对对水印图像相应部分的操作，这是因为我们在隐藏信息时没有对图像信息进行任何预处理，使得对图像的操作所影响的秘密图像的损坏位置比较集中，可能会影响秘密信息的正确表达。

为了减轻这些攻击对秘密图像整体效果的损害，我们首先对秘密图像进

行预处理，对秘密图像进行置乱，目的是利用若干步骤的矩阵变换，打乱原矩阵中各元素的位置，使原先有规则的元素分布。在经过多次变换后呈现无规则、接近随机的分布，从而起到对信息保密的作用。采用置乱的具体方法[35]详述如下。

设 M× M 大小的二维方阵 A 为：

A=a(i, j) |i, j=0 , 1 ,⋯ , M-1。

其中 a(i, j)为某一元素。利用矩阵变换的置乱步骤如下：

(1) 镜像运算：对原矩阵 A 做对称的镜像运算，对称轴既可取垂直中线(左右镜像)，也可取水平中线(上下镜像) ，两者取其一。

a) 当取垂直中线时，有 B=Mt(A)。其中 B=b(i，j)，b(i，j)为 B 的某一元素，且 b(i，j) =a(i，M－j－1)。当取水平中线时 b(i，j) =a(M－i－1，j)。

(2) 旋转运算: 将矩阵 B 的元素旋转 90 度，旋转方向可采用顺时针，也可采用逆时针，两者取其一。

b) 如果采用顺时针时，有 C=Rt(B)。其中 C=c(i，j)，c(i，j)为 C 的某一元素，且 c(i，j)=b(M－j－1，i)。如果采用逆时针，c(i，j)=b(j，M－i－1)。

(3) 循环移位运算：对经过上述变换的矩阵进行循环移位运算，移动的位数是一个随机数，移动的方向可以是循环右移，也可以是循环左移，二者取其一。

c) 采用循环右移一个随机数据 n 时，有 D＝Shift(C)，其中 D＝d(i，j), d(i，j)为 D 的某一元素。所得到的矩阵如下：

i. 当 j＜n 时 d(i，j)= c(i，j+n)

ii. 当 j＞n 时 d(i，j)= c(i，j－M+n+1)

d) 采用循环左移 n 时，所得到的矩阵如下：

i. 当 j＜n 时 d(i，j)= c(i，M－1－n+j)

ii. 当 j＞n 时 d(i，j)= c(i，j－n)

在将图像进行隐藏之前通常要进行置乱预处理，这样做的优点是可以避免

图像在嵌入后产生可见的图像轮廓，而且增强了算法的鲁棒性，增加了攻击的难度。我们所采用图像是 32×32 的二值图像，首先采用上述置乱的方法对图像进行置乱，我们置乱的方法是采用上下镜象运算，顺时针旋转 90 度，每一行循环移动的位数如下：

9 3 30 4 1 12 22 14 18 16 9 17 17 27 9 11 19 6 27 28 7 12 30 25 4 30 13 28 6 23 7 30

在经过一次置乱后图像如图 4.40 所示，可以看到，一次置乱并没有达到所要求的随机效果，我们对图像在嵌入前进行二次置乱，所得到的效果如图 4.41，在经过各种剪切操作攻击后所恢复的图像分别如下列各图所示。

图 4.40 一次置乱

图 4.41 二次置乱

图 4.42 置乱后的图像隐藏效果

Sim=81.64%

图 4.43

Sim=83.01%

图 4.44

Sim=80.96%

图 4.45

Sim=78.32%

图 4.46

Sim=89.06%

图 4.47

Sim=93.65%

图 4.48

从恢复的图像可以看到，采用置乱后，经过剪切处理后，秘密图像所有被破坏的内容不再集中于某个区域，在隐藏后图像某块区域受到的攻击分散到整个秘密图像的空间上，秘密图像的整体效果并没有受到太大的影响，使得对剪切攻击具有一定的鲁棒性。

第五章 总结展望

本文在介绍了信息隐藏的基本知识后，主要对静止图像的信息隐藏进行了研究分析。首先介绍了空间域中常见的信息隐藏方法——LSB 替换算法、奇偶性方法、调色板方法等，并结合人类视觉系统特点，提出基于图像方差、平坦度、模糊隶属度等隐藏技术，还对基于差值矩阵的隐藏进行了实验；然后，在频率域中对 DCT 域的隐藏算法进行了比较详细的论述，提出了 DCT 域自适应的隐藏算法、DCT 域的奇偶性嵌入算法、基于融合的信息隐藏技术，以及差值矩阵的频率隐藏算法并进行实验仿真。

以下是对下一步需要做的工作：

1．结合密码学的应用。针对密钥掩密技术中通信双方事先约定共享密钥这一假设并不总是可以实现的问题，可以借助 Shamir 三次传递协议等密钥交换协议，安全的生成一个双方共享的密钥。

2．小波域的信息隐藏。近年来，小波在许多科学和工程技术方面得到了广泛应用，小波同时具有较好的时频局部化特性，为传统的时域分析和频域分析提供了完美的结合。在 JPEG2000 图像压缩标准中，已经采用小波来做为图像压缩编码的主要技术。在小波域内的信息隐秘，可以充分利用人类的视觉模型(HVS)的一些特性，使嵌入信息的隐秘性和鲁棒性得以改善。小波域信息隐藏具有良好的研究前景。

3．有效的隐藏检测方法。隐藏技术和检测技术是相互制约、相互促进的，魔高一尺，道高一丈，基于某一数字媒体的隐藏技术会引起相关的检测技术的出现，而检测技术反过来又会促使产生新的隐藏技术。信息隐藏的检测与提取是今后信息隐藏技术的研究热点，在这方面的工作也将会对信息隐藏技术的发展起到积极的促进作用。

4．相关自主软件系统的开发。只有建立了自己的攻防平台，并经常加以补充最新技术，才能在信息安全方面处于“ 进可攻，退可守 ”的有利地位。

参考文献

[1]. 汪小帆，戴跃伟，茅耀斌，信息隐藏技术方法与应用.机械工业出版社，北京，2001

[2]. 尤新刚，周琳娜，郭云彪，信息隐藏学科的主要分支及术语，CIHW2001，pp.43.

[3]. 基于彩色静止数字图像的信息隐藏技术研究，http://www-900.ibm.com/developerWorks/cn/security/se-eshow/index.shtml

[4]. R. G. Schyndel，A. Z. Tirkel， and C. F. Osborne， A digital watermark. In: Proceedings of IEEE International Conference of Image Processing, Austin, Texas. Nov. 1994,2，pp.86~90.

[5]. Tutorial of JPEG 2000 Standard，http://www.jpeg.org/JPEG2000.htm

[6]. http://www.cotse.com/tools/stega.htm

[7]. http://www.funet.fi/pub/crypt/steganography/

[8]. Simmons, G. J., The Prisoners' Problem and the Subliminal Channel, In Advance in Cryptlopy, Proceedings of CRYPTO'83, Plenum Press, 1984, pp. 51 – 67.

[9]. 杨尚英，朱虹，李永盛，一种数字图像的信息伪装技术，CIHW2001，pp.172.

[10]. 卢燕，赵德斌，高文，一种基于小波变换的数字图像水印加入与抽取算法，CIHW2001，pp.276.

[11]. 丁玮,数字图像信息安全的算法研究，中科院博士论文,2000.5,北京,中科院计算机研究所.

[12]. Ding Wei, Yan Wei-Qi, Qi Dong-Xu, Digital Image Scrambling Technology Based on Gray Code, Proc. of the 6th International Conference on Computer Aided Design & Computer Graphics, Wen Hui Publishers, Dec., 1999, 3:900-904.

[13]. 李国富，基于正交拉丁方的数字图象置乱方法，北方工业大学学报，Vol. 23, No. 1, 2001, pp: 14 –17.

[14]. Human Visual System Features Enabling Watermarking，

http:// www-it.et.tudelft.nl/~inald/pubs/ Watermarking/ICME2002.pdf

[15]. Jiri Fridrich, Rui Du, Meng Long: Steganalysis of LSB Encoding in Color Images, ICME (2000)

[16]. 陈默，李维钊，图像块平坦测度与系数扫描方式选择，计算机与信息技术 2001 年第 1－2 期，pp: 76-80

[17]. 贾志科，崔慧娟，唐昆等，H.263 活动图象编码器控制研究，通信学报，20(7) 1999，pp:1-7.

[18]. 张哲峰，刘红梅，黄继武，黄夏菱，大容量无失真数据隐藏算法，CIHW2002 论文集，pp.1

[19]. 张益贞，刘滔，Visual C++实现 MPEG/JPEG 编解码技术，人民邮电出版社，2002.

[20]. Mohanty, S. P., Ramakrishnan, K. R., Kankanhalli, M. S., A DCT domain visible watermarking technique for images. IEEE International Conference on Multimedia and Expo, 2000, pp: 1029-1032.

[21]. Lin, S. D., Chin-Feng Chen, A robust DCT-based watermarking for copyright protection, International Conference on Consumer Electronics, 2000, pp: 10-11.

[22]. M. Barni, F. Bartolini, V. Cappellini, A. Piva, A DCT domain system for robust image image watermarking, Signal Processing, Vol.66, No.3, 1998, pp357-372.

[23]. D. Tzovaras, N. Karagiannis, M. G. Strintzis, Robust image watermarking in the subband or discrete cosine transform domain, in 9th European Signal Processing Conference(EUSIPCO'98), Island of Rhodes, Greece,8-11 Sept. 1998, pp:2285-2288.

[24]. Young Liang Guan, Jing Jin, An objective comparison between spatial and DCT watermarking schemes for MPEG video, Information Technology: Coding and Computing, 2001, pp: 207-211.

[25]. Guo-rui Feng, Ling-ge Jiang, Chen He, Dong-jian Wang, A novel algorithm for embedding and detecting digital watermarks, 2003 IEEE International

Conference on Acoustics, Speech, and Signal Processing, Vol. 3,2003, pp: 549-552.

[26]. Lam E Y, Goodman J W. A mathematical analysis of the DCT coefficient distributions for images. IEEE Trans. On Image Processing, Vol. 9, No. 10, 2000, pp:1661-1666.

[27]. Wen-Nung Lie, Guo-Shiang Lin, Chih-Liang Wu, Ta-Chun Wang, Robust image watermarking on the DCT domain, IEEE International Symposium on Circuits and Systems, Vol. 1, 2000. pp:228-231.

[28]. Suthaharan, S., Transform domain technique: robust watermarking for digital images, Proceedings of the IEEE, 2000, pp: 407-412.

[29]. Lin, S. D., Chin-Feng Chen, A robust DCT-based watermarking for copyright protection, International Conference on Consumer Electronics, 2000, pp: 10-11.

[30]. Han-Seung Jung, Nam-Ik Cho, Sang-Uk Lee, Image-adaptive watermarking based on warped discrete cosine transform, IEEE International Symposium on Circuits and Systems, Vol. 3, 2002, pp: 209-212.

[31]. 钟声，图象压缩技术及其应用，电子学报，Vol.23 No.10 1995：117-123

[32]. Christine I. Podilchuk, Wenjun Zeng, Image-Adaptive Watermarking Using Visual Models, IEEE Journal on Selected Areas in Communications, 1998,Vol.16, No. 4：525-540

[33]. 易开祥，数字图象加密与数字水印技术研究，浙江大学博士论文，2001,7

[34]. 丁玮，闫伟齐，齐东旭，基于置乱与融合的数字图象隐藏技术及其应用，中国图象图形学报，Vol. 5, No. 8, 2000.

[35]. 卢朝阳，周幸妮，一种新的数据信息置乱算法，计算机工程与科学，Vol. 20, No. 3, 1998, pp: 28-31.

致谢

在论文完成之际，我向关心我、爱护我的老师同学致以深深的谢意。

首先，感谢导师慕德俊对作者的关心和支持，感谢他给我们提供了一个良好的学习和工作环境。

感谢戴冠中教授，他所创造的和谐，民主、自由的学术气氛使我受益匪浅，他那渊博的知识、严谨的治学态度以及平易近人的作风，深深影响着我。

感谢张新家老师在我求学期间所给予的热情帮助，张老师正直的品格，踏实的工作态度和广博的知识，使我获益非浅。

感谢我的师兄夏煜、曹卫兵、刘航、邓智群、杨德明、苗胜、张开来、吕宝军等和师姐郎荣玲、刘利、谭旭阳等，感谢他们在学习上给我的支持与帮助，他们踏实的求学作风，都给我树立了很好的榜样。尤其感谢夏煜和曹卫兵两位师兄在我毕业设计期间的无私帮助。还要感谢两位师兄何明耘和丁景涛，他们知识广博，从他们那里学到了很多有用的信息，学到了如何学习。

感谢教研室里的同学，段雪峰、廖国威、张军、杨立友、胡伟、张治、徐超、王沛、于彩荣、李小梦、刘茜茜、陆琛、耿炎等，经过三年研究生的学习阶段，大家在一起共同学习和工作，共同努力，相互提高，关系融洽，亲如兄弟姐妹，我将永远怀念这个家。谢谢他们陪我共同度过了人生中一段难忘的时光。

感谢同学徐德文、杨涛、徐超，与他们相处的日日夜夜，记忆中充满了美丽的浪花。

最后，感谢我的父亲母亲，以及姐姐、妹妹、弟弟，是他们的默默关怀、鼓励和支持，使我走到现在。

再次感谢所有关心我、支持我的家人、朋友、同学和老师。