西安科技大学

硕 士 学 位 论 文

二维码与图像信息隐藏相结合的研究

专业名称：信号与信息处理

作者姓名：殷颢玻

指导教师：张释如

西安科技大学

学 位 论 文 独 创 性 说 明

本人郑重声明：所呈交的学位论文是我个人在导师指导下进行的研究工作及其取得研究成果。尽我所知，除了文中加以标注和致谢的地方外，论文中不包含其他人或集体已经公开发表或撰写过的研究成果，也不包含为获得西安科技大学或其他教育机构的学位或证书所使用过的材料。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做了明确的说明并表示了谢意。

学位论文作者签名：　　日期：

论文题目：二维码与图像信息隐藏相结合的研究

专　　业：信号与信息处理

硕 士 生：殷颢玻　　(签名)_____

指导教师：张释如　　(签名)_____

摘　要

随着因特网技术的不断进步，信息传输已经在现代社会的各个领域有了广泛的应用。为了确保信息的安全性和隐秘性，信息隐藏技术应运而生。经过二十余年的发展，信息隐藏技术已成为信息安全、通讯、计算机、信息处理领域中重要研究课题。

本文首先介绍了研究背景，二维码与信息隐藏技术的国内外发展现状，指出基于二维码的图像信息隐藏技术存在的问题，接着给出了二维码图像信息隐藏模型，然后提出了两种新的图像信息隐藏算法，分别是基于二维码的 LSB 新算法和基于二维码的 DCT 隐藏新算法。

基于二维码的 LSB 新算法是先将秘密信息 1 转换成二维码图像，再将二维码图像转换成灰度图像，然后将秘密信息 2 利用 LSB 算法写入到灰度图像中，这时的灰度图中保存了两份秘密信息，达到提升容量的目的。基于二维码的 DCT 新算法是将秘密信息编码为二维码，并转换为灰度图像，再将灰度图像利用 DCT 算法隐藏到载体图像，从而实现信息的 DCT 域隐藏。

第五章研究了两种算法的抗压缩性能，通过计算机仿真说明了本文算法具有一定的抗 JPEG 类压缩能力。最后一章总结全文内容，并指出下一步的研究方向。

关 键 词：二维码；信息隐藏；图像处理；LSB 算法；DCT

研究类型：理论研究

Subject ： Research on combination of QR code with image information hiding

Specialty ： Signal and information processing

Name ： Haobo Yin （Signature）_____

Instructor： Shiru Zhang （Signature）_____

ABSTRACT

With the continuous development of internet technology, information transmission has found wide applications in the areas of modern society. In order to ensure the security and confidentiality of information, information hiding technology arises at the historic moment. More than 20 years passed, information hiding has been an important research topic in the field of information security, computer, communications and information processing.

This thesis first introduces the research background, QR code and information hiding technology with present situation at home and abroad, points out the problems of image information hiding technology which is based on QR code, and gives QR code image information hiding model. This thesis then presents two kinds of information hiding algorithms, namely QR code based improved LSB algorithm and QR code based DCT hiding algorithm.

The QR code based improved LSB algorithm converted the No.1 secret information to QR code, transforms QR code to gray image, and uses the LSB algorithm to hide the No.2 secret information in carrier image, which achieves the goal of expanding capacity because of additional secret information. The QR code based DCT hiding algorithm encodes the secret information to QR code, changes QR code to gray image, and uses the DCT hiding algorithm to hide the secret information in carrier image, which finishes the information hiding process in DCT domain.

The chapter 5 researches the anti-compression properties of two types of new algorithms, and shows their resistance to JPEG like compression by computer simulation. Last chapter summarizes the full text content, and points out the next research direction.

Keywords ： QR code; Information hiding; Image processing; LSB algorithm; DCT

Thesis ： Basic Research

目 录

1 绪论

1.1 本文的研究背景及意义

信息技术从上世纪四十年代开始至今取得了迅猛的发展，现在已将人类的生产和生活带入了一个崭新的阶段。信息引发社会各界的激烈竞争，已经成为当今社会最重要的战略资源。从军事方面来看，人类社会发展已经越过了大刀长矛的“冷兵器”时代，大炮坦克的“热兵器”时代，直到现今逐渐转变到现代的“发现即摧毁”的“信息战”时代；在普遍存在的“制空权”、“制地权”和“制海权”的基础上，“制信息权”已经成为现代战争的突出特点，也就是说：谁掌握了战争的信息权，谁就掌握了战争的主动权。在当前的工业化与信息化社会中， “资金”和“技术”作为商业领域的重要发展手段，与信息化一起成为现代化工业社会商业竞争的“三大法宝”；在金融、贸易等重要的商业领域里，信息的重大作用甚至有远超过“资金”和“技术”，信息即生命，信息即金钱，信息即商机。信息的安全已经成为人类财富安全首要关注的问题，在信息技术发展领域，随着信息技术的不断发展，信息的安全性已经显得日益重要与越发紧迫。

信息隐藏[1]从 20 世纪 90 年代提出，是一种解决信息安全问题的新方法。这种技术是把隐秘信息隐藏到可公开的数字媒体的载体中，它的目的是为了安全的传递隐秘信息，保证载体的完整性和所有权归属等作用。与传统的加密技术相比较，它的不可读性隐藏了隐秘信息的内容，而且不可见性掩盖了隐秘信息存在的事实，这就对隐秘信息的安全提供了更好的保护。当前，在军事上和民用上来说，信息隐藏技术广泛应用于匿名、隐秘通信、证件防伪、版权标志等领域。利用信息隐藏进行隐秘通信可以避免内容加密引起的敌人注意缺陷，因此各个国家都普遍采用信息隐藏技术来进行隐蔽通信和间谍活动，常用于信息安全保护和信息战中。信息隐藏技术也被恐怖分子利用来从事恐怖活动，如早在 2001 年 9 月，美国 HINDU 新闻组就报道了恐怖分子头目“拉登”可能利用隐写图片向其同伙散布消息、传递信息、筹集资金、组织恐怖袭击、策划恐怖行动等[2]。

另一方面，二维条码[3]是一种可对信息进行高密度编码的技术，其在二维空间上由具有特殊机构的几何图像元素按一定规律和顺序组合成的图形，妙巧地利用构成计算机内部逻辑结构的“0”、“1”比特流的概念，即使用若干个与二进制相对应的几何图形来表示信息。其不仅可以保存英文、数字等符号信息，还可以保存中文、图片、声音、指纹等多种数据类型，且纠错能力很强，当纠错等级提高时污损 33%情况下依然可以完整读出信息。

当前信息隐藏算法的研究按嵌入域可划分为变换域、空间域等隐藏算法；按嵌入的载体可划分为图像隐写、视频隐写和音频隐写等。虽然由于嵌入域和嵌入载体的不同，

信息隐藏算法的研究会有不同的着眼点，但它们从充分载体特征的角度去寻求隐藏三要素（鲁棒性、容量、不可见性）间最好的权衡，并未考虑秘密信息的变化会对隐藏算法的影响。而本课题研究的主要内容是将二维码与图像信息隐藏技术向结合。在秘密信息嵌入到载体图像前，先用二维码技术对秘密信息进行编码，这样可以利用二维码的信息量大、抗污损高等特点，提高隐藏的容量和秘密信息抵抗攻击的性能。在信息隐藏时，考虑如何设计适合二维码特征秘密信息的隐藏算法，即从考虑秘密信息和载体两个角度入手，来探寻解决当前信息隐藏领域所存在问题的一条思路。

本课题的研究是以西安空间无线电技术研究所的国家自然科学基金面上项目(代号：61372175)为背景而展开的，该基金项目的主要研究内容是在卫星信道下的信息隐藏技术。利用卫星数据传输系统传输秘密信息属于一个较新的研究领域，而本课题是在二维码的基础上给出了一种解决数据传输信息隐藏问题的方法和思路。因此，本课题的研究具有一定的理论意义和实际应用价值。

1.2 国内外发展概况

1.2.1 二维码的发展现状

关于二维码, 在上世纪 80 年代末，美国、日本等国家的企业和研究机构就开始进行研究[3][4][5][6][7]，1989 年，美国国际资料公司已经发明了 Data Matrix，原名 Data Code；1991 年留美华人王寅敬(音)博士发明 PDF417 码，并由讯宝(Symbol)公司制定完成；1992 年，美国知名的 UPS(United Parcel Service)快递公司推出了 UPS 码，即为 Maxicode 二维码的前身；1994 年，日本 Denso 公司发明了 QR 码 (Quick Response Code)；2009 年，微软推出了一种新的二维码即“Microsoft Tag"，增加了色彩维度，即因此称为彩色条码。国外研究二维码标准化的研究机构主要包括美国标准化协会(ANSI)、国际自动识别制造商协会(AIMI)、新成立的国际标准化组织/国际电工委员会第一联合委员会的条码自动识别技术委员会(ISO/IEC/JTCI/SC31)，其中 ANSI 与 AIMI 已经完成 PDF417 , Q R code , Code One，Code 16K, Code 49 等码制的符号标准，国际标准化组织/国际电工委员会第一联合委员会的条码自动识别技术委员会(ISO/IEC/JTCI/SC31)已经制定了包括 PDF417 码的国际标准 ISO/IEC15438:2006，QR 码的国际标准 ISO/IEC 18004:2006， Data Matrix 的国际标准 ISO/IEC 16022:2006 等二维码的国际标准，并且在不断的完善中。

我国对二维码的研究始于 1990 年左右，由中国物品编码中心对几种常用的二维码，比如 PDF417, QR Code, Code One, Data Matrix, Code 16K, Code 49 这样的编码技术规范进行翻译，并且进行了跟踪研究。2003 年，上海龙贝信息科技公司推出了龙贝二维矩阵，2005 年，在中国编码中，已经完成了汉信码的研发[8]，在 2002 年和 2003 年两年时间里，深圳矽感科技公司已于研发了具有自主知识产权的 CM 二维码和 GM 二维码[9]。国家质

量监督局也制定了相关的二维码的国家标准，主要包括了 GTB 17172-1997《四一七条码》、GB/T 21049-2007《汉信码》以及 GB/T 18284-2000《快速响应矩阵码》。

1.2.2 信息隐藏的发展现状

在信息隐藏的发展历史中，早在古希腊时期，就已经有了古老的隐写术。古希腊的历史学家 Herodotus 的史著中记载着一个非常有名的故事：公元前 491 年，被放逐的斯巴达国王 Demaratus 在获知波斯皇帝 Xerxes 企图侵略希腊的意图后，将平时书写用的小蜡板的上层蜡刮除，再将 Xerxes 的企图刻在木板，重新用蜡封上，把消息成功送到了斯巴达皇宫。公元 16 世纪中期，意大利的卡尔达发明了漏格板，覆盖在密文上，可从漏格中读出明文，这是较早的一种分置式密码。我国古代也早有以藏头诗、藏尾诗及绘画等形式来进行信息隐藏的例子。历史上诸如此类的隐写方法还有很多。在近代，隐形墨水、缩微胶片都曾是信息隐藏非常重要的技术手段，这些技术在第一次世界大战中也被广泛应用[10]。在现代，又发明了许多方法用于信息的隐藏，如高分辨率缩微照片、语义编码、扩频通信等领域。

从数字媒体为载体的数字信息隐藏来看，国际上正式提出从事这方面的研究是由 1992 年 C. Kurak 等[11]提出的图像降级用于秘密交换图像开始的，其融合了数字信号处理、图像处理、语音处理、视频处理、密码等多学科和领域。在国际上，也就是 1996 年 5 月，第一届信息隐藏研讨会于在剑桥大学举行，在这次会议上首次将信息隐藏的理论作为一个新学科来研究和应用。另外一些非常知名的学术组织，主要包括 IEEE，ACM，EURASIP，SPIE 等，它们主办的学术会议中，主要是设置专题介绍或以杂志专辑的形式对信息隐藏技术进行讨论和分析的。

在国内，信息隐藏技术也受到了广泛的关注。在 1999 年的 12 月，由我国信息安全技术领域的何德全、周仲义、蔡吉人这三位院士、组织有关的科学研究单位联合发起的，在北京，由电子技术应用研究所举办，组成了全国第一届信息隐藏学术研讨会(CIHW)。CIHW 时至今日已有十届会议得到了成功的举办。国家级的 863 计划智能计算机专家组、中国科学院自动化研究所和北京邮电大学信息安全中心一起召开了专门的关于数字水印技术研讨会。

许多大学和研究院所都在研究信息隐藏技术，高校理论研究较多，研究机构以自身应用背景开展信息隐藏技术研究[12][13]，得到了国家自然科学基金、行业基金项目的支持[13] [14][15][16]。

1.2.3 基于二维码的信息隐藏发展现状

由于二维码的特殊性，当前国内外针对二维码图像的隐藏研究相对还较少。但随着二维条形码的广泛应用，二维码图像隐藏技术已开始逐渐受到国内外学者的重视。当前

对二维码隐藏的研究主要可分为以二维码为载体和以二维码为秘密信息等两种隐藏算法的研究。其中，研究主要集中于前者，例如：文献[17]将水印信息变成二值后，通过对 PDF417 形码中“条”进行移位嵌入数字水印；文献[18]提出了一种在 QR 二维码的频域中进行可逆信息隐藏算法；文献[19]根据当前移动电话大量使用的事实，提出了一种离线 QR 码认证的方法。较之于前者，将二维码作为秘密信息的研究相对要滞后，但随着研究的深入也取得了一定的研究成果，例如：文献[20]将秘密信息 QR 条形编码后嵌入载体图像中；文献[21]将视频的认证信息通过 QR 条形编码生成水印信息，然后结合 SVD(奇异值分解)、DWT 技术将其嵌入到视频信息中；文献[22]则是在嵌入前先对秘密信息进行 PDF147 编码，并在嵌入算法中结合了人类视觉系统(HVS)特性；文献[23]提出了一种基于二维条码 QR 码的安全复印系统，把的特点为具有信息容量大、保密防伪性能好、编码范围广、纠错能力强的 QR 码作为水印信息，实现了电子文档的权限控制、文档验证等，有效地保证了在过程中安全的传输文档。

虽然当前针对二维码的信息隐藏领域的研究正逐步展开，并得到越来越多研究者的关注。但当前的研究主要集中在以二维码为载体的水印算法方面。由于本课题是以国家自然科学基金(代号：61372175)项目为背景进行研究的，所以更侧重的是大容量的隐写术，即如何利用二维码信息量大、编码范围广、纠错能力强等优点和隐藏算法良好结合，从而提高隐藏性能方面的研究。虽然当前也有少量的以二维码为秘密信息方面的研究，但这些研究的都只是将编码后的二维码信息看成普通的二进制码流，然后按照一般信息隐藏的方法进行的信息的嵌入，实质上也并未充分考虑秘密信息是二维码时的秘密信息的一些特性。

1.3 论文主要工作及安排

信息隐藏是一种保障秘密信息在传输和存储过程中不被轻松的破坏或者是轻易的窃取，而采用的一种新型的技术，它主要研究的是如何利用多媒体数字信号本身存在的冗余以及人类感觉器官在感知上的局限性，将数字媒体文件或数字图像文件作为传输信息的载体，将秘密信息数据隐藏在一个宿主信号中而不被人所感知，以实现秘密信息隐藏的目的。经历十余年的发展和讨论研究，信息隐藏技术已经成为信息安全领域中一个重要的研究课题，在计算机、通讯、保密等领域中都有着非常广阔的应用。信息隐藏（Information Hiding）也可称为数据隐藏（Data Hiding）。

另一方面，当前制约隐写发展的一个很重要的因素就是隐写容量的问题。虽然随着研究的深入和研究者的不懈努力，近年来隐写的容量得到了较大的发展，但当要隐秘传输的高数据量的秘密信息时，会对隐写容量提出更高的要求。而二维码具有信息量大的特点，且能编码英文、图像、文字、数字等，在日常生活中得到广泛的使用。另外，二维码还具有很强的鲁棒性，在无损 33%的情况下仍能正确的提取信息，将其应用到隐藏

中可以有效的提高秘密信息抵抗攻击的能力。

因此，将信息隐藏技术与二维码技术相结合的研究具有重要的现实意义和研究价值。本课题的主要研究内容如图 1-1 所示。

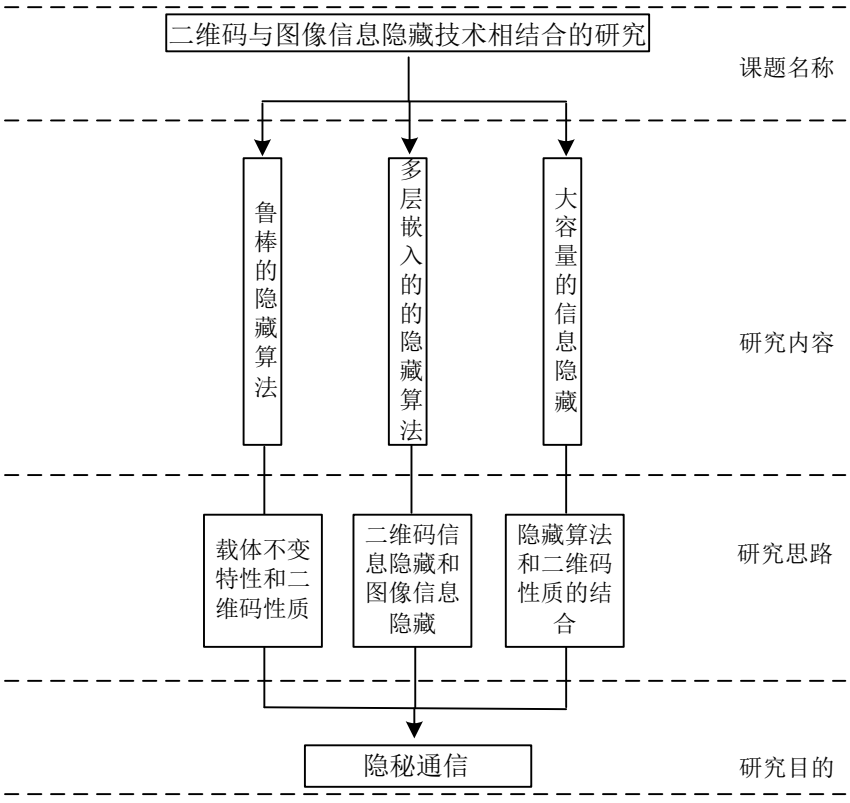


图 1.1 研究内容示意图

(1) 大容量的信息隐藏算法

主要考虑隐藏算法的大容量的问题，大容量相对的，不是绝对的。隐秘通信时隐写的容量显得至关重要， 如何提高容量成为了首要的任务。从两个角度来进行考虑：一是如何提高隐藏算法的容量；二是对秘密信息经过二维条码编码的比特流数据如何利用二维码的性质进行处理，使得嵌入同样比特数的情况下对载体的影响最小，这样有助于在相同图像质量的情况下嵌入更多的信息。

（2）多层嵌入的隐藏算法

二维码本身也可以作为载体进行秘密信息的隐藏，基于此考虑，我们可将有助于接收端二维码恢复的信息嵌入到二维码中，也可将一部分的秘密信息嵌入到二维码中作为隐藏容量的补充。该部分的设计思路如下：首先将二维码作为载体进行信息隐藏的嵌入，其中秘密信息可以是有助于接收端恢复二维码的特征信息也可以是一部分的要隐秘传输的秘密信息，最后再将含密的二维码嵌入到载体图像中。该部分的研究涉及到多层嵌入的思想和二维码与载体隐藏两者相协调的问题。目标是利用二维码作为载体的方法寻

求一种能获取更好隐藏算法性能的方法。

（3）鲁棒的隐藏算法

图像在传输、存储的过程中有时为了节约存储空间会进行有损压缩处理，另外含密图像还可能会遭受噪声、图像处理等有意或无意的攻击，这样可能会造成接收端秘密信息的无法正确提取，因此鲁棒性算法的研究也不可或缺。当前的鲁棒隐藏算法的目标都是在保证一定不可见性的情况下，尽量地减少秘密信息的误码率。但本课题由于是以国家自然科学基金(代号：61372175)为背景开展研究，关注的是接收端能恢复载体图像的质量，而不需拘泥于发送端不可见性的束缚；另外，二维码本身抗误码的能力较强。因此，该部分的研究内容主要集中在 JPEG 类算法有损压缩情况下，寻找接收端拥有更好载体质量、更大隐藏容量和更高抗压缩性的算法。

2 二维码与信息隐藏概述

2.1 二维码概述

2.1.1 二维码的基本概念

二维码[18][3]是使用特定的图形，通过在平面上不同的排列组合方式来表示信息。使用几何体的黑白颜色特征来表示数据信息，黑白巧妙地对应于计算机内部的 0,1 逻辑，在读取数据时，使用图像输入设备读取图像中的黑白块，通过分析黑白块的摆列方式来提取信息，这一步一般由计算机实现，即可自动化处理。每个黑白块字符大小不一，在不同码制下的含义不同，调整其排列方式可以得到不同程度的纠错功能。二维码技术目前已经广泛应用于现代商业活动，在电视上经常会出现商品的二维码购买链接，在大多数网站的文章结尾会有文章的地址链接，在购买的商品包装上会有商品特有的条码，在街头等位置会有公共二维码来表示此处的地理坐标，在某些证件上会有二维码表示证件信息，在火车票上会有二维码来防伪，在名片交流时还可以用二维码来传递名片信息。

2.1.2 二维码的分类

（1）堆叠式二维条码

堆叠式二维条形码(2D Stacked Code)：是多层符号(Multi-Row Symbology)的条码，是将一维条形码的高度截短，再层叠起来进行更多信息的表示资料。其编码原理为：以一维条码为基础，多行组合在一起，形成堆叠式二维条形码，由于每行是一个独立的一维条码，因此其继承了一维条码的特点，是用一维条码设备也可以识别读取。但由于行数不再是一行而是多行，需要对其行数进行判定并进行译码，其译码算法与编码解码软件也不完全相同于一维条码的算法技术。行排式二维条码主要有这几种码：PDF417、Code 16K、Code 49 等。它是一种具有高信息容量、多层、可变长度和纠正错误能力的二维条形码。它的容量为 1800 个大写字母，或 2700 左右个数字，或 500 多个汉字，或 1100 多个字节。由于其使用了 Rs 编码对其突发的差错进行校验，所以具有高容错率，并且可以选择到所需要的纠错等级。PDF417 二维条形码具有《中华人民共和国国家标准 GB/T17172 一 1997 四一七条码》规定它的基本特性的具体参数，同时规定了其尺寸要求、相关定义、符号结构以及其他的具体技术要求。

PDF417 条码编码形式属于行排式二维条码[17]。由于其组成条码的每一个字符符号是由 4 个条和 4 个空总共 17 个模块构成的，所以被称为 PDF417 条码。堆叠式二维条

码中的一个典型例子就是 PDF417 条码，示例如下图：

图 2.1 PDF417 编码的二维条形码示例

（2）矩阵式二维条码

矩阵式二维条码，简称矩阵式二维码，由于其外观像棋盘，因此又称为棋盘式二维条码。它使用黑白方块的空间分布来表示信息，一般排列为矩形。可以看做，在矩形中使用黑色方块表示二进制数字“1”，使用白色方块表示二进制数字“0”，通过空间上黑白方块的不同排列表示不通过信息。矩阵式二维码是一种基于组合编码、图像处理的新型的符号编码码制，具有的特点是可自动识别处理。最具有代表性的矩阵式的二维码有：QR Code、Code One、Data Matrix、Maxi Code 等。矩阵式二维条形码(2D Matrix Code)：矩阵式二维条形码是一种中心点到与中心点固定距离的多边形单元所组成的图形图案，用来表示信息和其它与符号相关的功能。QR code 是矩阵式二维码[3]。矩阵二维码符号是在 1994 年 9 月由日本 Denso 公司于研制成功。它是一种矩阵式编码的二维码，在矩阵相应像素元素位置上的信息由黑色方块表示二进制中的“1”,由白色方块表示二进制中的“0”，并用这些基础元素的排列组合组成代码。一个 QR 码[18]一般包括两部分，即功能图形和编码区域。QRCode 码(QuickResponseCode)(图 2.2)。

图 2.2 QRCode 编码的二维条形码

1）功能图形

功能图形包括寻像图形、定位图形、校正图形、分隔符号（如图 2.5 所示）。功能图形对于不同输入的数据和版本都保持同样的大小和形状，功能在于确定 QR 码的位置和为 QR 码的识别提供基准信息。其编码区域包括的是数据码字，纠错码字，格式信息和版本信息，具体的数值信息则随着输入数据，版本号纠错等级而变化。

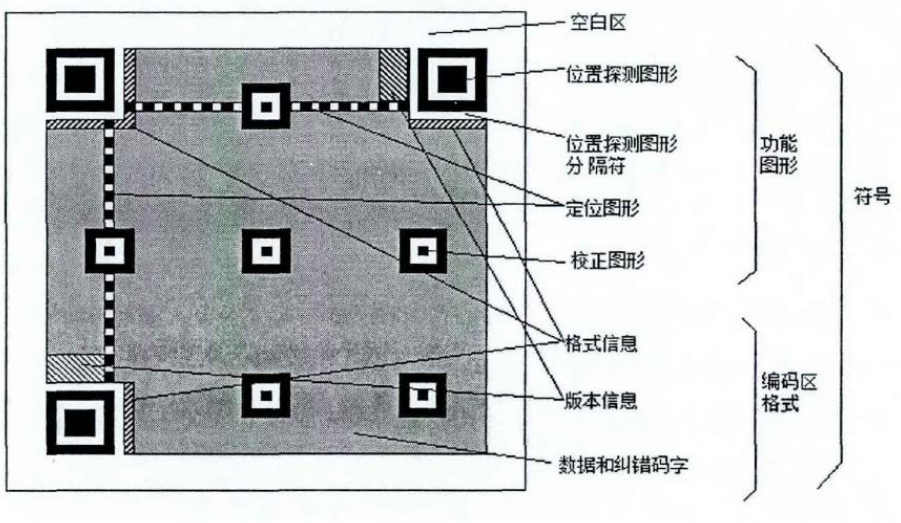


图 2.3　QRCode 编码的功能结构图

① 寻像图形

寻像图形主要用于定位二维码，具有相当明显的 QR 码特点。在二维码的左上角左下角和右上角，这三处位置一般放置位置探测图形，被用来做寻像图形使用。寻像图形的特点如图 2.4 所示，由三层嵌套的同心正方形表示，他们的大小从里往外分别是 3x3 个黑色方块、5x5 个白色方块和 7x7 个黑色方块。他们的位置分布具有相当明显的特点，在二维码图形中的其他部分出现相同特征图像的概率非常低，所以一般作为寻像图形使用，可以快速定位二维码的位置，只要定位出寻像图形，就可以准确的找到二维码位置。

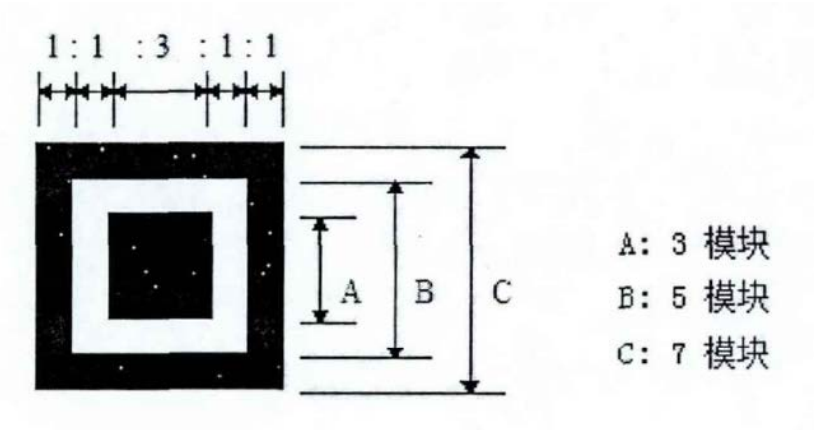


图 2.4 位置探测图形的结构

②定位图形

定位图形是由水平定位图形和垂直定位图像组成的，定位图形的宽度为一个模块的宽度，由黑白块交替形成，开始和结尾都是黑色方块，水平定位图形在二维码的左上方位置探测图形和右上方位置探测图形的中间，也就是符号的第六行。垂直定位图形则位于图形左上方位置探测图形和右下角位置探测图像之间，符号的第六行。定位图像可以表示符号的版本以及密度信息，是定位模块的基准。

③校正图形

校正图形在二维码中由 3 个同心正方形构成，中心是一个黑色模块，外侧是一个大小为 3x3 的白色模块。

④分隔符号

之前介绍过寻像图形，每个寻像图形由 3 个位置相同的位置探测图形构成，每个位置探测图形和相邻的编码区域之间有一个分隔符号，由白色模块组成的。

2）编码区域

编码区域用来表示有效信息，其中有二维码承载的信息还有纠错信息，格式信息，版本信息等。

2.1.3 二维码的特点及质量评价标准

本文主要以 QR code 为基础研究二维码与图像信息隐藏相结合。

二维码具有以下特点：

（1）编码密度高，二维码能够表示大量数据；

（2）编码范围非常广泛，可以使用二维码编码许多种类的语言文字、图片、音频、视频等信息。

（3）容错能力强，二维码本身具有纠错能力，当二维码受到污染时，由于本身具有一定的纠错能力，因此依然可以正确读取二维码表示的信息。

（4）可引入加密措施。保密性、防伪性好。

（5）译码可靠性高，由于本身具有一定的纠错能力，因此相对于一维条码，准确率比较高。

（6）条码符号形状、尺寸大小比例可变。

（7）成本非常低，易用于制作，非常持久、耐用。

（8）可以使用 CCD 阅读器或激光阅读器对二维码进行识读。

由于二维码的复杂度高于一维码，在容错方面比一维码有了很大的提升，但在实际生活与生产过程中，还要检测评鉴二维码的印制质量，常用峰值信噪比来评价。

峰值信噪比（PSNR），是一种对图像进行评价的客观标准。但它具有局限性，“Peak Signal to Noise Ratio”缩写是 PSNR。它的意思是峰值信号和噪声之比，一般情况下，经过图像压缩后，输出的图像的低频信息会受到一定影响，使用这个值即可分析出压缩前后的图像变化差距，从而量化图像品质。目前 PSNR 已经被广泛的运用在衡量算法的处理结果是否达标。它是原图像与处理后图像之间的均方误差取(2^n-1)^2 的对数值（即信号最大值的平方，n 表示每个采样值的比特数)，单位为 dB。 MATLAB 中的公式用法如下：

PSNR=10*log10((2^n-1)^2/MSE

其数学公式如图所示：

$$PSNR = 10 \times \log_{10}\left(\frac{(2^n-1)^2}{MSE}\right)$$

其中，MSE 就是原图像与处理后图像之间的均方误差。

dB 是 PSNR 的单位。一般情况下 PSNR 值越大，表示图像失真不严重。

目前 PSNR 被广泛使用在对图像画质的测量上，在一般情况下，PSNR 值越大直观看上去效果越好，PSNR 值越小直观看上去效果越差，当然，也不会总是如此。直观上看到的效果受人眼的视觉感官影响，因此直观看到的结果和图像误差并不成正比，会受到一些其他因素影响。

(1) 均方误差 MSE(Mean Square Error)

均方误差一般于统计过程，均方误差可以有效地表现统计特征，它的计算公式如下：

$$\mathrm{MSE} = \mathrm{E}\left\{\left[\mathrm{f}(\mathrm{x},\mathrm{y}) - \mathrm{f_r}(\mathrm{x},\mathrm{y})\right]^2\right\} \tag{2.1}$$

这里 $\mathrm{f}(\mathrm{x},\mathrm{y})$ 是原始数字图像的像素值，$\mathrm{f_r}(\mathrm{x},\mathrm{y})$ 是加入水印后数字图像的像素值。

(2) 信噪比 SNR（Signal-to-Noise Ratio）

信噪比是有效信号和噪声信号的功率的比值，在数字图像处理中，SNR 是衡量数字图像处理结果的重要尺度，其计算公式如下：

$$\mathrm{SNR} = 20\log_{10}\frac{\sigma}{\sqrt{\mathrm{MSE}}} \tag{2.2}$$

$$\sigma^2 = \frac{1}{\mathrm{M}\times\mathrm{N}}\sum_{\mathrm{x}=0}^{\mathrm{M}-1}\sum_{\mathrm{y}=0}^{\mathrm{N}-1}\left[\mathrm{f}(\mathrm{x},\mathrm{y}) - \overline{\mathrm{Y}}\right]^2, \quad \overline{\mathrm{Y}} = \frac{1}{\mathrm{M}\times\mathrm{N}}\sum_{\mathrm{x}=0}^{\mathrm{M}-1}\sum_{\mathrm{y}=0}^{\mathrm{N}-1}\mathrm{f_r}(\mathrm{x},\mathrm{y})$$

其中 $\bar{Y}$ 是加入水印后数字图像像素值的平均值，M，N 分别是数字图像的宽度和高度值。

(3) 峰值信噪比 PSNR（Peak Signal-to-Noise Ratio）

SNR 是测定数字图像处理质量的尺度，有计算麻烦的缺点。为了解决这个问题，在实际中，常采用峰值信噪比来衡量数字图像处理结果，其计算公式如下：

$$PSNR = 10\log_{10}\frac{A^2}{MSE} \tag{2.3}$$

在上式中，A 表示数字图像像素能取得的最大值，在大多数情况下是 255。

2.2 信息隐藏的分类及其特征

2.2.1 信息隐藏的分类

信息隐藏技术[24][12]一般分为隐密技术和水印技术。隐密技术又称为密写术，已经有了很久的历史，它是将秘密信息写在普通的载体上，写完之后，从普通的载体上无法发现其中的秘密信息，通过传输写入秘密信息后的载体即可以传输秘密信息。水印技术已经广泛使用在版权保护、操作追踪等领域，它是将具有可鉴别性的具有特殊意义的标记通过某些技术手段永久的嵌入在宿主数据中，写入这样的标记后宿主数据依然可用。

信息隐藏系统的模型如图 2.5 所示。

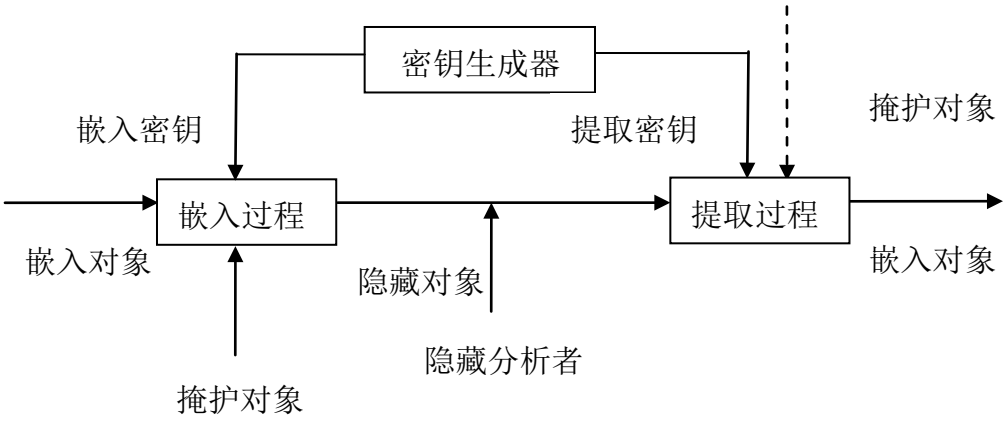


图 2.5 信息隐藏系统模型图

信息隐藏系统的模型关键名词解释：

掩护对象：掩护对象是一种公开信息，在有些地方又称载体对象或者宿主对象等。

嵌入对象：指需要通过某些方法隐藏的秘密信息。

嵌入过程：嵌入过程指的是将嵌入对象通过某些算法嵌入到掩护对象的过程，经过这个过程会生成隐藏对象。

提取过程：提取过程值得是通过某些手段将隐藏对象中的嵌入对象提取出来的过程，这里的手段与之前嵌入的手段是相对应的。

由上面的信息隐藏系统模型不难看出，我们使用嵌入密钥将嵌入对象嵌入到掩护对象汇总，完成这个嵌入过程之后会生成隐藏对象。一般来说，嵌入对象可以是文本、图像、音频或者视频。如果嵌入过程使用的嵌入信息算法比较优秀，那么嵌入之后生成的隐藏对象和原来的掩护对象几乎没有差别，仅凭人眼是无法识别出其中的变化的。隐藏对象在实际的传输过程中，可能会受到多种干扰，当然也可能会收到攻击，例如被窃听，被分析等，隐藏分析专家可以通过检测隐藏对象，发现其中的嵌入对象，提取其中的嵌入对象，甚至删除和替换其中的嵌入对象。查明嵌入对象和检测嵌入对象是被动攻击完成的，删除和替换嵌入对象是主动攻击完成的。

在提取嵌入对象过程中需要有提取密钥，通过提取密钥配合之前的嵌入算法的逆算法可以将嵌入对象提取出来。在某些情况下，提取嵌入对象的过程不需要掩护对象的参与，这样的系统称之为盲隐藏嵌入系统，反之，在提取嵌入对象的过程中需要掩护对象参与的系统称之为非盲隐藏嵌入系统。

信息隐藏技术的特点是利用载体信息的冗余性，载体信息收到轻微影响不影响其包含的信息，将秘密信息通过某些手段嵌入到载体信息里，将嵌入秘密信息的载体信息发不出去即将秘密信息发布了出去，在外界看来载体信息并没有变化，达到掩饰秘密信息存在的效果。这样的隐藏可以避免秘密信息被他人察觉，引起他人注意，有一定隐蔽性，具有较好的安全性。正是由于隐藏技术有这样的一些特点，所以目前已经被广泛使用在信息加密，秘密通信等领域，而且达到了较好的效果。

2.2.2 信息隐藏的特征

上面介绍了信息隐藏系统的结构，分析了信息隐藏技术的特点，接下来总结一下信息隐藏的一般性的特征。大体上说，信息隐藏技术具有鲁棒性，不可感知性，安全性，自身恢复性和安全性的特点。

（1）鲁棒性

鲁棒性指的是，秘密信息不会因为载体的改变而丢失的能力。这里说的改变包括信号在传输过程中由于信道噪声或被滤波、有损压缩或者重新采样、数字/模拟或模拟/数字转换等。鲁棒性在有些文献中又称为健壮性，所阐述的内容相同，即在含密载体收到常规信号处理、变形、裁剪、压缩等操作之后，隐藏在其中的秘密信息依然保持完好，

并且在一定程度上可以被准确采集到。在数字版权保护领域，对于该领域的秘密信息的攻击是不可避免的，而且在大多数情况下攻击者会主动攻击，他们会通过各种手段在破坏或者损坏被嵌入的信息，在该领域需要较高的鲁棒性来保证数字版权的完整。在有些领域鲁棒性并不是很重要，不会有鲁棒性要求，例如在真假鉴别领域的水印，在该领域，水印要求是脆弱的或者是半脆弱的，容易损坏而不能具有鲁棒性。

（2）不可感知性

不可感知性指的是通过信息隐藏算法将秘密信息写入到载体之后，载体信息的内容不会丢失，不影响载体的基本特性。另外由于人眼感官具有不敏感性，在载体经过信息隐藏算法写入数据后人眼无法察觉到其中的变化。秘密信息写入到载体之后含密载体的特征与载体写入秘密信息之前是一致的，其噪声分布一致，非法用户无法判断秘密信息是否存在。

（3）不可见性

不可见主要是对人类而言的，人类视觉系统对某些信息是不敏感的，经过信息隐藏算法处理后，含密载体没有明显的变化，而隐藏的秘密信息无法被人类直观的发现。

（4）安全性

安全性指的是，信息隐藏算法具有一定的抗攻击特性，在遭受到外界攻击是，具有一定的抵抗能力，不会丢失秘密信息。

（5）自恢复性

自恢复性指的是，含密载体经过一系列变换操作之后，可能会是载体发生较大的变化，产生很多个片段，凭借这些片段，经过一系列运算，依然可以恢复秘密信息，在恢复过程中，不需要载体信息。

上面总结了信息隐藏技术的特征。由以上分析可知信息隐藏的技术具有不可感知性、鲁棒性、自恢复性，不可见性和安全性等多个方面，并视其应用场合不同而有所不同。

2.3 典型的信息隐藏算法

近二十年以来，信息隐藏技术迅速发展，应用在多个领域，作者研究发现，有许多学者提出自己的信息隐藏算法如[24][25][26][27]，这些算法各自具有不同的特点，在目前公开的算法中，最常采用的是空域技术和变换域技术。

2.3.1 空域技术

空域技术是用秘密信息比特替换载体信息的不重要部分，从而实现对秘密信息进行隐藏的技术。在接收秘密信息时，只要知道之前在嵌入秘密信息时的嵌入规则，即可提取秘密信息。只要再写入秘密信息时改动足够小，那么攻击者是很难察觉到这样的改动

的[l]。空域技术的特点是信息隐藏容量大，具有良好的不可见性，但是鲁棒性较差。在所有空域技术中，最低有效位方法（LeastSignificant Bits）最具有代表性。该方法的原理是使用秘密信息比特位和载体比特位进行某种运算，使用运算结果代替载体原值，此方法已经有了较长时间的使用历史，相关文献很多。

人类视觉系统对外界的变化不是很灵敏，有自己的局限性，因此使用合适的算法在载体中嵌入秘密信息后，人眼看上去并没有什么变化。这样的算法例如最低有效位算法(Least Significant Bits, LSB)，它的原理是将秘密信息写在信息每个像素的最不显著位上，对载体的改变非常小，既达到信息隐藏的目的，又达到不被发现的目的。最低有效位算法是一种典型的空域隐藏算法，具有写入容量大，对载体改变小等特点，然而由于信息都写在最不显著位，所以秘密信息很容易被压缩等操作破坏。

除此之外还有一种很常用的信息隐藏算法，该算法的思路是改变图像的像素值亮度，通过调节像素点的亮度值来嵌入秘密信息，具体做法是随机选取多个像素点，其中对应的两个像素中，如果有一个点的亮度增加一位，那么另外一个点的亮度降低一位。这样的好处是整幅图片的平均亮度不会改变。通过调整参数等方法，这种算法还具有一定的抗压缩，抗图像裁剪的能力，具有一定鲁棒性。该方法的不足是，其嵌入容量很有限，对于串谋攻击抵御能力很弱。由于其具有以上特点，这种算法常用在嵌入信息量比较少的场合，例如发票信息的防伪等。另外还有伪随机书替换、将秘密信息写编码在基于调色板的图像中等多种常用信息隐藏算法。

（1）LSB 算法

LSB 的全称是英文 Least Significant Bit ，直译为中文意思是最不重要比特位，它是空域信息隐藏最常用算法之一。LSB 算法的原理是利用数字图像处理中位平面的原理，在数字图像中，改变最低位的信息对图像整体带来的影响人眼难以察觉。例如在一个深度为 8 的灰度图中，灰度值为 0 到 255，对应于二进制的八个位，最低位的加 1 对灰度值的影响是加 0 或者加 1，但是最高位加 1 对灰度值的影响很大是加 0 或者加 128。由此可见修改的位越低，对整体图像的影响越小。另外嵌入一个比特的信息会使用一个像素值，所以嵌入的信息量越大，影响的像素值越多，对图像的影响越大。正是因为如此，LSB 信息隐藏算法具有隐蔽性好，信息容量大且容易实现的特点。

LSB 信息隐藏算法的实现较为简单，本文第三章有详细阐述，这里不再赘述。传统 LSB 算法在实际嵌入信息时，考虑到对于大多数图像，最低位一般是噪声信息，没有很多的图像内容，所以最常采用的嵌入方法是序贯式嵌入和随机间隔式嵌入，应用这种嵌入方法的信息隐藏软件如 S2T00ls、EZStego、Steganos 等。

作者通过查阅文献发现，目前国内外专家学者对 LSB 隐藏和分析技术进行了很多深入研究如[27][29][30][31], 提出了很多基于传统的 LSB 隐藏算法方法的改进算法，这些算法有些已经较为成熟，例如 RPQ(the Raw Quick Pairs) 信息隐藏算法，该算法是一

种 24 位彩色图像中空域 LSB 隐藏信息的检测方法，该方法具有实现简单且计算复杂度较小的特点，该方法只适用于彩色图像，而且图像中的色彩数不超过图像总像素数目的 50%时比较可靠，当颜色数小于像素数目的 30%时可以得到较好的判别效果。另外 Fridrich 等人给出了 RS 方法(Regular and Singular groups method)。RS 方法的原理是通过统计图像中正则组和奇异组数量的变化来估计嵌入长度，适合于彩色或灰度图像，当信息非顺序嵌入时可以比较精确地估计隐藏长度。除此之外，还有 Dumitrescu 等人通过样本对分析对 LSB 隐藏信息进行检测 SPA(Sample Pair Analysis)方法，当嵌入在 LSB 上的信息的比例大于 3%时，该方法能以相当高的精度估计出隐藏信息的长度。以上这些方法都能很好的实现将秘密信息嵌入到载体中，目前隐写分析技术正在不断发展，对信息隐藏的不可见性要求越来越高，只有保证不可见性不可感知性足够高，才能有效地逃避隐写分析，这就对信息隐藏算法提出了新的要求，这也是未来一段时间内该领域的研究重点和研究难点。另外根据已有研究结论，在将秘密信息嵌入到载体之前进行加密等预处理，在不可见性不变的情况下，可以有效提高算法的安全性。

（2）最小直方图失真（LHA）算法

最小直方图失真（LHA）算法思想来源于 LSB 算法，它避免了简单的 LSB 算法中的不平衡，并尽量保持直方图不发生变化。和 LSB 算法类似，载体图像中的每一个像素都可以写入一位或者多位秘密信息。基本思想是，如果秘密信息当前比特值与载体图像当前比特值的最后一位相同，那么载体图像当前位值不变；如果上述两个值不相同，那么使用秘密信息当前比特值替换载体图像当前比特值的最后一位，得到的结果就是载体图像当前灰度值加 1 或者减 1。这种算法一定程度上提高了不可感知性。

以上着重介绍了空域两种常用的信息隐藏算法，简明扼要的介绍了 LSB 算法和 LHA 算法的基本原理，总结和分析了当前空域信息隐藏的共有特点以及现阶段所存在的问题。

2.3.2 变换域技术

变换域技术的原理是将秘密信息通过某种方法嵌入到载体信息的某一个变换域中。这里的载体信息可以是视频、音频或者图像等，其基本原理相同。在读取秘密信息时，经过反变换提取。变换域技术比空域技术的抗攻击能力强很多，而且在一定程度上具有不可觉察性。目前比较流行的变换域技术有 DCT 信息隐藏算法，DWT 信息隐藏算法等，他们都具有较好的不可见性以及较强的鲁棒性，目前应用很广泛。

简单理解：空域技术可以通过控制某些位来实现，频域技术可以通过修改频域信息来实现。

例如在空域中有信息是 10101010，对于这个信息，他的偶数位并没有用，只用他的奇数位就可以表达该信息，那我们可以用他的偶数为来实现信息隐藏，比如秘密信息

1101 可以分别放到第 2、4、6、8 位上，这样别人无法判断，但是相关人员可以根据解密规则得到秘密信息 1101 ，如果这个信息通过频域技术来实现信息隐藏，那么只有知道了信息隐藏算法，才可以根据其反变换取到原始的秘密信息，第二种相应技术的复杂性和技术性都更高。

在使用变换域方法实现信息隐藏时，首先将载体信息通过一定的变换方法变换到频域，然后根据低频信息的改动容易被人类感知，高频信息容易被干扰和破换的原理，将秘密信息通过一定的规则写在频域的中频部分，来实现秘密信息隐藏。目前研究方向主要是基于离散余弦变换（DCT）[28]的信息隐藏，基于小波域的信息隐藏[29-31]以及基于其它正交域的信息隐藏等，还有人将信息隐藏和数据压缩放在一起，实现压缩域内的信息隐藏。

（1）DCT 算法

离散余弦变换的原理是，使用傅里叶变换的对称性，对图像边界进行褶翻操作，得到图像的偶函数形式，然后对这个偶函数进行二次离散傅里叶变换，得到的结果中只有余弦项，因此称之为离散余弦变换，英文简称 DCT 变换。它是一个实数域的变换。

在使用 DCT 信息隐藏算法[32] [33]嵌入载体后，从载体图像中提取秘密信息时，需要计算 DCT 变换系数，使用嵌入算法的逆操作提取。在经过 DCT 变换图像中，左上角部分是低频系数，右下角部分是高频系数，中间部分是中频系数，高频部分代表图像中快速变化的部分，例如边缘信息等细节，高频部分中存在很多噪声，这些信息在进行压缩操作或者滤波操作时容易损失或者变化，图像中的中频部分存在图像的大部分可视信息，对人类来说是最重要的部分。大多数信息隐藏算法都会尽量保留图像的中频部分，不对其进行更改，另外对于低频部分的更改也会导致图像可视信息的严重干扰，因此中高频部分是信息隐藏的理想区域。在这里进行信息隐藏，既不会引起图像可视部分的变化，又不会被轻易干扰。在数字水印领域，对于这方面的研究也很多，例如著名的 Cox 算法，该算法的特点是将秘密信息写入到 DCT 域中，作者的主要贡献是提出了“鲁棒性数字信息应嵌入到图像中视觉感知最重要的部分以提高其鲁棒性”的重要观点。另外国内外学者还提出很多频域的改进算法，例如自适应的 DCT 算法[34]等，以及 DCT 域其它算法 [35~39]。

（2）DWT 算法

DWT（Discrete Wavelet Transform）中文称之为离散小波变换，最早使用在数值分析，由于其具有很多独特的优势，目前已经被广泛的应用在了信息隐藏等领域。离散小波变换使用在数字图像处理领域的基本思路是，对图像进行多分辨率分解，每经过一级小波变换会得到四个子图，如图 2.6 所示。得到的这些子图分别是：低频部分的逼近子图 LL1、水平方向细节子图 HL1、垂直方向细节子图 LH1 以及对角线方向的细节子图 HH1 。通过第一级小波变换得到的低频部分的逼近子图 LL1 还可以继续进行小波

分解，得到第二级的四个子图，以此类推。

图 2.6 图像三级小波分解图

基于离散小波变换的信息隐藏算法一般步骤如下：

第一步：利用多级离散小波变换对载体图像进行变换，从而得到不同分辨率下的细节子图以及逼近子图；

第二步：根据一定的标准，选取某个子图(例如上图中，可以是 LH2,HL2 等)，通过变换函数 h 将秘密信息 m 嵌入：

$$f' = h(f, m, \beta)$$

上式中 f 和 f ′ 分别表示的是，秘密信息嵌入前和秘密信息嵌入后相应的小波系数，β 表示嵌入强度。假设这里嵌入的秘密信息是图像信息，则先将图像进行一级小波分解再嵌入秘密信息；

第三步：将含密图像进行小波反变换，即可完成隐藏过程。

在提取秘密信息时，首先对载体图像和隐蔽图像进行相应级别的离散小波变换，得到其不同的分辨率子图，通过上一步的公式进行逆变换操作，从而还原隐藏的信息 m。如果秘密信息是图像，那么完成这一步操作之后，还要进行小波重构，才能还原图像信息。

通过以上分析，我们不难总结出离散小波变换与 DCT 变换 以及 DFT 变换，有自己的独特的优势：

优势一：离散小波变换具有良好的时间频率局部性。小波变换可以保留图像信号的局部性，如局部纹理信息、亮度信息等，这些信息对于图像分析和处理非常关键，一旦丢失，就导致马赛克效应，影响视觉效果。小波变换很好的解决了这一问题。

优势二：离散小波变换具有多尺度变换。通过第一级的离散小波变换得到的结果还可以继续进行离散小波变换，重复多次进行离散小波变换即可得到多尺度的变换结果。

优势三：离散小波变换计算复杂度小。从全局变换的角度来看，图像尺寸较大时，利用离散小波变换 DWT 的复杂度为要优于 DCT。

离散小波技术还广泛应用在多个领域，例如 MPEG-4 和 JPEG2000 压缩标准就是

以离散小波变换作为其核心技术，正因为这样，因而它进行此类有损压缩之后具有很好的鲁棒性。小波多分辨分析可以更好地控制秘密信息在载体图像中的分布，调和了鲁棒性和不可见性。

通过以上的分析，我们不难总结出频域与与空域算法相比较，变换域的算法具有如下共同特点：

特点一：通过变换域进行秘密信息隐藏，秘密信息的能量会散布到空间域的所有像素，提升了算法的不可见性，而且具有一定抗攻击能力；

特点二：通过变换域进行秘密信息隐藏，可以利用人类视觉系统的频率掩蔽效应，进一步提升算法不可见性；

特点三：通过变换域进行秘密信息隐藏可与国际数据压缩标准兼容，实现压缩域内的信息隐藏算法可以有效抵抗相应的有损压缩；

特点四：通过变换域进行秘密信息隐藏，其隐藏容量一般都很小，不易于盲提取，难以应用在隐蔽通信，可以应用于数字水印。

由于小波域具有其特有的优势，对这方面的研究也越来越多。利用小波多分辨分析能够对宿主图像中的水印分布进行良好的控制，很优秀的解决鲁棒性和不可见性之间的相互制约。另外 Kundur 提出一种基于小波融合的水印嵌入方法，这种算法是对不同分辨率级别下的水印图像和载体图像的小波系数进行求和。为了保证嵌入秘密信息后的载体图像不被发现，引入了对人类视觉系统的考虑，使用小波系数进行水印嵌入，对算法性能有了有效的提升，这种数字水印算法具有很好的效果。

2.4 信息隐藏系统的评价方法

信息隐藏系统的主要评价指标是鲁棒性，不可感知性以及信息隐藏容量。在目前情况下，暂时还没有一个统一的评价标准或者评价体系。其中鲁棒性主要通过实验来验证其有效性，很少有研究人员从理论上证明鲁棒性，因此评价不够客观和标准。一般情况下使用峰值信噪比或者信噪比来度量系统的失真情况，由于它们都会受到其他因素影响，因此由峰值信噪比或者信噪比来度量系统失真程度是否准确还存在争议。使用人类主观的感知来评价也缺少标准，同样会受到多种因素影响，因此也没有一个完善的评价模型。很多文献从不同角度对信息隐藏的特点进行过描述，信息隐藏的主要技术指标有：不可察觉性、鲁棒性、隐藏容量。下面具体描述每种指标：

不可察觉性（Imperceptibility）：不可感知性又称为不可见性，在有些文献中也称为不可感知性。不可觉察性表示秘密信息嵌入载体之后，载体的变化，不易被察觉，这里的变化包括主管质量以及统计规律。对于非法用户来说，如果载体是图像，那么修改结果应该不易被人类视觉系统发现，如果载体是音频，那么修改结果应该不易被人类听觉系统所发现，当然这里的非法用户如果是其他系统的话，对应于其系统不可检测到嵌

入在载体中的秘密信息。具有不可觉察性，才能够有效地保证含密信息在各种网络中传输而不被发现。目前，学术界普遍采用峰值信噪比（PSNR）从数量上表达秘密信息嵌入后的不可见性指标。尽管对此很有争议，但很多学者仍采用峰值信噪比来衡量不可见性，为了量化表示不可见性，本文也采用峰值信噪比来定量表示不可见性。令 A 是嵌入前的灰度图像，S 是含密图像，M、N 分别是 A 的行数和列数，则嵌入后的峰值信噪比计算公式如下。

一般地，秘密信息嵌入后的不可见性约在 20dB-40dB 之间。

鲁棒性（Robustness）：鲁棒性表示信息隐藏算法具有一定的稳定性，在含密信息收到一定攻击和非法探测后，依然可以完整的还原秘密信息。在信息传输过程中的鲁棒性指的是数字信息经过网络传输后，虽然信号发生了失真或者丢失，但是依然可以恢复秘密信息，并且错误率很低，恢复的秘密信息完整、可靠。上面所说的攻击包括数字/模拟和模拟/数字转换，低通滤波器滤波，图像旋转位移等操作，以及对图像进行压缩、重新编码等。

隐藏容量（Capacity）：隐藏容量表示信息隐藏算法在满足之前不可觉察性的前提下，在数字载体中可以写入的秘密信息的最大比特数。我们之前了解的数字水印技术对隐藏容量没有特别的要求，但是在通信系统等方面需要隐藏容量越大越好。

对于一般的信息隐藏算法，以上三个特性难以同时满足，隐藏容量与不可觉察性和鲁棒性之间相互制约，如果信息隐藏算法的隐藏容量较高，那么不可觉察性或者鲁棒性就会较差，不同的信息隐藏算法具有不同的特点，具体使用那种信息隐藏算法还要看具体的应用环境，根据实际情况实际需求选择最合适的信息隐藏算法。

2.5 图像压缩理论概述

本文的最后使用了图像压缩来检验算法的抗压缩性能，因此在这里简要介绍图像压缩理论以及标准。常见的图像压缩标准有 JPEG 和 JPEG2000，图像压缩方法一般由预测编码方法，正交变换编码和金字塔编码等。接下来我们详细了解 JPEG 和 JPEG2000 图像压缩标准。

2.5.1 JPEG 图像压缩标准

JPEG(Joint Picture Expert Group)是联合图像专家组(JPEG)的缩写，该专家组是由国际电报电话咨询委员会(CCTIT) 和国际标准化组织(ISO)管理的。JPEG 标准的而出现是为了解决连续色调图像的压缩问题。通过这个压缩方法，可以保证一定图像质量的情况下有一个较大的压缩比，正是因为这样的特性，JPEG 压缩方法是目前广泛应用的压缩技术。JPEG 压缩最常用的模式是基线系统(Baseline)，即基于 DCT 变换的顺序型模式。

在对数字图像进行 DCT 变换操作之后，得到的频域图像的左上角对应于数字图像

中的低频分量，右下角对应于数字图像中的高频分量(DCT 变换又可看做空域低通滤波器)。在数字图像中低频分量包含了图像中的大多数重要信息，例如亮度信息等，高频信息主要是图像中的图形边缘等，另外还有噪声信息。低频信息和高频信息相比，低频信息明显更重要，去掉一定的高频信息可以达到压缩目的，同时图像质量会有所下降，但是不会下降很多。在这里一般采取量化操作，根据制定的量化表采用一定规则可以保持低频分量抑制高频分量，从而达到压缩的目的。

2.5.2 JPEG2000 图像压缩标准

2000 年 12 月公布的 JPEG 2000[40]标准，是对 JPEG 标准的更新换代。JPEG2000 标准是为了适应低带宽、高噪声的环境以及为了满足数字图书馆、医疗图像、因特网上服务的需求而制定的。JPEG 2000 比 JPEG 优越，它不再采用 DCT 算法，改用以离散小波变换（DWT）算法为主的多分辨率编码方法。JPEG2000 是基于小波变换的图像压缩标准，主要工具是小波变换，将图像由时域空间变换到频域空间，从而实现压缩。最后进行量化编码，得到压缩后的数据。算法框图如图 2.7 所示：

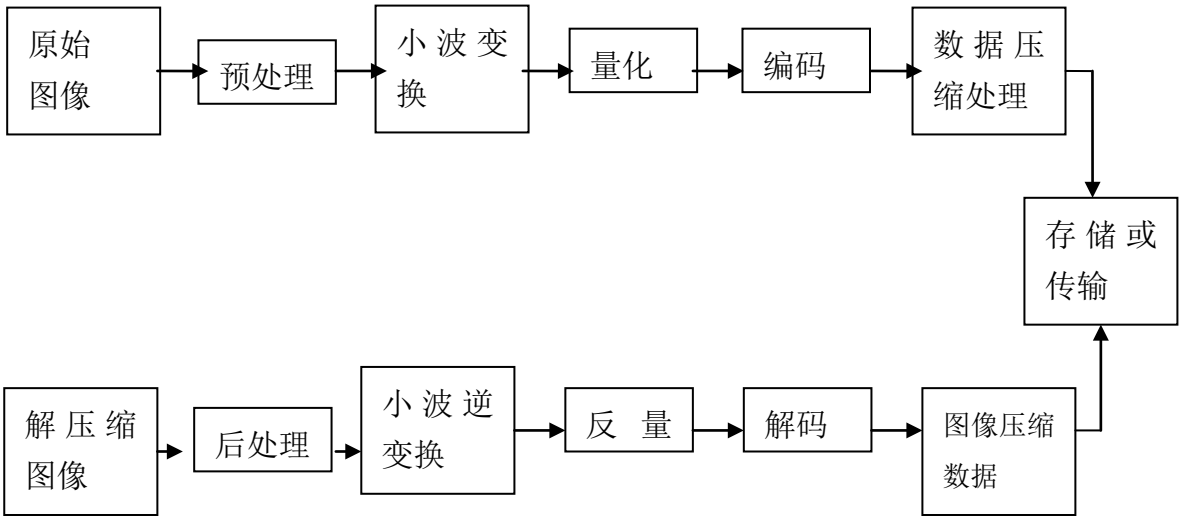


图 2.7JPEG2000 编解码系统的算法框图

JPEG2000 标准[40]采用小波变换编码。DCT 等算法在大多数情况下处理结果达不到 JPEG2000 的效果，正是由于采用了小波变换进行变换编码，所以 JPEG2000 的压缩效率较高，JPEG2000 在对图像进行压缩时，会对每一个网格分别进行离散小波变换，得到一个和原图大小一样的小波系数图。JPEG2000 进行小波变换的步骤是：首先使用高通滤波器和低通滤波器对图像的水平方向和垂直方向进行卷积操作，得到的 4 块图像，

每块图面积为原图的 1/4。他们是水平和垂直方向的低频图 (LL)、水平和垂直方向高频图(LH)、水平和垂直方向低频图(HL)、水平和垂直方向高频图(HH)。后三个称为细节子图，第一个称为低分辨率子图，这里得到的结果是图像进行一级小波分解后的处理结果；紧接着对水平和垂直方向的低频图再使用上述同样的运算进行运算，处理得到图像的二级小波分解图和三级小波分解图。在进行解码操作时，假设仅仅合成了水平和垂直方向的低频图子带的信号，得到的图像具有普通分辨率。假设合成了上面 4 个子频段的信号，得到的图像具有高分辨率。

以上介绍了 JPEG 使用小波变换的基本原理，在掌握原理后，我们在网络中进行图像传输时，可以首先从发送端发送水平和垂直方向的低频子带信号图，接收端在接收到这个信号之后开始进行解码操作，从而得到低分辨率图，与此同时，发送端选择性的将剩余的水平和垂直方向高频、水平和垂直方向低频、水平和垂直方向高频进行分级发送，用户得到低分辨率图像后，可以根据需要，选择是否加载高分辨率的图像，这样既降低了传输时的带宽消耗，减少了不必要的数据传输，又提升了用户体验。下面展示一个进行小波变换的例子，处理过程不是本文研究重点，这里仅仅展示结果，结果如图 2.8 所示（小波系数规范到 0～255 之间）。

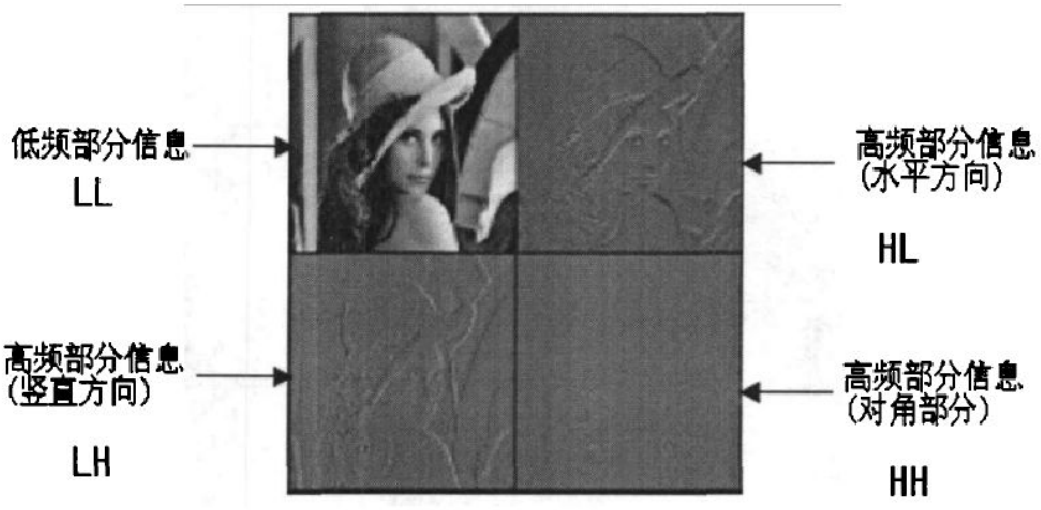


图 2.8 图像的一次小波分解

图 2.8 中的 LL，HL，HL，HH 含义在之前已经介绍，这里不再赘述。根据图 2.8 不难发现对 LL 继续进行小波分解，可以得到另一组结果，如此多次可得到多级小波分解结果。完成多级小波变换之后，还会进行 EBCOT 编码等步骤，可以实现调节分辨率等功能，这个已经超出本文研究范围，这里不再进行后续讨论。

3 二维码的空域信息隐藏算法

3.1 引言

空域也称时空域，不对信号作任何频率变换而得到的信号域就是时空域。数字图像信息隐藏算法主要分为空域信息隐藏算法和变换域信息隐藏算法[42]。空域法是修改图像的像素值，将秘密信息通过某些方法使用图像像素值来表示，常见的方法有 LSB 方法、纹理块映射编码方法、Patchwork 方法等。在大多数情况下，空间域算法容易编码实现，且嵌入容量大，程序效率高，但鲁棒性较差，易受到压缩等攻击。本章通过分析传统 LSB 算法，分析图像压缩前后变化，提出一种空域新算法，并对这个新算法进行分析。

3.2 空域 LSB 信息隐藏算法

3.2.1 LSB 嵌入算法的实现

LSB（LeastSignificantBits）算法，又称最不显著位算法是时域/空域的典型算法之一。该算法核心是使用秘密信息替换载体图像的最低二进制位完成信息嵌入，通过读取载体图像最低二进制位，即可提取秘密信息。该算法对图像的最低位进行了改动，而图像的最低位平面具有类噪声特性，人类视觉系统对此不敏感。这种算法具有简单、嵌入数据量大、对图像信息改动小等特点，广泛应用在图像隐写术中。对于一般的 RGB 图像，每个颜色分量对应于计算机中的一个字节，载体图像可以抽象为字节流，秘密信息可转换为 0,1 二进制比特流。

设载体图像字节流为：

$$C = B_1 B_2 B_3 \cdots B_n, B_i = b_{i1} b_{i2} \cdots b_{i8}, i = 1,2,\cdots n$$

待嵌入的秘密信息比特流为

$$M = m_1, m_2, \cdots, m_l$$

式中：$b_{ij}, m_k \in \{0,1\}$。

LSB 算法从载体图片字节流的每个字节中选择嵌入位，用 m_k 来替换约定位置上的 b_{i8}，嵌入后生成的含密图像表示为 $C' = B_1' B_2' \cdots B_n'$，

假设将秘密信息嵌入到 RGB 通道的 BMP 位图中，位图的长为 m 像素，宽为 n 像

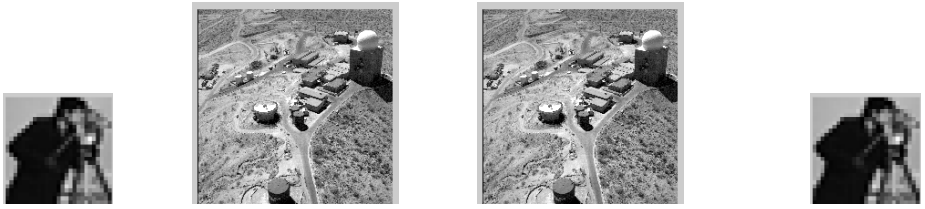
素，在每一个颜色通道中都可以写入一个二进制数，即在 RGB 通道的 BMP 位图中可嵌入的秘密信息的容量是 m*n*3/8 字节。同理对于灰度图像，假设该图长为 m 像素，宽为 n 像素，该图中可嵌入的秘密信息的容量是 m*n*1/8 字节。

使用典型的 LSB 算法进行嵌入时，对于 RGB 通道的 BMP 位图，可以分别操作 R、G、B 三个通道。每个通道的每个像素之间都是独立的，每个像素都可转换为一个 8 位 的二进制组，例如该像素值是 139，转换结果是 10001011，假设要写入的秘密信息是 0，那么根据 LSB 算法，该像素值被修改为 10001010，对应像素值是 138，用这个像素值替换载体图像对应位置的原始值，即完成了一位秘密信息的嵌入。这样对图片像素值的改动很小，最不显著，嵌入的秘密信息是不可见的。但是，图像的最低位往往容易被压缩、滤波等操作影响，另外通过这样的变化操作，会使图像的最低平面 0,1 分布产生较明显的变化，留下嵌入痕迹，易被统计分析，破译秘密信息。因此该算法鲁棒性差，易被滤波、压缩等操作破坏。

3.2.2 LSB 嵌入算法的仿真实验

通过分析 LSB 算法原理，本文作者利用 MATLAB 实现了 LSB 算法，该算法可以将目标图像直接嵌入到载体图像中。

按照最基本算法原理，对此算法进行仿真。利用传统 LSB 将目标图像直接嵌入到载体图像中，将秘密信息以二进制形式读取，然后依次写入到载体图像对应像素的最低位。实验结果如图 3-1 所示。从左到右依次是，目标图像，载体图像和嵌入目标图像的载体图像，最后是提取出来的目标图像，载体图像前后的 PSNR 为 49.9dB,图像直观看上去没有变化。目标图像前后对比发现完全相同，即理想状态下目标图像提取出来和原图应该是相同的。



(a)秘密信息　(b)载体图像　(c)含密图像　(d)提取的秘密信息

图 3.1 LSB 算法的信息隐藏

3.3 基于二维码的 LSB 新算法

3.3.1 二维码生成

互联网有大量二维码生成软件，大多数生成软件只能将文本转换为二维码，一般只支持 300 个字符。由于本文需要研究利用图像生成二维码，目前的二维码生成软件不能满足需求，因此根据网络开源项目 zxing，结合 base64 技术设计了自己的二维码生成软件，可以将图片或文字转换成二维码。

zxing 是一个开源 java 项目，可以编码和解码多种类型的条形码，支持格式包括 UPC-A，UPC-E，EAN-8，EAN-13，QR code 等，支持多种平台。目前已经广泛使用。

Base64 是一种常见的网络传输编码方式，它使用 64 个可打印字符来表示二进制数据，编码后的信息难以直接发现，并且易于加密和解密，适用范围很广。

以下是二维码生成软件的生成效果：

（1）二维码内容：

Xi`an University of Science and Technology

生成二维码图像：

图 3.2 二维码 1

（2）二维码内容：

At the beginning of the new semester, every student is required to register with the department. In the case of failure to register, he has go to department to go through the formalities for leave, and those absent for two weeks without asking for leave are thought to drop out.

生成二维码图像：

图 3.3 二维码 2

（3）二维码内容：

Xi’an University of Science and Technology lies in Xi’an, a world-famous city with numerous ancient and historical sites and remains. Its head campus stands blocks away from the Big Wild Goose Pagoda well known at home and abroad and its newly built Lintong campus close to another popular tourist resort Huaqing Hot Springs. Shaanxi provincial CPC Committee and Shaanxi provincial government and the Xi’an municipal government officially recognize the university as the Model University and Garden Campus respectively.

生成二维码图像：

图 3.4 二维码 3

（4）二维码内容：

图 3.5 秘密信息

生成二维码图像：

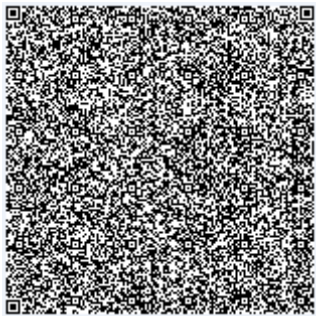


图 3.6 二维码 4

3.3.2 二维码转换为灰度图

根据二维码特性，二维码的信息由黑和白来表示，相当于 0 和 1。大多数二维码生成软件生成的二维码结果都是二值图像，直接对其使用 LSB 等算法的效果不佳，因此本文提出，将二维码编码为灰度图，利用二维码编码后的灰度图来进行后续信息嵌入步骤。二维码编码为灰度图原理如图 3.5 所示。

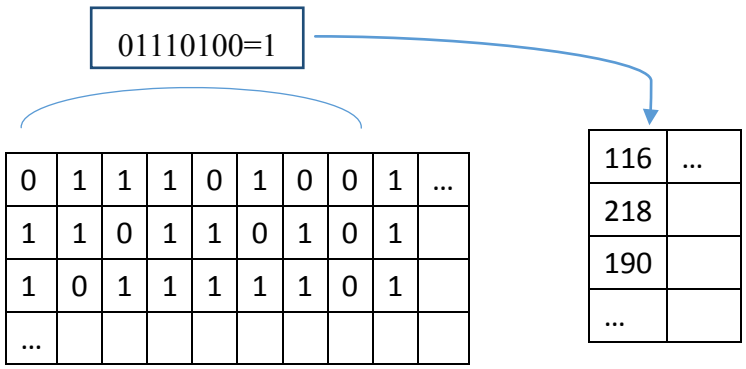


图 3.7 二维码编码为灰度图

二维码转换为灰度图的步骤如下：

(1)从二维码图像(1,1)位置开始，依次取出八个连续的像素值；

(2)将取出来的连续的八个有效像素值，根据其值转换为由 0 和 1 组成的八位二进制数；

(3)将这八位二进制数转换为一个 0~255 之间的值作为灰度图的像素值，写到灰度图对应位置。

(4)如果还有值，继续执行步骤(1)。

这里将上面刚刚生成的四个二维码转换为灰度图，转换结果如图 3.8 到 3.11 所示。

二维码 1 及其编码后的灰度图如图 3.8 所示。

(a)二维码　　(b)灰度图

图 3.8 二维码 1 及其灰度图

二维码 2 及其编码后的灰度图如图 3.9 所示。

(a)二维码　　(b)灰度图

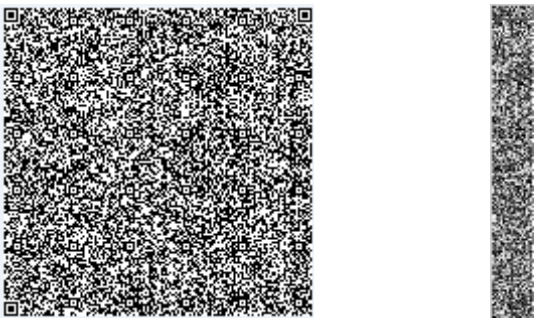
图 3.9 二维码 2 及其灰度图

二维码 3 及其编码后的灰度图如图 3.10 所示。

(a)二维码　　(b)灰度图

图 3.10 二维码 3 及其灰度图

二维码 4 及其编码后的灰度图如图 3.11 所示。



(a)二维码　　(b)灰度图

图 3.11 二维码 4 及其灰度图

根据以上二维码编码为灰度图的结果不难发现，生成的灰度图大小为编码前二维码大小的 1/8，同样大小的二维码图片，写入信息量越大，生成的二维码越复杂，每个黑白块所占的像素值越小。另外编码后的灰度图直观上没有明显的二维码特征。

3.3.3 二维码和 LSB 相结合的新算法

二维码具有容错能力强的特点，LSB 具有容量大、对载体图像影响小等特点，本文提出将二维码与 LSB 相结合，利用二维码为载体，将秘密信息写入二维码。考虑到充分利用二维码的容错能力强的特点，我们将 LSB 算法进行改进，将秘密信息写在二维码编码后的灰度图的高位。本文提出的新算法框图如图 3.12 所示。

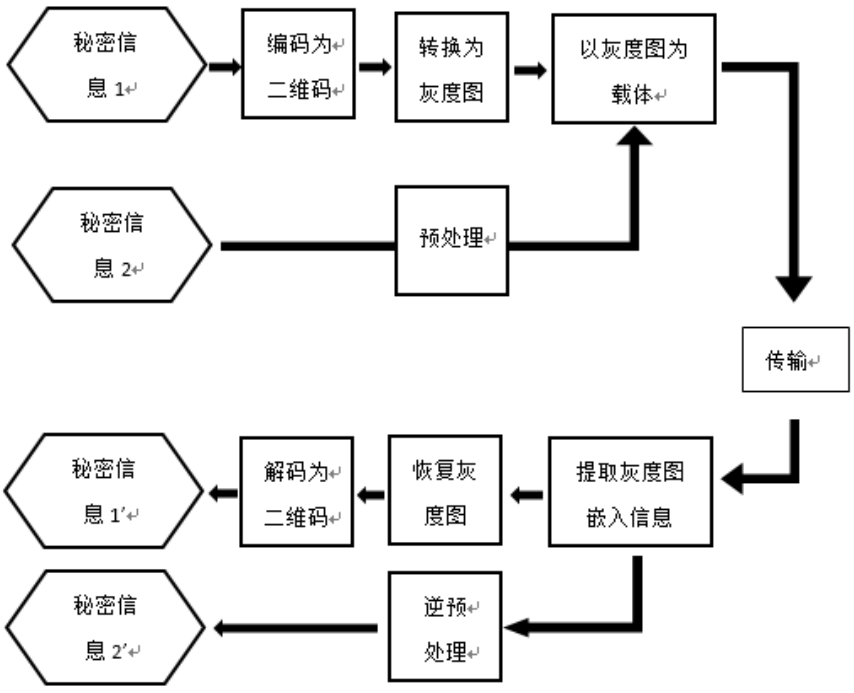


图 3.12 二维码与 LSB 结合的算法

新算法各主要步骤介绍如下：

编码为二维码：这一步主要实现将秘密信息 1 编码为二维码。二维码具有编码范围广等特点，因此这里的秘密信息不仅仅可以是文本，还可以是图片，音频，视频的信息。一般的编码软件是将文本编码为二维码，长度一般不超过 300 个字符，对本文来说远远不够，在本文中，作者使用 Base64 技术实现将图片编码为字符，然后借用开源框架 zxing 生成二维码图片，实现将秘密信息编码为二维码，编码字符长度大约 2100 个字符。

转换为灰度图：这一步主要实现将上一步生成的二维码编码为灰度图。上一步生成的二维码尺寸较大，而且是一个二值图，对这样的二值图直接使用 LSB 等算法效果很差，如果将这个二值图扩张为灰度图，那将会导致二维码图片大小变得很大，在传输过程中会浪费一定的带宽。因此在本文方法中，提出将二维码编码为灰度图，具体编码方式已经介绍，这里不再赘述。

预处理：这一步主要实现对秘密信息 2 的处理，秘密信息 2 可能是文本、音频、视频等。在本章开始介绍过 LSB 算法的缺点，其中提到过该算法会在最低有效位平面留下嵌入痕迹。在这里将秘密信息 2 进行置乱，变换等操作，将原始信息打乱，让其看上去像是背景噪声，可以提高算法的保密性。因为在本文课题背景的实际应用情景下不需要对信息进行加密，所以在本文中不对这种情况进行研究。

以灰度图为载体：这一步利用改进的 LSB 算法将秘密信息 2 写入到灰度图中。这一步实现了以二维码为载体的信息嵌入。这一步充分考虑二维码编码为灰度图之后灰度图的特性，将秘密信息写在灰度图的最高有效位与写在灰度图的最低有效位对二维码来说，都是变化了一个像素点，但是把秘密信息写在最高有效位能够明显提升算法的抗压缩能力。因此在本文算法中将有效信息写在灰度图的高位来嵌入有效信息。

传输：这一步表示含密图像在不同网络下的传输。本文研究课题的背景是在卫星信道中，但是本文算法不仅限于此，对本文算法来说这里的传输可能是在互联网中传输，或者是某些专门的特殊网络中。

提取灰度图嵌入信息：这一步发生在传输完成之后，在信息接收端收到含密图像之后，首先进行高位信息提取，提取出嵌入在灰度图中的信息。提取完成之后，无需对灰度图进行处理。提取完后提取出来的秘密信息进行逆预处理，含密灰度图进行恢复灰度图处理。

逆预处理： 这一步和之前的预处理相对应，将提取出来的秘密信息进行还原。如果之前进行了置换等操作，在这里进行反变换以还原秘密信息 2。由于时间关系，本文中暂未对其进行仿真。

恢复灰度图：这一步是恢复灰度图为二维码。经过提取灰度图嵌入信息后，将灰度图转换为二维码，由于之前已经在二维码图像中写入了秘密信息，因此灰度图质量受到一定影响，产生了一些噪声，转换为的二维码也产生了对应的噪声，不过这些噪声不影

响灰度图转换为二维码图片。

解码为二维码：这一步是将二维码解码，获得秘密信息。由于之前写入了秘密信息，因此二维码受到了影响，这里解码二维码利用到了二维码的容错特性，在一定情况下，二维码中的秘密信息可以完全恢复。

以上详细介绍了本文提出的二维码与 LSB 结合的新算法的各个关键环节，及其所涉及技术。通过这些介绍将本文提出的基于二维码的 LSB 新算法完整的呈现给读者。

3.4 新算法的具体实现

3.4.1 新算法具体实现步骤

本文基于以上研究结果提出了自己的基于二维码的信息隐藏算法，在具体实现过程中，为了保证新算法具有一定的抗压缩能力，根据之前分析，我们在以灰度图为载体嵌入信息时使用了最高有效位，即将有效信息写在最高位。

具体算法步骤如下：

（1）读入秘密信息 1，并将其编码为二维码。

（2）将二维码图像编码为灰度图像。

（3）读入秘密信息 2，将其进行预处理。

（4）以灰度图像为载体，将处理后的秘密信息 2 写入灰度图像最高有效位。

（5）灰度图像成为含密图像。

含密灰度图像此时可能通过多种方法传输，传输完成后进行以下信息提取算法：

（1）接收含密灰度图像。

（2）从含密灰度图像中提取秘密信息 2。

（3）将秘密信息 2 逆预处理，还原秘密信息 2。

（4）将含密灰度图还原为二维码图像。

（5）将二维码图像解码，还原秘密信息 1。

3.4.2 新算法的关键代码

以上介绍了算法的关键环节，以及文字描述，在本文中，作者使用 matlab 工具来仿真，现在介绍算法关键步骤的 matlab 实现代码。

图片转换为信息流关键代码如下。

分解图像中的数据：

```
for i=1:imagey
    for j=1:imagex
        tdata=strcat(tdata,num2str(dec2base(T(i,j),2,8)));
```

```
    end;
end;
```

解析读取出来的秘密信息：

```
for i=1:8:lsblen
    %以 8 位为单位取出数据
    for j=0:7
        tempforpixresult = bin2dec(strcat(tempforpix,num2str(tdataread(i+j))));
    end;
    tempforpix='';
    k=((i-1)/8)+1;
    decodey=ceil(k/width);
    decodex=k-(decodey-1)*width;
    QR2(decodey, decodex)=tempforpixresult;
end;
```

改进的 LSB 算法的关键代码如下。

嵌入：

```
for f2=1:n
    for f1=1:m
        xkdpixbin=dec2base(D_target_pic(f1,f2),2,8);
        if tdata(p)=='1'
            xkdpixbin(1)='1';
        else
            xkdpixbin(1)='0';
        end
        D_target_pic(f1,f2)=bin2dec(xkdpixbin);
        if p==lsblen;
            break;
        end
        p=p+1;
    end
end
```

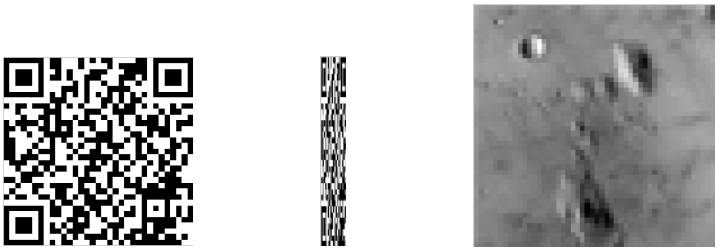
```
读取：
for f2=1:n
    for f1=1:m
        %取得当前像素值的八位二进制数的最高位
        xkdpixreadbin=dec2base(LsbRead(f1,f2),2,8);
        if xkdpixreadbin(1)=='1'
            tdataread=strcat(tdataread,'1');
            %fwrite(ffr,1,'ubit1');
        else
            tdataread=strcat(tdataread,'0');
            %fwrite(ffr,0,'ubit1');
        end
        if p==lsblen;
            break;
        end
        p=p+1;
    end;
end;
```

3.4.3 新算法的仿真实验

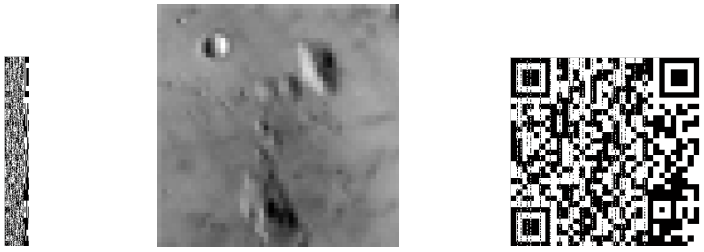
以上介绍了本文算法的结构图、关键步骤以及关键的几段代码。本文作者对本文算法实验的结果及讨论如下。实验中所用的秘密信息图片均来源于标准图像库。

实验一：

在本实验中，使用的本文作为秘密信息 1，用以生成二维码。假设秘密信息 1 为：Xi`an University of Science and Technology. 实验结果如图 3.13 和 3.14 所示。

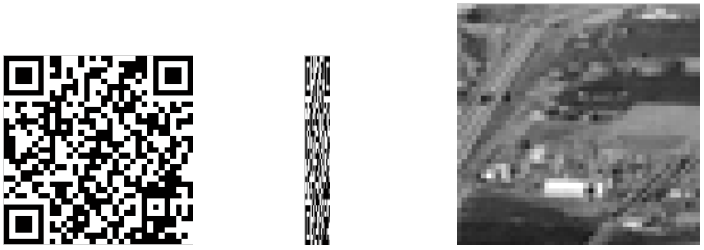


(a) 二维码　　(b) 灰度图　　(c) 秘密信息

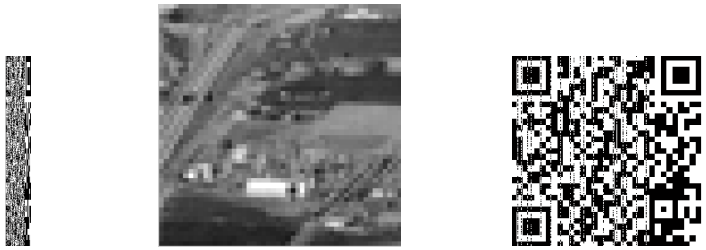


(d)含密灰度图　　(e)提取的秘密信息　　(f)还原的二维码

图 3.13 基于二维码的 LSB 新算法实验结果 1



(a)二维码　　(b)灰度图　　(c)秘密信息



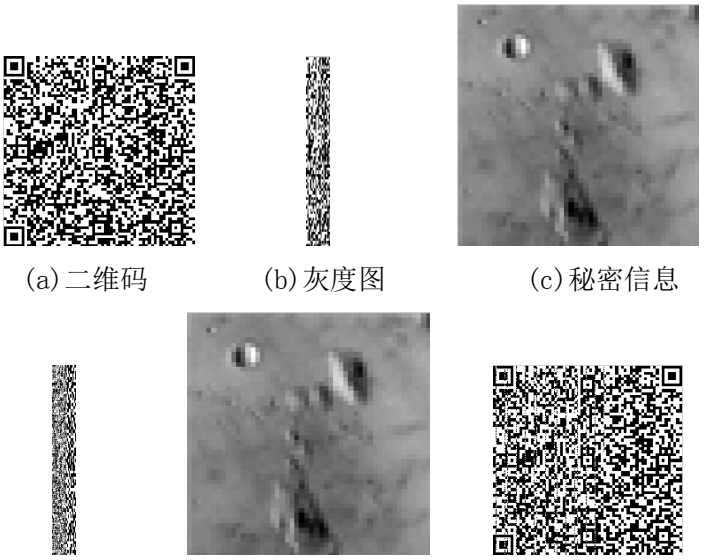
(d)含密灰度图　　(e)提取的秘密信息　　(f)还原的二维码

图 3.14 基于二维码的 LSB 新算法实验结果 2

实验结果表明，利用本文算法将秘密信息写入灰度图之后，灰度图出现了较为明显的变化，但是提取出来的秘密信息完整，还原的二维码虽然受到一定影响，出现了了很多噪声线条，但是这个并不影响二维码的解码，在新算法实验结果 1 和 2 中，还原的二维码都可以正确读取二维码的内容。

实验二：

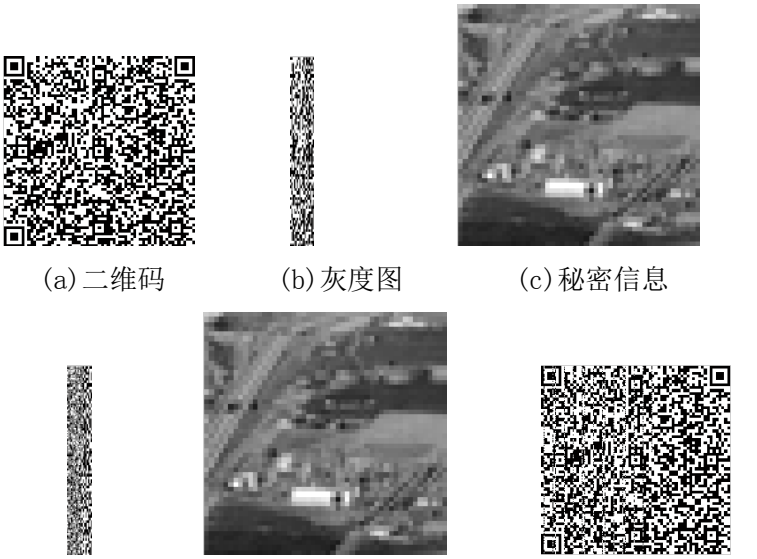
在本实验中，使用的本文作为秘密信息 1，用以生成二维码。假设秘密信息 1 为：At the beginning of the new semester, every student is required to register with the department. In the case of failure to register, he has go to department to go through the formalities for leave, and those absent for two weeks without asking for leave are thought to drop out.实验结果如图 3.15 和 3.16 所示。



(a)二维码　(b)灰度图　(c)秘密信息

(d)含密灰度图　(e)提取的秘密信息　(f)还原的二维码

图 3.15 基于二维码的 LSB 新算法实验结果 3



(a)二维码　(b)灰度图　(c)秘密信息

(d)含密灰度图　(e)提取的秘密信息　(f)还原的二维码

图 3.16 基于二维码的 LSB 新算法实验结果 4

3.4.4 新算法的仿真结论

实验表明，隐藏在灰度图中的秘密信息可以完整的被提取出来，还原的二维码也可以正确的读取到结果。不同的秘密信息嵌入灰度图像之后对灰度图像的影响不同，对还原的二维码也有不同的影响，不过还原的二维码都可以正确的解码。对二维码中本身表示的信息没有影响。

在上述试验中，秘密信息 1 生成二维码，然后将这个二维码编码为灰度图，接下来，

将秘密信息 2 写入灰度图中，最后将灰度图写入到载体图像中。读取信息的时候，首先从载体图像中读取灰度图，然后从灰度图中读取秘密信息 2，然后将灰度图还原为二维码，最后读取二维码中的秘密信息。实验证明，这种算法可以有效地将两份秘密信息通过一个载体图像传递到目的地。

3.5 本章小结

本章首先介绍了 LSB 算法的原理，分析了 LSB 算的优势和劣势，然后使用 LSB 算法进行了仿真实验，发现利用 LSB 嵌入信息后，载体图像有变化，但是肉眼不易察觉。

紧接着根据第二章研究结果，实现了本文的二维码的生成方法，本文方法中既可以用文字生成二维码，也可以使用图片生成二维码，随后列举了一些生成的效果图。接下来介绍了本文的二维码转灰度图的原理，给出了转换原理图。详细描述了与具体实现步骤，其核心思想是将二维码以 8 位为单位转换为一个灰度图对应位置的像素值。小节最后，给出了本文提出的基于二维码的 LSB 新算法，画出了算法框图，详细描述了每个关键步骤。

本章最后对新算法的具体实现进行了介绍，给出了新算法的文字描述以及关键部分的 matlab 源代码。最后通过两个具体实验说明了本文算法的有效性，隐藏在二维码编码的灰度图中的秘密信息 2 可以被正确提取，二维码本身表示的秘密信息 1 也可以被准确解码，两份秘密信息都可以准确的传递。

4 二维码的 DCT 域信息隐藏算法

4.1 引言

信息隐藏是指把一种秘密信息隐藏在另一种信息中得到含密载体，一般情况下，难以发现普通信息中隐藏有秘密信息，即时已知有秘密信息隐藏在其中也很难提取出来。

数字图像是信息隐藏算法目前较多采用的一种载体，具有较大冗余空间等特点，主要有两类算法，分别是空间域信息隐藏算法和变换域信息隐藏算法。空域算法在之前已经介绍过。频域信息隐藏算法的原理是利用数学变换，将图像变换为频域图，通过将秘密信息隐藏在频域图中来实现信息隐藏，解密时利用反变换来还原秘密信息，主要有离散余弦变换域DCT算法、离散傅里叶变换域DFT算法、离散小波变换域DWT算法等。一般情况下，空域的信息隐藏算法之前有过介绍，它具有隐藏容量大、鲁棒性弱的特点。频域的信息隐藏算法具有鲁棒性强的特点，但是其嵌入容量较小，算法复杂度高，在实际使用过程中有信息嵌入和提取速度慢的特点。

作者通过查阅文献发现，很多学者对此已经有过一定的研究[28-39] [41-45]，有学者提出将变换后的频谱进行均匀化处理，也有提出通过调整变换后的频域图的DCT系数正负值来实现信息隐藏，也有提出将原图进行分块变换，通过调整分块变换结果的相对系数来实现信息隐藏，也有提出利用编码技术对频域图进行处理，实现信息隐藏。

通过这些改进使得信息隐藏算法在隐藏容量上有一定的提高，但对于图像传输过程中可能遇到的抗压缩问题研究甚少，本节主要研究DCT信息隐藏算法，在第五章会研究压缩对隐藏算法的影响，并通过标准图像验证了本文算法的性能。

4.2 频域 DCT 信息隐藏算法

4.2.1 DCT 嵌入算法的实现

离散余弦变换（DCT）属于一种正交变换图像编码方法，是有损图像压缩JPEG的核心。它是一种以实数的余弦函数为变换核的实数域变换。离散余弦变换的原理是利用傅里叶变换的对称性，对图像进行二维离散傅里叶变换得到的结果中仅包含余弦项。实际上对一幅图像进行离散余弦变换变换后不难发现，很小一部分变换系数中包含大多数图像中重要的可视信息。图像处理和图像信息隐藏技术只运用二维离散余弦变换。

二维的DCT变换公式如下：

$$F(p,q)=a(p)a(q)\sum_{m=0}^{M-1}\sum_{n=0}^{N-1}f(m,n)\cos\left[\frac{(2m+1)p\pi}{2M}\right]\cos\left[\frac{(2q+1)q\pi}{2N}\right] \quad (4.1)$$

其中 $p=0,1,\mathrm{L},M-1;q=0,1,\mathrm{L},N-1,$ DCT 反变换的公式如下

$$f(m,n)=\sum_{p=0}^{M-1}\sum_{q=0}^{N-1}a(p)a(q)F(p,q)\cos\left[\frac{(2m+1)p\pi}{2M}\right]\cos\left[\frac{(2n+1)q\pi}{2N}\right] \tag{4.2}$$

其中 $m=0,1,\mathrm{L},M-1;n=0,1,\mathrm{L},N-1,$ 以上两个公式中 $a(p),a(q)$ 由下式定义：

$$a(p)=\begin{cases}\sqrt{\dfrac{1}{M}}, & p=0\\ \sqrt{\dfrac{2}{M}}, & p=1,2,\mathrm{L},M-1\end{cases},a(q)=\begin{cases}\sqrt{\dfrac{1}{N}}, & q=0\\ \sqrt{\dfrac{2}{N}}, & q=1,2,\mathrm{L},N-1\end{cases}$$

为了更深一步的研究 DCT 运算的实现以及改善其效果，我们引入DCT 变换矩阵，$M\times N$ 变换矩阵 T 由下式得到：

$$T_{p,q}=\begin{cases}\dfrac{1}{\sqrt{M}} & p=0,0\le q\le M-1\\ \sqrt{\dfrac{2}{M}}\cos\pi(2q+1)p/2M, & 1\le p\le M-1,0\le q\le M-1\end{cases} \tag{4.3}$$

我们有矩阵 A ，它是 $M\times N$ 的矩阵，则 $T\times A$ 也是 $M\times N$ 的矩阵，该矩阵的列包含矩阵 A列的一维 DCT。A 的二维 DCT 可以通过计算 $B=T\times A\times T'$ 获得。由于 T 是一个实标准正交矩阵，所以其逆变换的形式与变换形式一致，因此，B 的二维逆 DCT 由 $T'\times A\times T$ 给出。这使得算法的程序实现非常容易。由于DCT变换具有这样的实现特点，因此通常也可以吧DCT变换当做一个典型的图像正交变换。

图4.8显示了lena图像DCT变换前后对比结果，a图示lena原始图像，b图示DCT系数的光谱图，通过这个图很容易看出DCT系数的低频和高频系数的分布规律。

(a)原始图像　　(b)DCT变换域图像

图 4.8 DCT 变换

随着余弦函数的频率增大，表现在这里就是p、q不断增大，得到的系数就是原始图像在余弦函数上的投影，因此其中包含有低频、中频和高频系数。通过观察不难发现，在b图中，从左上到右下是一个系数递减的过程，即低频系数都在左上角，高频系数在右下角，高频系数的绝对值小于低频系数的绝对值。

4.2.2 DCT 嵌入算法的仿真实验

基于DCT变换的信息隐藏算法[42]的一般做法是，通过变换图像块中某两个DCT系数的相对大小来嵌入秘密信息。为了保证该算法的容量，一般情况下需要将图像分块，每一块中编码一个秘密信息比特位。进行秘密信息嵌入时，采用某些方法控制选取图像块b_i以表示第i个消息比特的编码空间。

选定的图像块后，利用DCT块区域特性来调整相应位置的系数，由于高频分量是图像压缩的主要对象，会影响秘密信息，若在此处隐藏影响算法的鲁棒性，而人类视觉对低频部分最敏感，在此处隐藏会降低算法的不可见性。因此，中频部分是较好的隐藏点，通常的做法是利用人眼对不敏感的特点，修改中频部分的系数来完成秘密信息的隐藏。

我们用（u_1,v_1），（u_2,v_2）来表示这两个中频系数的索引，DCT信息隐藏算法描述如下：

if（要隐藏信息='1'）

change （u_1,v_1）〈（u_2,v_2）

e1se

change（u_1,v_1）>（u_2,v_2）

该算法的原理是通过读取秘密信息的值，主来调整DCT系数满足这一规则。如果这两个系数的相对大小与要编码的秘密信息的值不匹配，我们调整两个系数的相对大小，使之满足之前的规则。所以change的实质性操作是交换或者不交换。在实践中发现，由于这一对系数大小相差不大，难以保证在隐秘图像在保存、网络传输以及提取信息时再次被读取等过程中不发生变化。

利用之前分析，在Matlab上仿真实现之后，进行两组实验，两组仿真结果分别如图4.9、4.10所示。

(a)秘密信息　(b)载体图像　(c)含密图像　(d)提取的秘密信息

图 4.9 传统 DCT 变换后提取目标图像实验 1

(a)秘密信息　(b)载体图像　(c)含密图像　(d)提取的秘密信息

图 4.10 传统 DCT 变换后提取目标图像实验 2

4.3 基于二维码的DCT新算法

4.3.1 新算法流程图

根据上一节分析不难发现，DCT算法具有较好的抗压缩能力，根据之前介绍，二维码具有较好的容错能力，本文将此二者结合，研究其是否会有较大容量，同时还具有较好的抗压缩性能。

在第三章已经研究了二维码的生成以及二维码转换为灰度图，这里不再赘述，首先给出基于二维码的DCT新算法流程图。

基于二维码的DCT新算法流程图如下：

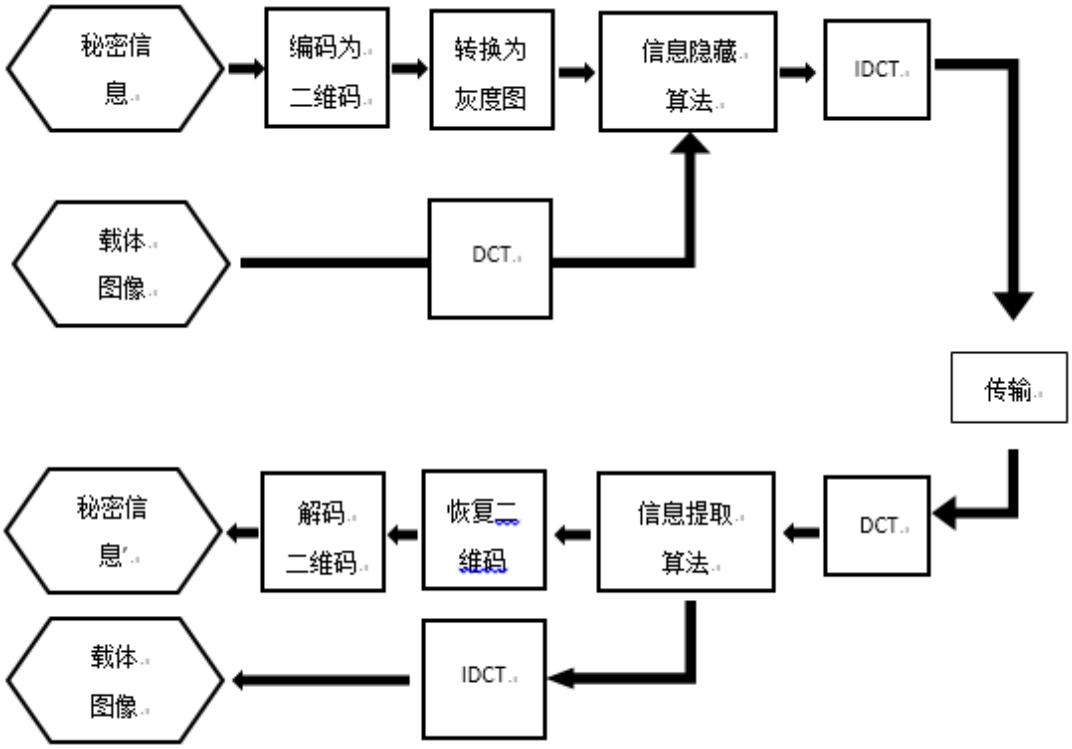


图 4.10 基于二维码的 DCT 新算法流程图

4.3.2 新算法流程图说明

新算法各主要步骤介绍如下：

DCT：在算法中有两处使用到DCT变换，分别是给载体图像嵌入信息时和对传输结束的图片进行秘密信息提取之前。DCT变换的原理在之前已经有详细介绍，这里不再赘述。通过DCT变换，将图像转换为频域的图片，从而进行后续的信息隐藏等操作。本文算法使用Matlab 2014a进行仿真，直接调用系统中自带的函数 dct2( ) 实现。

IDCT：在算法中有两处使用到了IDCT变换，分别在嵌入秘密信息等待传输前和利用信息隐藏算法提取出秘密信息之后。IDCT是DCT反变换，通过此操作可以将DCT变换后得到的频域图像转换为一般的空域图像。通过此算法，可以将嵌入秘密信息之后的图片直观的展示出来。本文算法使用Matlab 2014a进行仿真，直接调用系统中自带的函数 idct2( ) 实现。

编码为二维码：在此算法中编码为二维码，是将秘密信息编码为二维码图像，使用的技术与之前第三章介绍的一致，这里不再赘述，通过将信息编码为二维码，能够增强信息的抗干扰能力，提升算法的抗压缩性能。

转换为灰度图：这里的转换为灰度图操作，与之前第三章所介绍的转换为灰度图操作步骤一致。这里将二维码转换为灰度图可以有效降低二维码图片的大小，相对提升了

算法的容量，在实际操作中，这一步骤意义重大。

信息隐藏算法：这里的信息隐藏算法指的是，将秘密信息写入DCT图像的方法，主要实现手段就是调整不同的中频系数的值的大小，用来表示数据，这样的操作可能对图像造成一定的影响。

传输：这一步表示含密图像在不同网络下的传输。这里的传输可以是在卫星信道中，当然不仅限于此，对本文算法来说这里的传输可能是在互联网中传输，或者是某些专门的特殊网络中。

信息提取算法：信息提取算法与信息隐藏算法相对应，采用怎样的信息隐藏算法决定采用怎样的信息提取算法。这里的提取算法只要与信息隐藏算法对应上即可正确提取出秘密信息。在本文算法中，这一步获取到了灰度图。经过信息提取算法提取到的灰度图可能已经产生一些噪声，这些噪声在灰度图中是难以发现的，因为二维码的灰度图直观的看上去，不易找出特定规律。

恢复二维码：这一步主要完成将灰度图转换为二维码，具体转换方法与第三章一致，这里不再赘述。如果之前的灰度图中有噪声，通过这一步，噪声信号变得很明显，表现为二维码上的若干黑白点。

解码二维码：这一步表示将上一步的二维码中的秘密信息解码出来，具体过程与第三章相同，这里如果二维码已经受到严重污染，那么二维码中的秘密信息是提取不到的。

以上详细介绍了新算法的的主要步骤，以及各个步骤在算法中的作用，通过这些介绍将本文提出的基于二维码的DCT新算法完整的呈现给读者。

4.4 新算法的具体实现

4.4.1 新算法具体实现步骤

前一小节已经详细的介绍了新算法的框图以及各个关键步骤。现在将算法在实现过程中的具体步骤以及两段关键代码予以说明。

算法的具体步骤如下：

（1）读入秘密信息，并将其编码为二维码。

（2）将二维码图像编码为灰度图像。

（3）读入载体图像，将其进行DCT变换，得到DCT图像。

（4）利用信息隐藏算法将灰度图作为秘密信息写入DCT图像中。

（5）将含密DCT图像进行IDCT变换，得到空域图像。

含密灰度图像此时可能通过多种方法传输，传输完成后进行以下信息提取算法：

（1）接收含密空域图像，对其进行DCT变换，得到DCT图像2。

（2）从DCT图像2中提取秘密信息。

（3）这里得到的将秘密信息就是灰度图，将灰度图变换为二维码。

（4）将提取了秘密信息的图像进行IDCT变换，还原载体图像。

（5）将二维码图像解码，还原秘密信息。

4.4.2 新算法的关键代码

本文作者使用了Matlab对该算法进行实验仿真，本算法关键代码如下：

编码；

```
for f2=start:n
    for f1=1:2:m
        if info(p)=='1' && DCT (f1,f2)<DCT (f1+1,f2)
            temp=DCT (f1,f2);
            DCT(f1,f2)=DCT(f1+1,f2);
            DCT(f1+1,f2)=temp;
        end
        if   info(p)=='0' && DCT(f1,f2)>DCT(f1+1,f2)
                temp1=DCT(f1,f2);
                DCT(f1,f2)=DCT(f1+1,f2);
                DCT(f1+1,f2)=temp1;
        end
         if p==dctlen;
             break;
         end
        p=p+1;
    end
end
```

解码：

```
for f2=start:n
    for f1=1:2:m
        if   DCT(f1,f2)>DCT(f1+1,f2)
            tdataread=strcat(tdataread,'1');
        else
            tdataread=strcat(tdataread,'0');
        end
```

```
            if p==dctlen;
                break;
            end
            p=p+1;
        end
    end
```

4.4.3 新算法的仿真实验

按照图4.10的算法流程，对其进行实现。

将秘密信息转换为二维码，我们这里使用的秘密信息假设为：You are invited to become a member of the XUST Alumni Association. This opens the gateway to a wealth of information about XUST and helps you to recontact your classmates. This is just one of the ways helps you, one of our treasured alumni stay involved with our University.

根据之前算法步骤，这一步读入秘密信息，并将其编码为二维码。生成的二维码图像如图4.11所示。

图 4.11 二维码

将二维码编码为灰度图：

图 4.12 二维码编码为灰度图

将灰度图作为秘密信息嵌入载体图像：

（a）载体图像　　（b）含密图像

图 4.13 载体图像和含密图像

此时含密图像将在网络间传输，传输完毕后从含密图像中提取出灰度图：

图 4.14 提取到的灰度图

将灰度图还原为二维码

图 4.15 灰度图还原得到的二维码

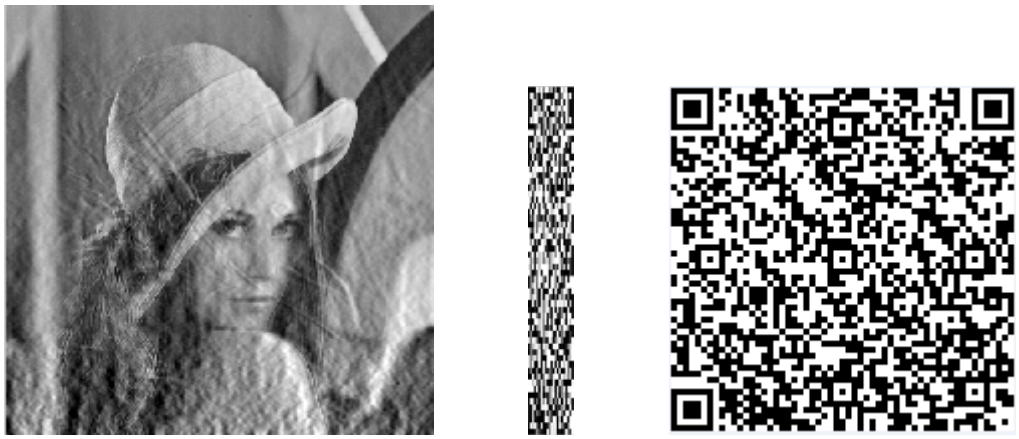
通过通用解码软件可以看到，秘密信息完好。

为了证明这种算法的有效性，接下来再给出两组实验结果：

1）秘密信息为：No matter how many miles separate you from your University, it strives to stay in contact with you and thus strengthen alumni friendship for Xi’an University of Science and Technology.

实验结果：

（a）二维码　　（b）灰度图　　（c）载体图像

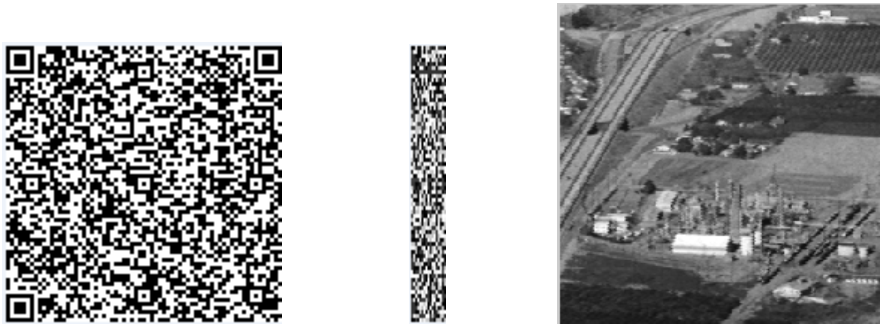


（a）含密图像　　（b）灰度图　　（c）还原的二维码

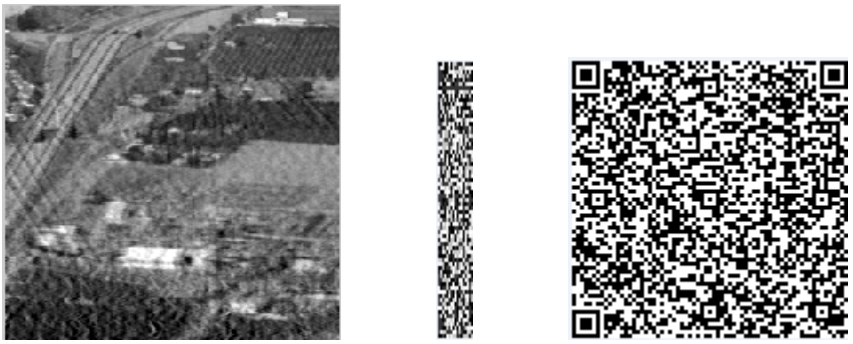
图 4.16 基于二维码的 DCT 新算法实验结果 1

2）秘密信息为：The university has been making active and universal international academic exchanges with sixty universities from over twenty countries and areas. In has set up certain friendly intercollegiate relations with the United States, Russia, Japan, the Netherlands and other foreign countries.

实验结果：



（a）二维码　　（b）灰度图　　（c）载体图像



（a）含密图像　　（b）灰度图　　（c）还原的二维码

图 4.17 基于二维码的 DCT 新算法实验结果 2

4.4.4 新算法的仿真结论

对以上两组实验所还原的二维码，通过扫码可以发现，信息完整，无丢失。通过以上两组实验不难发现，嵌入二维码对载体图像有了一定的影响，影响了载体的视觉效果。同时也不难发现，本文算法可以有效的将信息隐藏在载体图像中，并且完整的取出。

由此可知基于二维码的DCT新算法可以有效地隐藏秘密信息，并且秘密信息不会损坏。

4.5 本章小结

本章首先详细分析了DCT算法的原理，然后再Matlab平台上仿真实现了DCt信息隐藏，并给出了仿真结果。

接下来提出了基于二维码的DCT新算法，给出了算法框图，详细描述了各个关键环节，整体上给读者介绍了本文新算法的结构。

紧接着作者给出了新算法的具体实现步骤，同时给出了，作者在Matlab平台实现本算法时的几个关键步骤的代码。

最后给出该算法的实现过程，并给出两组实验结果，说明了算法的正确性。

5 隐藏算法的抗压缩研究

5.1 引言

近年来网络技术突飞猛进，多媒体信息的各种需求也增加了。根据本文之前分析，图像作为关键的信息隐藏载体，大量的信息传递进行图像处理时，传输的困难在时间和空间上凸显了出来。从经济或技术这两个方面上来看，依靠硬件创新这是不可能满足人们的需求的。通过压缩处理该图像，调整图像信息，除去存在的冗余图像等处理，对传输来说是非常有用的，这样以来，需要对图像压缩的方法和技术进行研究。有损和无损压缩是两种常见的压缩类型。无损压缩方法，有行程编码技术，霍夫曼编码压缩，算术压缩技术。有损压缩的基本思想是由新的组明确表示，或者分解相关数据，使用不同的原理组来表示不同的数据。构造新组时，大部分的系数接近零系数，剩余的信息可以被存储在较小的数据包中，可以忽略。通过压缩进行数据转换时，阈值系数是非零数据实现为无损编码，阈值系数一下的数据被设定为零。

前两章完成了对LSB算法和DCT算法的分析，并提出了自己的算法，本章重点研究这两种算法的抗压缩性能。

5.2 基于二维码的 LSB 新算法的抗压缩研究

5.2.1 LSB 嵌入算法的抗压缩性能研究

1) 利用JPEG压缩后的秘密信息

本文使用了冈萨雷斯数字图像处理一书中的JPEG压缩、JPEG2000压缩程序来进行仿真实验。使用传统LSB方法隐藏信息后，再对写有隐藏信息的载体图像做JPEG压缩处理，在不同quality值时的图片处理结果如上图所示。结果发现，即便是quality=1的情况下，藏入的图片也无法恢复。在早期作者尝试直接嵌入整幅图片到载体中，后来发现，图片的格式很容易损坏，而且格式信息一旦损坏，是无法正确读取图片内容的，后来作者对算法进行了修改，只将图片中的像素信息嵌入到载体图像中，这样即使图像信息已经很模糊，也是可以提取到图片的像素信息，恢复图像。

Quality为1时提取结果如图5.1所示。

(a)秘密信息　(b)载体图像　(c)含密图像　(d)提取的秘密信息

图 5.1 JPEG 压缩(quality=1)后提取目标图像

Quality为10时提取结果如图5.2所示。

(a)秘密信息　(b)载体图像　(c)含密图像　(d)提取的秘密信息

图 5.2 JPEG 压缩(quality=10)后提取目标图像

图5.1中秘密信息很难识别，图5.2是无法识别。Jpge压缩方法不易控制，对LSB信息隐藏算法嵌入的秘密信息影响严重。

2)利用JPEG2000压缩后的秘密信息

使用LSB方法隐藏信息后，再对写有隐藏信息的载体图像做JPEG2000压缩处理，在不同压缩比值时的图片处理结果如上图所示。结果发现，如果将整个图片文件嵌入并进行压缩，在压缩比为3的情况下，藏入的图片也无法恢复，主要原因与JPEG压缩处理后无法读取图片信息原因相同，即图片的格式信息损坏，无法正确读取图片。在使用本文之前提到的改进算法后，模糊可以看到一些像素信息。

压缩比为1.17时提取结果如图5.3所示。

(a)秘密信息　(b)载体图像　(c)含密图像　(d)提取的秘密信息

图 5.3 JPEG2000(压缩比=1.17)压缩后提取目标图像

压缩比为1.4时提取结果如图5.4所示。

(a)秘密信息　(b)载体图像　(c)含密图像　(d)提取的秘密信息

图 5.4 JPEG2000(压缩比=1.4)压缩后提取目标图像

压缩比为1.7时提取结果如图5.5所示。

(a)秘密信息　(b)载体图像　(c)含密图像　(d)提取的秘密信息

图 5.5 JPEG2000(压缩比=1.7)压缩后提取目标图像

图5.4中秘密信息受到了噪声的污染，但是整体上清晰可辨，图5.5受到了较严重影响，在本实验中只有船的轮廓模糊可辨，图5.6提取到的秘密信息已经完全无法辨认了。根据以上结果可以分析得出，JPEG2000的压缩比更容易控制，能够给算法效果的分析带来便利，因此在此后的文章中使用JPEG2000来进行压缩实验。

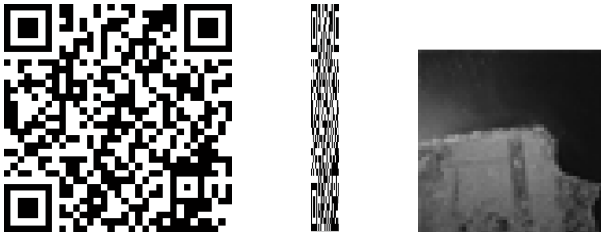
5.2.2 基于二维码的 LSB 嵌入算法的抗压缩性能研究

传统LSB算法对压缩非常敏感，由于有效信息被隐藏在了最低位，压缩后对最低位影响很大，导致信息丢失。在这里本文提出一种新的思路，将有效信息写在最高位，这样以来可以显著提升算法的抗压缩性能，同时保证了算法的大容量。

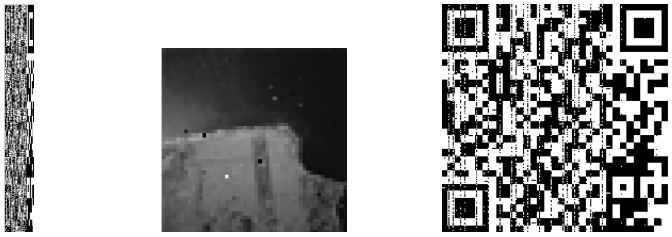
由于二维码的特殊性，我们将二维码编码为灰度值，编码为灰度值的二维码又有了自己新的特性，它的高位和低位分别对应二维码图像的一个像素点，对于二维码来说这两处像素点的重要程度是相同的，因此把信息隐藏在高位也不会对二维码内容带来影响。

先给出第一组实验结果，实验中使用到的二维码内容是：Xi`an University of Science and Technology。

压缩比为1.17时结果如图 5.6所示，秘密信息前后PSNR= 33.9dB。



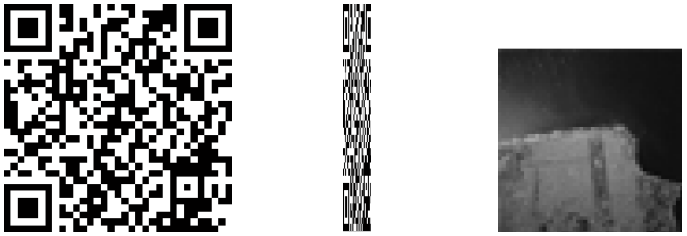
(a)二维码　(b)灰度图　(c)秘密信息



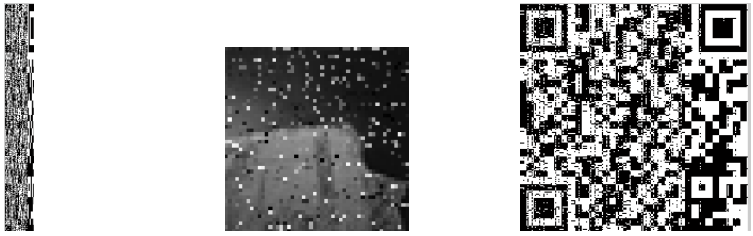
(d)压缩后含密图像　(e)提取的秘密信息　(f)二维码

图 5.6 基于二维码的 LSB 新算法压缩实验 1-1

压缩比为1.4时结果如图 5.7所示，秘密信息前后PSNR= 18.0dB。



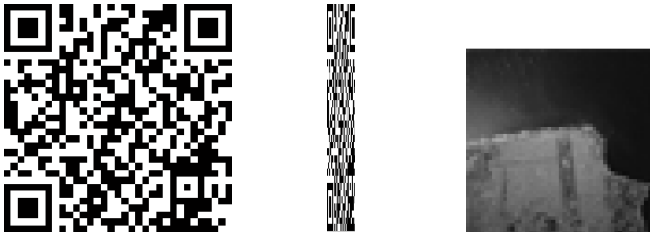
(a)二维码　(b)灰度图　(c)秘密信息



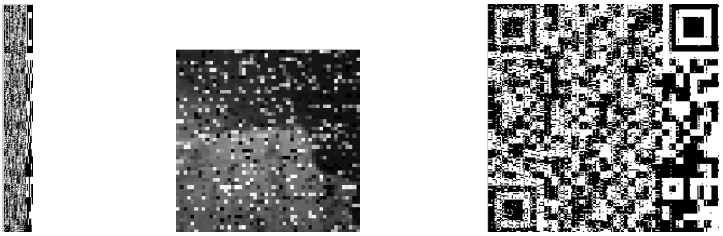
(d)压缩后含密图像　(e)提取的秘密信息　(f)二维码

图 5.7 基于二维码的 LSB 新算法压缩实验 1-2

压缩比为1.7时结果如如图 5.8所示，秘密信息前后PSNR= 14.2dB。



(a)二维码　(b)灰度图　(c)秘密信息

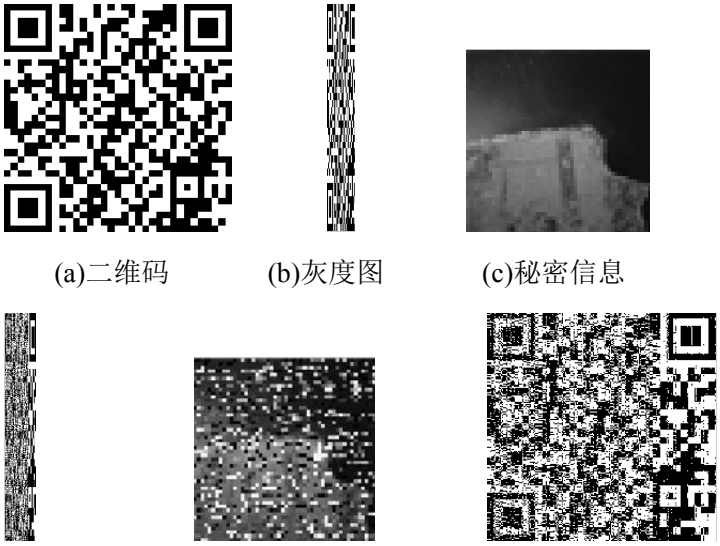


(d)压缩后含密图像　(e)提取的秘密信息　(f)二维码

图 5.8 基于二维码的 LSB 新算法压缩实验 1-3

此时二维码已经不能直接解码，通过处理后才可以正确解码。而提取到的嵌入图像依然模糊可见。

压缩比为2.5时结果如图 5.9所示，秘密信息前后PSNR= 12.1dB。



(a)二维码　(b)灰度图　(c)秘密信息

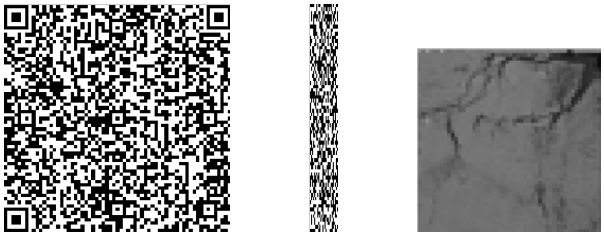
(d)压缩后含密图像　(e)提取的秘密信息　(f)二维码

图 5.9 基于二维码的 LSB 新算法压缩实验 1-4

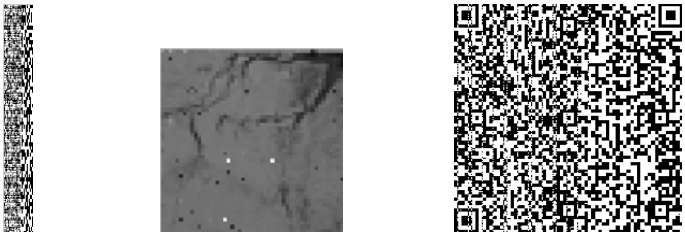
此时二维码已经较为严重的模糊，提取到的嵌入图像依然模糊可见。

接着给出第二组实验结果，实验中使用到的二维码内容是：At the beginning of the new semester, every student is required to register with the department. In the case of failure to register, he has go to department to go through the formalities for leave, and those absent for two weeks without asking for leave are thought to drop out。

压缩比为1.17时结果如图 5.10所示，秘密信息前后PSNR= 31.7dB。



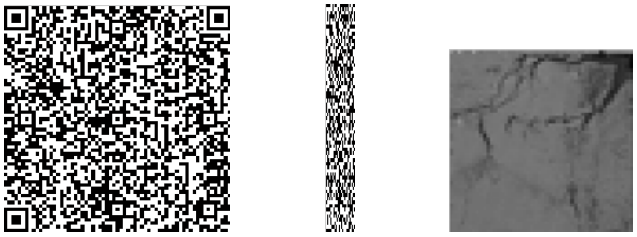
(a)二维码　　(b)灰度图　　(c)秘密信息



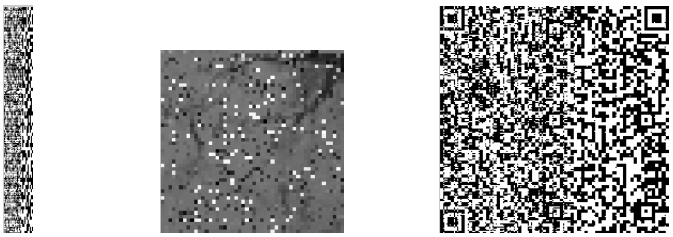
(d)压缩后含密图像　　(e)提取的秘密信息　　(f)二维码

图 5.10 基于二维码的 LSB 新算法压缩实验 2-1

压缩比为1.4时结果如图 5.11所示，秘密信息前后PSNR= 17.3dB。



(a)二维码　　(b)灰度图　　(c)秘密信息



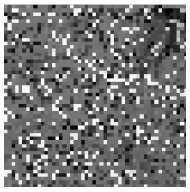
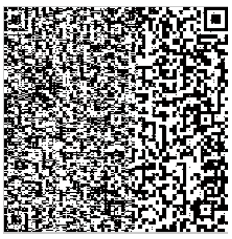
(d)压缩后含密图像　(e)提取的秘密信息　　(f)二维码

图 5.11 基于二维码的 LSB 新算法压缩实验 2-2

压缩比为1.7时结果如如图 5.12所示，秘密信息前后PSNR= 13.1dB。



(a)二维码　　(b)灰度图　　(c)秘密信息

(d)压缩后含密图像　　(e)提取的秘密信息　　(f)二维码

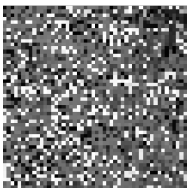
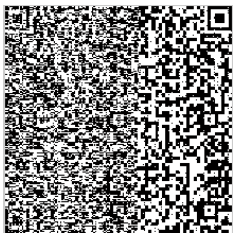
图 5.12 基于二维码的 LSB 新算法压缩实验 2-3

此时二维码已经不能直接解码，通过处理后才可以正确解码。提取到的嵌入图像比较模糊，需要经过处理才可分辨清楚。

压缩比为2.5时结果如如图 5.13所示，秘密信息前后PSNR= 11.4dB。



(a)二维码　　(b)灰度图　　(c)秘密信息

(d)压缩后含密图像　(e)提取的秘密信息　　(f)二维码

图 5.13 基于二维码的 LSB 新算法压缩实验 2-4

此时二维码已经较为严重的模糊，难以解码，提取到的嵌入图像相当模糊，基本不可见。

可以很明显的看出，利用二维码特性将秘密信息隐藏在高位，带来很大的抗压缩性

能提升。另外，二维码表示的秘密信息越多，二维码越容易被破坏。

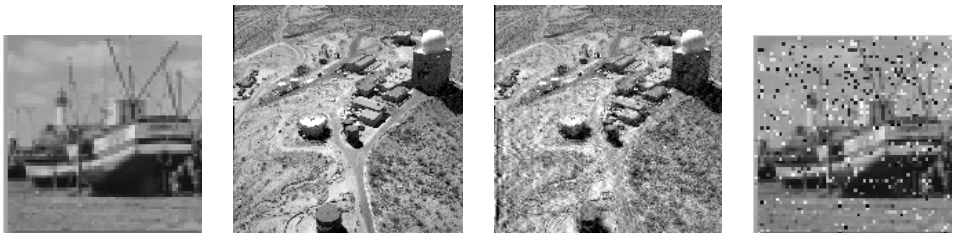
在本文方法中，通过一个载体图像，传递了两份有效信息到地面，一份是二维码代表的信息，另外一份是利用最高有效为算法藏在二维码转化成的灰度图中的信息，在经过2倍压缩后，两份信息都基本完好。综上所述，本文提出的将有效信息写在二维码转换成的灰度图的高位这种算法，具有相对较大的容量和抗压缩的特点。

5.3 基于二维码的 DCT 新算法的抗压缩研究

5.3.1 DCT 嵌入算法的抗压缩性能研究

对已实现的DCT嵌入算法，利用JPEG2000压缩进行分析，分析结果如图5.14到5.17所示：

1）在压缩比为1.17情况下结果如图5.14所示。



(a)秘密信息　(b)载体图像　(c)压缩后的含密图像　(d)提取的秘密信息

图 5.14 传统 DCT 变换并压缩后提取目标图像 1

2）在嵌入前压缩比为2.5情况下结果如图5.15所示。

(a)秘密信息　(b)载体图像　(c)压缩后的含密图像　(d)提取的秘密信息

图 5.15 传统 DCT 变换并压缩后提取目标图像 2

3）在嵌入前压缩比为3.5情况下结果如图5.15所示。

(a)秘密信息　　(b)载体图像　　(c)压缩后的含密图像　(d)提取的秘密信息

图 5.15 传统 DCT 变换并压缩后提取目标图像 3

不难看出，DCT算法的抗压缩能力比较强，在压缩比2.5的情况下，依然模糊可见目标图像。

针对仿真数据进行分析不难得出，算法以秘密信息来调制DCT系数使之完成对秘密信息的隐藏。但这样算法的隐藏信息量变得很少，一幅512×512灰度图像在满足视觉不可感知性要求时的嵌入容量一般只有1000bits左右[44]。

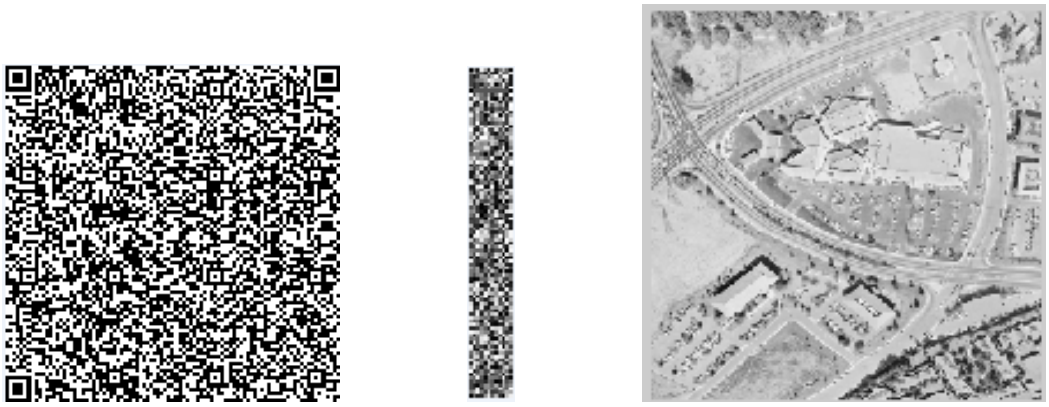
结论：以二维码图片为载体的DCT算法有一定抗压缩性能，但是容量有限。

5.3.2 基于二维码的 DCT 嵌入算法的抗压缩性能研究

传统DCT算法具有优良的抗压缩性能，而二维码本身就具有一定的纠错能力，因此将这两者结合，会有更好的抗压缩能力。

在压缩比为1.17情况下：

这里给定二维码内容为：The university succeeded in hosting a series of international academic conferences such as t he international symposium on applications of Computer Methods in Rock Mechanics and Engineering. The university has also established jointly cultivating undergraduates and postgraduates cooperative relationship with international famous universities like Michigan Technological University, university of Missouri-Rolla, Troy state University of the United States and Monash University of Australia. In the year 2004, it sent its first group of fourteen undergraduates to America for advanced studies.



（a）二维码　　（b）灰度图　　（c）载体图像

（d）含密图像

（e）压缩后含密图像

（f）提取的灰度图

（g）还原的二维码

图 5.18 基于二维码的 DCT 新算法实验结果 1

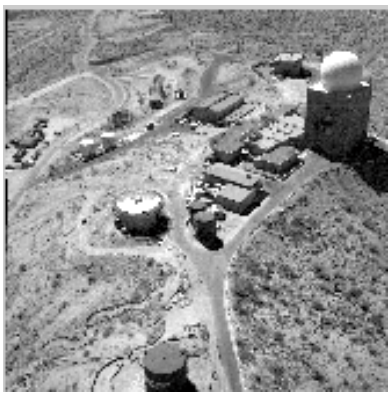
在这种情况下利用解码软件可以识别出二维码。

在压缩比为1.7情况下：

这里给定二维码内容为：Here we write to you with an intention to get help from you for recommending foreign teachers to our University in the future, starting from September, 2004 till later years in the future.

（a）二维码

（b）灰度图



（c）载体图像

（d）含密图像

（e）压缩后含密图像

（f）提取的灰度图

（g）还原的二维码

图 5.19 基于二维码的 DCT 新算法实验结果 2

由图5-19分析知，这种压缩比下依然可以完整还原二维码信息。由此不难发现，基于二维码的DCT新算法具有较好的抗压缩能力。

5.4 本章小结

本章中先对JPEG压缩和JPEG2000压缩算法做了讨论，通过LSB嵌入算法的多组实验体现出了JPEG2000压缩的优秀之处，JPEG2000更加易于使用。

接下来讨论了本文提出的基于二维码的LSB新算法，LSB算法抗压缩能力很弱，与二维码技术结合有具有了一定的抗压缩能力，以二维码为载体，把信息写在二维码编码位的灰度图高位中，使得算法得到了较好的抗压缩能力。

最后分别讨论了DCT嵌入算法以及本文提出的基于二维码的DCT新算法，通过多个实验，证明了本文提出的算法同样具有一定抗压缩能力。

6 总结和展望

信息隐藏技术的研究始于20世纪90年代，是一项崭新且有着古老思想渊源的信息保护技术。自提出以来，国内外学术界、工业界、政府和军方研究机构投以极大的热情，掀起了信息隐藏的研究热潮。

本文分析了信息隐藏技术的国内外发展状况，总结了二维码技术、典型的信息隐藏算法、图像压缩技术等，分别研究了空域和频域的信息隐藏算法，并将其与二维码技术相结合，提出了相对应的信息隐藏新算法。结合本课题研究背景，本文重点考虑压缩在图像隐藏中对秘密信息的影响。现将主要工作总结如下：

(1) 研究了信息隐藏背景，该技术的国内外研究现状。为后续隐藏算法的研究做铺垫。

(2) 研究了空域信息隐藏新算法。提出了结合二维码的LSB新算法，并对算法进行了详细的叙述、仿真，分析实验数据，得到较好效果。

(3) 研究了频域的信息隐藏算法。提出了基于二维码的DCT新算法，在DCT域进行信息隐藏来隐藏秘密信息，对算法进行了实验仿真，分析实验数据，证明了算法的可用性。

(4) 对本文中提出的新算法进行抗压缩性能比较研究，分别研究了LSB信息隐藏算法、基于二维码的LSB信息隐藏算法、DCT信息隐藏算法和基于二维码的DCT信息隐藏算法。说明了新算法在隐藏容量和抗压缩能力上的提升。

本文提出的结合二维码的信息隐藏算法还有一些不足之处，可以从以下几方面进行改进：

在以二维码转换成的灰度图像作为载体嵌入信息时，需要在算法上避开二维码格式所在区域，以免造成二维码无法识别。

对本文算法再做改进时，可以制作二维码格式模板，由于二维码格式是固定的，将信息隐藏在其格式所在位置，在后续处理时可以先提取格式所在位置的有效信息，之后提取其他位置的信息，最后根据格式模板，恢复二维码所表示的信息。

改进二维码识别算法，很多时候提取出来的二维码直观看上去还是有一定信息的，然而其格式已经损坏，现有的解码方式无法对其进行解码。

今后可以结合其它先进的信息隐藏算法，如[47][15]来研究二维码信息隐藏。

致谢

岁月如歌，光阴似箭，三年的研究生生活即将结束。经历了系统的理论课学习、找工作的喧嚣与坎坷，我深深体会到了写作论文时的那份宁静与思考。回首三年来的研究生求学历程，我百感交集，思绪万千，对那些引导我、帮助我、激励过我的人们，心中充满了无限感激。

首先，我感谢导师张释如教授（博士）对我的悉心指导。在我有关二维码论文选题定题，到开题报告的写作，再到论文的研究、写作修改定稿，她前前后后倾注了大量的心血。在我理论课学习和论文研究期间，她除了给我生活上的关照、工作学习上很多指导以外，还常常抽出休息时间给我指点迷津，甚至她在出国访问、做大学客座教授期间还检查我的工作情况。在此，谨向我敬爱的张老师表示我最诚挚的敬意和感谢！

其次，我要感谢我的校外老师周诠研究员（博士）百忙中对我的耐心指导。他是中国空间技术研究院西安分院(西安空间无线电技术研究所)信息与通信工程博士生导师，中国航天科技集团公司电子与通信学术技术带头人，国家重点实验室数据传输领域专家，国家航天重大研究项目以及国家自然科学基金项目负责人。他担任陕西省图象图形学学会副理事长，陕西省创造学会副理事长，中国图象图形学学会常务理事、数码影像专业委员会委员，中国体视学会理事、图象分析分会副主任委员，中国电子学会高级会员、信息论分会委员，中国通信学会高级会员等学术职务。在我论文选题、研究、写作、修改过程中，周老师抽出了宝贵的时间，给了我许多指导与建议，在此我表示由衷的敬仰和衷心的感谢！

同时，我要感谢所有教导过我、关心过我的老师。特别是通信与信息工程学院的李国民教授、李白萍教授、韩晓冰教授、刘琳教授、吴延海教授等所有给我传授教学和实验实践知识的各位老师。

在此也要感谢我生活学习了三年的母校——西安科技大学，母校给了我一个宽阔的学习平台，让我不断吸取新知，充实自己。

感谢一直关心与支持我的同学和朋友们！感谢我寝室的姐妹们，学院2012级全体研究生同学，感谢他们给予我的所有关心和帮助！两年来，我们朝夕相处，共同进步，同窗之谊，我将终生难忘！此外，我还要感谢薛朗平同学在论文期间给我的关心和帮助。

最后，感谢我的父母，特别是我的母亲，在多少个日日夜夜，母亲除了照顾我生活以外，还督促我搞研究等等。父母的养育之恩无以为报，他们是我求学路上的坚强后盾和靠山，在我面临人生选择的迷茫之际，他们为我鼓劲打气、排忧解难，他们对我无私的爱与照顾是我不断前进的动力。

参考文献

[1] F.A.P.Petitcolas, R.J.Anderson, and M.G.Kuhn. Information hiding-A survey [J]. Proc. IEEE, vol. 87, no.7, pp.1062-1078,1999.

[2] J. Kelley. Terror groups hide behind Web encryption[N]. USA Today News, 2001- 02-05.

[3] 吴佳鹏. 二维条码识读技术及其应用研究[D]. 博士论文, 天津大学, 2009

[4] ISO/IEC 16022:2006.Data Matrix bar code symbology specification[S].

[5] ISO/IEC 15438:2006.Information technology-Automatic identification and data capture techniques-PDF417 bar code symbology specification (second ed.)[S].

[6] ISO/IEC 18004:2006.Information technology-Automatic identification and data capture technology-QR code 2005 bar code symbology specification[S].

[7] Microsoft.Microsoft Tag[EB/OL].http://tag.microsoft.com/home.aspx, 2011-11-13.

[8] GB/T 21049-2007.中华人民共和国标准-汉信码[S].

[9] SJ/T 11350-2006.二维条码 紧密矩阵码[S].

[10] 杨义先, 钮心忻. 多媒体信息伪装综述[J]. 通信学报, 2002, 23(5):18-26.

[11] C.Kurak and J.McHugh. A cautionary note on image down grading [C] .In Proceedings of the 8th IEEE Annual Computer Security Applications Conference. pp.153-159, 1992.

[12] 王丽娜，张焕国，叶登攀. 信息隐藏技术与应用[M], 湖北：武汉大学出版社，2009

[13] 冯新岗，基于卫星数据传输的图象信息隐藏技术研究[D]，博士学位论文，中国空间技术研究院，2010

[14] 李晓博，卫星数传系统中的图像信息隐藏算法研究[D]，博士学位论文，中国空间技术研究院，2013

[15] 朱历洪, 周诠. 卫星遥感图像的鲁棒无损信息隐藏传输算法[J]，宇航学报，2015, 36(3):315-323.

[16] Hai Fang, Quan Zhou. Robust Watermarking Scheme for Multispectral Images: Using Discreate Wavelet Transform and Tucker Decomposition[J], Journal of Computers. 2013,8(11): 2844-2850

[17] 赵博,黄进. 基于 PDF417 条码的信息隐藏方法[J]. 计算机工程与设计,2007, 28(19): 4806- 4809.

[18] Sartid Vongpradhip, Suppat Rungraungsilp. QR Code Using Invisible Watermarking in Frequency Domain[C]. 2011 Ninth International Conference on ICT and Knowledge Engineering. pp. 47-52, 2011.

[19] Wen-Pinn Fang. Offline QR Code Authorization Based on Visual Cryptography [C].

2011 Seventh International Conference on Intelligent Information Hiding and Multimedia Signal Processing. pp.89-92, 2011.

[20] Chin-Ho Chung, Wen-Yuan Chen, Ching-Ming Tu. Image Hidden Technique Using QR-Barcode [C]. 2009 Fifth International Conference on Intelligent Information Hiding and Multimedia Signal Processing. pp.522-525, 2009

[21] G.Prabakaran, R.Bhavani, M.Ramesh. A Robust QR- Code Video Watermarking Scheme Based On SVD and DWT Composite Domain [C]. Proceedings of the 2013 International Conference on Pattern Recognition, Informatics and Mobile Engineering. pp.251-257, 2013.

[22] 李明建, 赖惠成. 基于编码和二维条形码的数字水印[J].计算机工程与应用, 2008, 44(2): 67-69.

[23] 柴天天.基于二维条码 QR 码的安全复印系统设计与实现[D]. 硕士论文, 北京邮电大学, 2011.

[24] 冯新岗, 周诠. 基于图像复杂度分类的卫星遥感图像信息隐藏[J].宇航学报,2010,31(7): 1850-1854.

[25] 李晓博, 周诠. 基于直方图修改的卫星遥感图像无损隐藏传输[J].宇航学报, 2013, 34(5): 686-692.

[26] Bender W D, Gruhl N. Morimoto. Techniques for Data Hiding[J].IBM Systems Joumal,1996,35(34):131-336

[27] 夏光升. 信息隐藏技术研究 北京邮电大学博士学位论文，2003：8-10

[28] S.Voloskynovskiy，S.Pereira and T.pun，Attack modeling：Towards a second generation watermarking benckmark [J] ． Signal Processing．2001.81：1177-1214

[29] Khorasani M K. Sheikholeslami M M. A DWT-SVD Based Digital Image Watermarking Using a Novel Wavelet Analysis Function[C]. Fourth International Conference on Computational Intelligence, Communication Systems and Networks (CICSyN), Thailand , 2012: 254 – 256

[30] M.Zhao,Y.Dang. Color image copyright protection digital watermarking algorithm based on DWT&DCT[C].In：Proceedings of 2008 International Conference on W ireless Communications, Networking and Mobile Computing, Scientific Research Publishing,USA,2008:659-662.

[31] Po-Chyi Su C-C Jay Kuo. Steganography in JPEG2000 Compressed Images[J]. IEEE Trans. on Consumer Electmnics 2003 49(4):824-832

[32] 孟宪浩等. 一种基于二维 DCT 变换的图像信息隐藏方法 光电技术应用, 2009.06

[33] Z．Wang Z，A．C．Bovik，L．Lu．Why is image quality assessment so difficult [A] In：

Proc．IEEE International Conference on Acoustics，Speech，and Signal Processing[C]，Orlando，2002，v01．4：IV-3 3312-3 316

[34] 黄继武. SHI YUN Q. 一种自适应图像水印算法.自动化学报, 1999

[35] 黄继武,YunQ SHI, 程卫东. DCT 域图像水印:嵌入对策和算法.电子学报,2000, 28(4):57-60

[36] 黄继武, YunQ SHI, 姚若河. 基于块分类的自适应图像水印算法.中国图象图形学报,1999, 4(8):640-643

[37] Cheng W D, Huang J W, Liu H M.A 3D-DCT-Based Information Hiding Algorithm for Color Images[J]. Acta Automatica Sinica, 2003,29(2):258-265

[38] 李钢,杨杰. 改进的基于离散小波变换的数字水印技术[J].红外与激光工程,2003, 32(1):96-100.

[39] 刘九芬,黄达人,胡军全. 数字水印中的双正交小波基[J].中山大学学报(自然科学版),2002,.41(4):1-5

[40] ISO/IEC FCD15444-1 JPEG2000 image coding system 2000

[41] D.Nister，C.Christopoulos. An Embedded DCT-based still image coding algorithm[J]. IEEE Signal Processing Letters. 1998, 5(6):135-137.

[42] 魏佳圆. 遥感图像抗压缩信息隐藏技术研究[D]. 硕士论文, 中国空间技术研究西安分院, 2013.

[43] 谢建全, 阳春华,黄大足等. 一种大容量的 DCT 域信息隐藏算法[J]. 中国图象图形学报, 2009,14(8):1542-1546.

[44] 余鹏飞, 刘兵. 基于离散余弦变换的大容量信息隐藏盲提取算法[J].计算机应用, 2006,26(4): 815-817.

[45] MILLER ML, DOERR G J, COX IJ. Applying Informed Coding and Embedding to Design a Robust High-Capacity Watermark[J]. IEEE Transactions On Image Processing, 2004, 13(6):792-807.

[46] Hai Fang, Quan Zhou，Xiaojun Li, Robust Reversible Data Hiding for Multispectral Images[J], Journal of networks, 2014,9(6):1454-1463