图像信息隐藏技术与设计

1 前言

本章主要介绍信息隐藏技术的背景和研究意义、国内外信息隐藏技术研究现状，列举了本文的主要研究内容，最后给出了全文的结构安排。

1.1 信息隐藏技术的背景和研究意义

二十世纪九十年代以来，网络信息技术在全世界范围内得到了迅猛发展，它极大地方便了人们之间的通信和交流。借助于计算机网络所提供的强大的多媒体通信功能，人们可以方便、快速地将数字信息(数字音乐、图像、影视等方面的作品)传到世界各地，一份电子邮件可以在瞬息间传遍全球。但同时计算机网络也成为犯罪集团、非法组织和有恶意的个人利用的工具。从恶意传播计算机病毒，到非法入侵要害部门信息系统，窃取重要机密甚至使系统瘫痪；从计算机金融犯罪，到利用表面无害的多媒体资料传递隐蔽的有害信息等等，对计算机信息系统进行恶意攻击的手段可谓层出不穷。

因此，在全球联网的形势下，网络信息安全非常重要，一个国家信息系统的失控和崩溃将导致整个国家经济瘫痪，进而影响到国家安全。各国政府和信息产业部门都非常重视网络信息安全的研究和应用。密码技术是信息安全技术领域的主要传统技术之一，是基于香农信息论及其密码学理论的技术，一般采用将明文加密成密文的秘密密钥系统或者公开密钥系统，其保护方式都是控制文件的存取，即将文件加密成密文，使非法用户不能解读。但加密技术主要适用于文本的加密，而对音频、视频、图像等多媒体数据类型来说，由于它们的数据量往往很大，如何对超大数据量的多媒体数据进行有效的加、解密仍是一个难题。而且信息加密是利用随机性来对抗密码攻击的，密文的随机性同时也暴露了消息的重要性，即使密码的强度足以使攻击者无法破解出明文，但他仍有足够的手段来对其进行破坏，使得合法的接收者也无法阅读信息内容。随着计算机性能的大幅度提高，软硬件技术的迅速发展，加密算法的安全性受到了严重挑战。

由于加密技术的局限性，最近十几年以来，一种新的信息安全技术——信息隐藏技术(Information Hiding)迅速地发展起来。信息隐藏的渊源可以追溯到古

希腊的隐形技术(Steganography)，其希腊文的字面意思是“掩饰性地写”，也就是把一种信息隐藏于另一种信息中。数字化产品的出现，给这些古老的思想赋于了新的表达方式：将机密信息嵌入到公开的图像、视频、语音及文本文件等载体信息中，然后通过公开信息的传输来传递机密信息。对加密通信而言，可能的监测者或非法拦截者可通过截取密文，并对其进行破译，或将密文进行破坏后再发送，从而影响机密信息的安全；但对信息隐藏而言，可能的监测者或非法拦截者难以从公开信息中判断机密信息是否存在，难以截获机密信息，从而保证机密信息的安全。为了增加破译的难度，还可以把加密技术和隐藏技术相结合，即先对待嵌入对象进行加密得到密文，再把密文隐藏到载体对象中，最后通过载体的传输来传递机密信息，达到藏匿消息的目的。信息隐藏技术在保密通信、版权保护等领域中都具有广泛的应用价值，根据不同的应用背景，信息隐藏技术可以分为隐写术(Steganography)和数字水印(Digital Watermarking)两个重要分支。数字水印主要是为了保护知识产权，通过在原始媒体数据中嵌入信息来证实该媒体的所有权归属。数字水印的主要目的不是限制对媒体的访问，而是确保媒体中的水印不被篡改或消除。因此稳健性是数字水印的最基本要求之一。数字水印的稳健性是指水印图像经过一些常见的改变后，水印仍具有较好的可检测性。这些改变包括常见的图像处理(如数据压缩、低通滤波、图像增强、一次抽样、二次量化和D／A转换等)、几何变换和几何失真(如裁剪、尺度拉伸、平移、旋转、扭曲等)、噪声干扰、多重水印(multiple watermarking)的重叠等。对不同的应用场合，要求有不同的稳健性。需要指出的是，存在另一种与稳健水印性质相反的水印，称为易损水印(fragile watermarks)，它们被用来证实原始媒体是否被改变过。稳健性在整个水印系统设计中具有非常重要的分量，这也是将隐写术和数字水印区别对待的原因之一。隐写术主要考虑的是安全性(即统计特性上无法检测隐密信息的存在)和嵌入容量，不可见性等。

信息隐藏技术的发展，为社会提供一种新的隐蔽通信手段的同时也带来了新的威胁。高度发达的计算机网络使得通过互联网进行信息共享和交流变得非常普遍和容易。

信息隐藏技术的研究在信息安全领域中具有重要的地位，它对于军事、情报、国家安全方面的重要意义不言而喻。它包括了数字隐写与隐写分析两个方面。一

方面要以尽可能隐蔽的方式将信息深藏于浩如烟海的数字多媒体信号中，毫不引起对方的怀疑而达到隐蔽通信的目的；另一方则要以各种手段检测可疑信息的存在，寻找敌对隐蔽通信的信源，阻断隐蔽通信的信道。设计高度安全的隐写方法是一项富于挑战性的课题，而对隐写的准确性分析往往比隐写本身更加困难。数字隐写与隐写分析的交互发展正方兴未艾，成为互联网时代信息战技术的一个新课题。信息网络上的攻防技术水平将反映一个国家的科技水平和防范意识。

1.2 本课题国内外研究现状

出于对知识产权保护和信息安全的需求，上世纪90年代以来，国内外开始对信息隐藏技术投入了大量的关注和研究。为了便于学术交流，1996年5月，国际第一届信息隐藏学术讨论会(International Information Hiding Workshop，mw)在英国剑桥牛顿研究所召开，对信息隐藏的部分英文术语和学科分支进行了统一和规定，标志着一门新兴的交叉学科——信息隐藏学[2]的正式诞生。

1998年，美国政府报告中出现了第一份有关图像数据隐藏的报告。目前，已支持或开展信息隐藏研究的机构既有政府部门，也有大学和知名企业。从公开发表的文献看，国际上在信息隐藏方面的研究已经取得了一定的成绩。从1996年以后提出了一些成功的隐写方法，还出现了一些隐写工具。适用的技术包括将LSB嵌入法[11]直接用于图像的像素、颜色指数、变换系数，结合JPEG和MP3编写的隐写，应用扩频技术的隐写法等。近年来还出现了许多其它方法，例如基于小波变换[3]的有损压缩嵌入技术，具有抗压缩的能力；通过修改量化表嵌入数据，在提高嵌入量的同时能达到很高的隐蔽性。一些隐写算法被开发成工具，其中有数以百计的隐写软件可在互联网上获得。对隐写分析的研究也取得了不少的进展。已发表的成果包括面向JPEG图像隐写、LSB嵌入、调色板图像等隐写分析法。近年来的一些研究成果包括Memon等基于图像和音频质量测度的隐写检测技术，以及Westfeld针对MP3Steg等几种隐写算法进行的低嵌入量隐写分析。

隐写的安全性一直是研究者关注的重要问题。一些隐写分析方法要求无限的计算能力和关于载体的详细统计知识，这往往不现实，于是人们提出了实用的隐写安全性概念。最多可嵌入多少信息而不会导致统计可检测性是另一个重要问题。针对LSB嵌入法和基于压缩图像的隐写，结合安全性考虑等作了理论分析。

在国内，以数字水印[i]为代表的信息隐藏技术虽然起步比较晚，但发展却十分迅速，已经有相当一批有实力的科研人员和机构投入到这一领域中。1999年12月，我国信息安全领域的何德全、周仲义、蔡吉人与有关应用研究单位联合发起并组织召开第一届全国信息隐藏学术研讨会(CMW1999)。CIHW已成为国内最具代表性的信息隐藏学术交流活动，至今已举行了六届全国会议。第六届(CIHW20064)于2006年8月上旬在哈尔滨工业大学召开，聚集国内众多从事多媒体信息安全技术研究的专家学者，就多媒体信息安全技术及数字版权保护技术等领域的最新研究成果展开研讨，经42位专家评审，从近150篇论文中评审出78篇组成论文集，发表在哈尔滨工业大学学报增刊上。此外，全国网络与信息安全技术研讨会(NETSEC)、中国可信计算与信息安全学术会议(CTCIS)、全国图像图形学学术会议(NCIG)等各类学术研讨会都涉及到信息隐藏。各类研讨会总结、交流国内外近年来关于信息隐藏的先进技术和重大应用，研讨具有创新意义的研究方法、前沿动态及发展趋势。

所谓信息安全只有相对的意义，攻守双方在不断发展和变化中的矛盾统一，因而研究工作也在两个对立的方向展开。在隐写方面，用小波交换和矢量量化等技术将原图像嵌入到像素的低位，使隐藏图像和原图像在视觉上难以分开，提取出来的恢复图像具有可接受的质量。基于图像位平面复杂度估计和统计滤波实现隐蔽信息检测的技术则是国内学者在隐写分析方面较早发表的成果。运用网络信息论中率失真及随机编码等理论对安全性限制下的隐写容量进行了研究。

信息隐藏技术的研究目前已经取得了很大进展，国际上先进的隐写技术现已能做到：使隐藏有其它信息的信息不但能经受人的感觉检测和仪器设备的检测，而且还能抵抗各种人为的蓄意攻击，但是隐写分析还处于起步探索阶段。总的来说，信息隐藏技术尚未发展到完善实用的阶段，仍有不少技术性问题需要解决。此外，信息隐藏技术发展到今天。还没有找到自己的理论依据，没有形成理论体系。目前，使用密码加密仍是网络上主要的信息安全传输手段，信息隐藏技术在理论研究、技术成熟度和实用性方面都无法与之相比，但它潜在的价值是无法估量的，随着研究的深入发展，它将在未来的信息安全体系中发挥重要的作用。

1.3 本文的主要研究内容、研究方法和结构安排

信息隐藏技术使用的载体有图像、视频、语音及文本等数字媒体，包括数字

隐写与隐写分析两个方面的内容，本文以使用最为广泛的数字图像作为研究对象，以基于数字图像的隐写方法作为研究内容。文章介绍了信息隐藏技术的基本知识和图像信息隐藏的常用算法，像信息隐藏技术，并且运用MATLAB7.0进行大量的实验测试，对该方法的性能进行检验分析，表明该方法具有一定的优点。本文内容主要如下：

(1)信息隐藏技术的背景、研究意义，国内外研究现状，信息隐藏技术的基本原理，信息隐藏技术的术语和模型，信息隐藏系统的基本属性，信息隐藏技术的分支及其应用。

(2)数字图像处理的基本概念和知识， 空域隐藏算法[5]，变换域隐藏算法[6]。着重讨论了基于离散余弦变换[9]的图像信息隐藏算法及其应用。

2 信息隐藏技术概述

信息隐藏技术作为一个新兴的研究领域，横跨数字信号处理、图像处理、语音处理、模式识别、数字通信、多媒体技术、密码学等多个学科。它把一个有意义的信息(如含有版权信息的图像)通过某种嵌入算法隐藏到载体信息中，从而得到隐密载体，非法者不知道这个载体信息中是否隐藏了其它的信息，而且即使知道，也难以提取或去除隐藏的信息。隐密载体通过信道到达接收方后，接收方通过检测器利用密钥从中恢复或检测出隐藏的秘密信息。本章首先指出了信息隐藏技术的依据，通过与信息加密作比较，介绍了信息隐藏技术的基本原理，然后描述了信息隐藏技术的术语和模型、信息隐藏系统的基本属性，最后介绍了信息隐藏技术的分支及其实际应用。

2.1 信息隐藏技术的基本原理

2.1.1 信息隐藏技术的依据

信息隐藏技术通常使用文字、图像、声音及视频等作为载体，信息之所以能够隐藏在多媒体数据中，主要是利用了多媒体信息的时间或空间冗余性和人对信息变化的掩蔽效应。

(1)多媒体信息本身存在很大的冗余性，从信息论的角度看，未压缩的多媒体信息的编码效率是很低的，所以将某些信息嵌入到多媒体信息中进行秘密传送是完全可行的，并不会影响多媒体信息本身的传送和使用。

(2)人的视觉或听觉感官系统对某些信息都有一定的掩蔽效应。在亮度有变化的边缘上，该边界“掩蔽”了边缘邻近像素的信号感觉，使人的感觉变得不灵敏、不准确，这就是视觉掩蔽效应。通常人眼对灰度的分辨率只有几十个灰度级，对边缘附近的信息不敏感。利用这些特点，可以很好地将信息隐藏而不被觉察。

2.1.2 信息隐藏与信息加密原理比较

信息隐藏与信息加密都是把对信息的保护转化为对密钥的保护，因此信息隐藏技术沿用了传统加密技术的一些基本思想和概念，但两者采用的保护信息的手段不同。信息加密是把有意义的信息加密为随机的乱码，如图2.1所示，窃听者知道截获的密文中可能包含重要的信息，但无法破译。

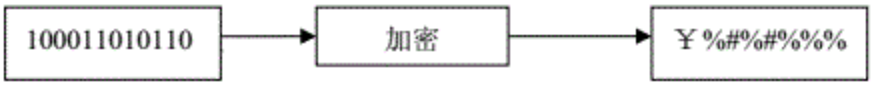

图2.1 信息加密示意图

信息隐藏则是把一个有意义的信息隐藏在另一个称为载体的普通信息中得到隐密载体，然后通过普通信息的传输来传递秘密信息。如图 2.2 所示。非法者不知道这个普通信息中是否隐藏了其他的信息，而且即使知道，也难以提取隐藏的信息。

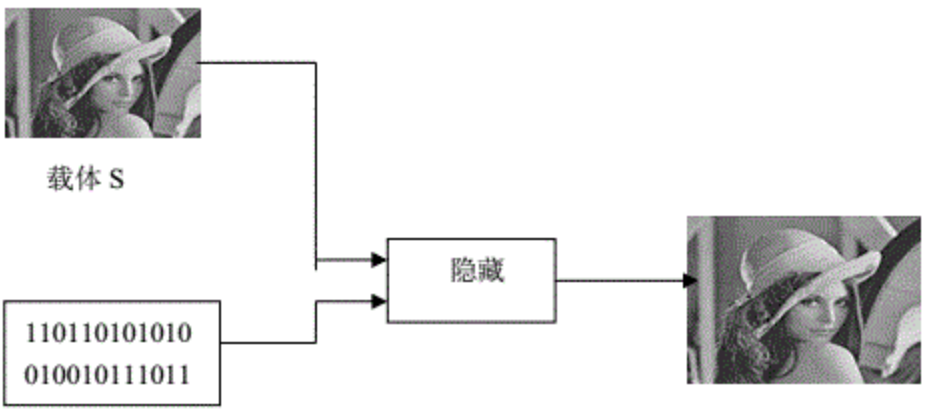

图 2.2 信息隐藏示意图

为了增加破译的难度，进一步提高秘密信息的安全性，还可以把加密技术和隐藏技术相结合，即先对消息M加密得到密文C，再把C隐藏到载体S中，如图2.3所示。

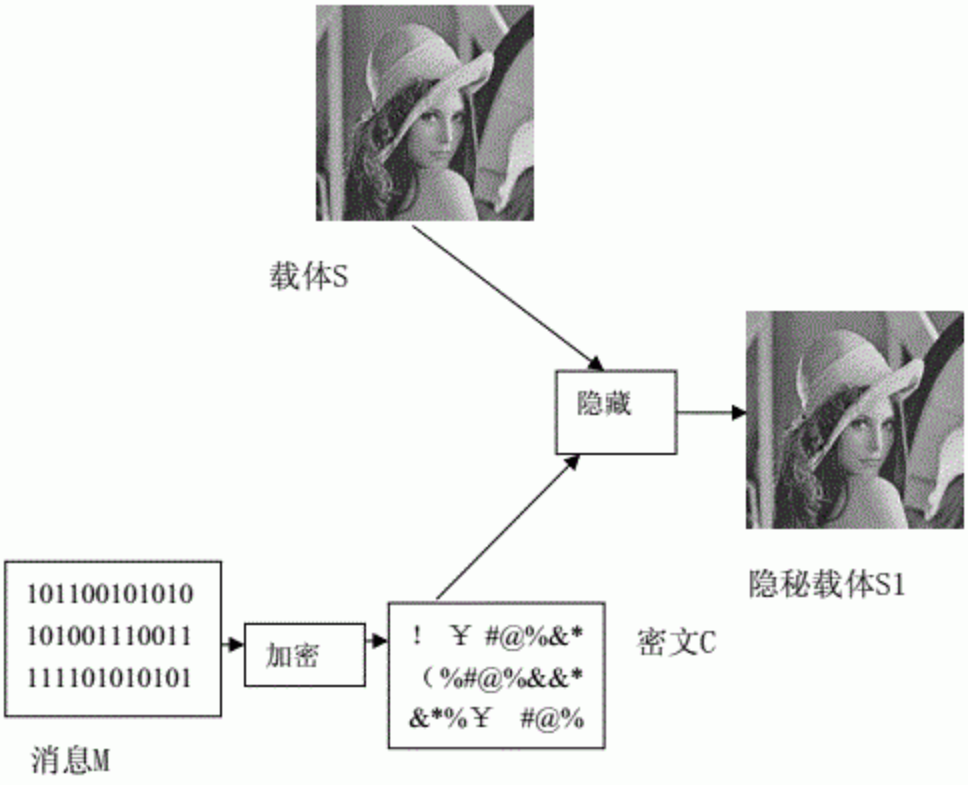

图2.3 信息加密和隐藏结合示意图

这样，攻击者要想获得消息，就首先要检测到消息的存在，并知道如何从隐密载体S1中提取C及如何对C解密以恢复消息M。

2.2 信息隐藏技术的术语和模型

一个信息隐藏系统的一般化模型可用图2.4表示。我们称待隐藏的信息为秘密信息(secretmessage)，它可以是版权信息或秘密数据，也可以是一个序列号；称公开信息为载体信息(cover message)，这种信息隐藏过程一般由密钥(Key)来控制，通过嵌入算法(Embedding algorithm)将秘密信息隐藏于公开信息中形成隐蔽载体(stego cover)，隐蔽载体则通过信道(Communication channel)传递，然后检测器(Detector)利用密钥从隐蔽载体中恢复/检测秘密信息

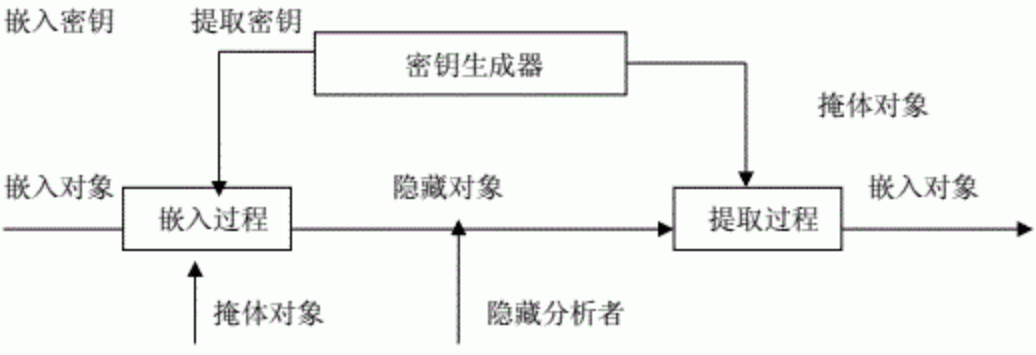

图 2.4 信息隐藏系统的一般模型

该系统主要包括一个嵌入过程和一个提取过程，其中嵌入过程是指信息隐藏者利用嵌入算法，将秘密信息添加到掩体对象中，从而生成隐藏对象这一过程。隐藏对象在传输过程中可能被隐藏分析者截获并进行处理。提取过程是指利用提取算法从接收到的、可能经过修改的隐藏对象中恢复秘密信息，提取过程中可能需要掩体对象的参与，也可能不需要，通常前者称为非盲提取，后者称为盲提取。

该模型中没有包括对秘密信息的预处理和提取后的后处理，在有些情况下，为了提高保密性需要预先对秘密信息进行预处理(例如加密)，相应地在提取过程后要对得到的信息进行后处理(例如解密)，恢复出秘密信息。

2.3 信息隐藏系统的基本属性

信息隐藏系统有三个基本属性包括：不可感知性、鲁棒性和嵌入量。

(1)不可感知性(Invisibility)，也称透明性，隐蔽性，是指嵌入信息的操作不应使原始载体信息的质量有明显下降，即不产生明显的信息嵌入痕迹，使得在通信过程中的携带秘密信息的载体不会引起第三方的怀疑。信息隐藏的不可感知性是信息隐藏的根本属性，“隐”就是不可感知的意思。只有将秘密信息隐藏到载体数据中进行传输，才有可能起到保护作用，所以不可感知性是秘密信息安全传输的前提。

(2)鲁棒性(Robustness)，也称稳健性，指信息隐藏系统抵抗由正常信号处理引入的失真和由恶意攻击操作所造成的数据畸变的能力，包括传输过程中的信道噪声、滤波操作、重采样、有损编码压缩、D / A或A / D转换等。鲁棒性强调信息传输的可靠性。

(3)嵌入量(Capacity)，指承载信息的载体可以容纳秘密信息的多少。通常以秘密信息大小与载体信息大小之比来表示。嵌入量考虑的是传输的信息量。不可感知性、鲁棒性和嵌入量从根本上决定信息隐藏系统性能的三个属性，三者之间是一个矛盾的统一体，它们彼此之间相互制约，并且在一定条件下可以相互转化。例如，鲁棒性与嵌入强度有直接关系，嵌入强度越大鲁棒性越强，但往往大强度的信号调制会导致不可感知性的下降; 同样，嵌入量的增加往往导致对原始载体信息的修改增加，也会使得不可感知性下降。在转化方面，增加密文信号的冗余或带宽会提高鲁棒性，而这是以牺牲嵌入量为代价。实践往往要根据具体应用模式在三者之间寻求适当平衡点。

对于数字水印来说，上述三项性能的重要性排序是鲁棒性、不可感知性、嵌入量。鲁棒性意味着水印不能被干扰或恶意处理去除，这是版权确认的保证，因此最重要；隐蔽性保证了数字产品的商用价值；至于嵌入量，只要能够标识一些必要的信息，并没有过高的要求。而对于隐写来说，这三项性能的重要性排序是隐蔽性、嵌入量、稳健性。隐蔽性包括视／听觉隐蔽性和统计上的隐蔽性，意味着监控者无法察觉，所以最重要；隐蔽通信往往高传输率，战争状态下还要求实时传送，故嵌入量其次；隐写通常应用于无扰信道，所以对稳健性的要求最低。正是由于信息隐藏基本特性之间相互依赖相互制约的特点，造就了信息隐藏技术的多样性和复杂性。

2.4 信息隐藏技术的分支

在1996年召开的第一届信息隐藏技术的国际学术会议上，对信息隐藏的术语进行了统一和规范，提出了信息隐藏学科的框架与分支，如图2.5所示。

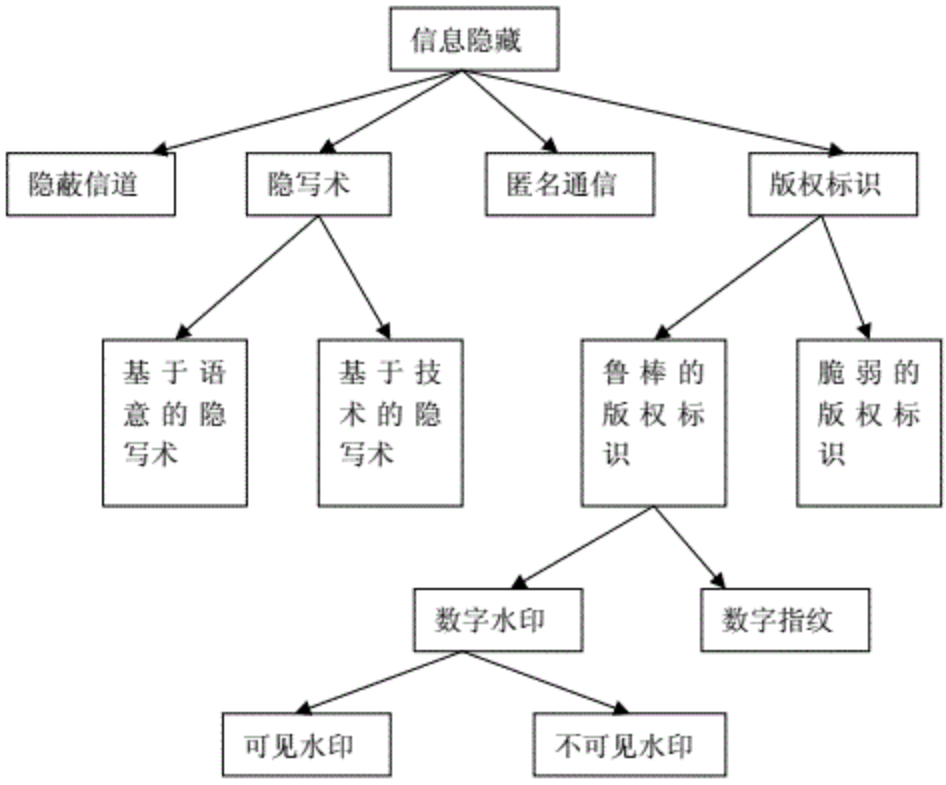

图 2.5 信息隐藏的主要分支

信息隐藏的四个主要分支包括：隐蔽信道(Covert channel)、匿名通信(Anonymity)、隐写术(Steganography)和版权标识(Copyright marking)。

尽管信息隐藏技术有诸多分支，但真正活跃的信息隐藏技术主要有两个，即

隐写术和数字水印(Digital watermarking)，也就是前面所指的版权标识(Copyright marking)。前者旨在保护秘密信息的安全传输，主要应用于隐蔽通信；后者目的在于保护载体本身的属性，主要用来进行知识产权保护。与密码学和密码分析学的交错发展相类似，随着信息隐藏研究的不断深入，与信息隐藏相对抗的信息隐藏攻击检测研究也开始出现，并逐步成为信息隐藏研究中的又一重要分支。依照检测手段把检测方法进行了分类，对当前几种主要的信息隐藏检测算法进行了详细的介绍。

2.5 信息隐藏技术的应用

信息隐藏技术在政府、军事情报部门、银行系统、商业系统等诸多领域发挥着重要作用，广泛应用于通信保密、数字作品的版权保护、商务活动中的票据防伪、验证资料的完整性等方面。

(1)隐蔽通道通信

隐蔽信道是一种通讯信道，它存在于计算机系统中，其特点是信息的传递方式违背了系统的安全原则，从而成为一个隐蔽的信息传输通道。这些信道在为某一程序提供服务时，可以被一个可信赖的程序用来向它们的操作者泄露消息。

(2)匿名技术通信

匿名技术是不暴露身份和个人特征的一种技术，该技术主要应用于网络环境下。网络匿名可分为发送方匿名和接受方匿名，分别保护通信双方的身份，所使用的主要技术有匿名重发和网络代理等。

(3)秘密通信

最初信息隐藏技术主要用来进行秘密传递消息，它隐藏了通信收发双方以及通信过程的存在，而且隐藏后的信息可以通过公开信道进行传输，不用担心信息被截获和破译。运用信息隐藏技术可以对那些涉及国家安全的军用卫星图片、军用设施图纸、电子商务的敏感信息、重要文件的数字签名以及个人隐私等秘密信息进行保密，确保这些信息在互联网上被安全、快捷地传递与使用。它同时也可以用于个人、商业机密信息的保护、电子商务中的数据传递、网络金融交易重要信息的传递以及个人的电子邮件业务保护等。

(4)数字作品的版权保护

现代信息社会，各种数字服务，如数字图书馆、数字电视、数字新闻等，为

人们的工作、学习和生活带来了方便和快捷。但与此同时，对数字作品的版权保护日益成为迫切需要解决的问题。为了保护数字服务提供商的正当利益，抵制未经授权的拷贝和发行，信息隐藏技术中的“数字水印”、“数字指纹”等将著作权、公司标志、有特殊意义的文本、购买者序列号等重要信息嵌入数字视频、声频或图像等多媒体数据中，以防止非法拷贝或者用来跟踪、追查盗版者及盗版产品的出处。目前，该技术已被广泛应用于MP3和网上图像的版权保护。

(5)资料认证和篡改检测

当数字作品被用于交通、法庭、医学、新闻及商业时，如以数字形式记录的事故现场照片、犯罪现场记录、医学诊断照片等，由于这些数据本身具有容易修改的特点，常常需要确定它们的内容是否被篡改、伪造或经过特殊处理。通过采用嵌入脆弱水印的方法，将一些与介质内容或作者身份相关的数据信息嵌入到数字媒体中，一旦资料被篡改，水印就被破坏，这样，通过提取验证水印，就可以检测出介质是否被篡改，从而验证资料的完整性。

(6)商务活动中的票据防伪票据防伪是在彩色打印机、复印机输出的每幅图像中嵌入唯一的、不可见的数字水印。当需要时，可以通过实时地扫描票据来判断水印的有无，辨别票据的真伪。

(7)抗否认机制

抗否认机制一般用在电子商务中，这是保证一些个体或单位不能否认自己曾经产生的一些行为。在电子商务中，交易双方的任何方不得抵赖自己曾经做出的行为，也不能否认曾经接受到对方的信息，这是网络电子交易的重要环节。日前电子商务中，一般用数字签名和身份认证来保证。这时我们可以采用信息隐藏技术，在交易双方的任何一方发送或者接收信息时，必须把自己的数字签名和身份信息、以二进制的方式嵌入到要传递的信息中去。接收方在收到后对它的签名进行认证。一般来说，在嵌入这类信息时，同时要加上时间戳作为另外一层防护。

3 图像信息隐藏技术

目前信息隐藏研究中使用的载体信息有几种：文本、图像、语音信号、视频信号和应用软件。数字图像由于大量存在，因而被研究最多的是图像中的信息隐藏，而且，图像信息隐藏所研究的方法往往经过改进可以轻易地移植到其他的载体中。在国内15种有关图像工程的重要中文期刊中关于图像和信息隐藏的文献，2003年有49篇，2004年有57篇，2005年有48篇，信息隐藏已成为图像技术中的一个重要研究热点。

用于进行隐蔽通信的图像信息隐藏算法可以分为两大类：基于空域的信息隐藏算法和基于变换域的信息隐藏算法。基于空域信息隐藏算法中的典型算法是LSB算法，该算法的主要特点是在载体图像中嵌入的隐藏信息数据量大，但是嵌入位置固定，安全性差，嵌入的隐藏信息易被破坏，鲁棒性不高；基于变换域信息隐藏算法中的典型算法是离散余弦变换域的信息隐藏算法，该算法嵌入信息能够抵御多种攻击，具有较好的鲁棒性，并且嵌入方式多种多样，增加了攻击者提取的难度，具有一定的安全性，但是该类算法嵌入的隐藏信息数据量较小，不适合于进行大数据量的隐蔽通信。

本章首先介绍了图像的定义和类型，图像的数字化处理过程，灰度直方图的概念和作用，常用的颜色模型，讨论了图像质量评价方法；然后讨论了两种空域隐藏算法：LSB替换算法和基于统计的信息隐藏算法；接着介绍了变换域隐藏算法的原理和优越性，在此基础上讨论了基于离散傅里叶变换的图像信息隐藏算法、基于离散余弦变换(DCT)的图像信息隐藏算法、基于离散小波变换的图像信息隐藏算法，对基于离散余弦变换(DCT)的图像信息隐藏算法做了详细的论述，给出了算法流程、程序和实例效果。

3.1 数字图像处理的基本概念和知识

3.1.1 图像

图像是用各种观测系统以不同形式和手段观测客观世界而获得的，可以直接或间接作用于人眼并进而产生视知觉的实体。人的视觉系统(HVS：human

Vision system)就是一个观测系统，通过它得到的图像就是客观景物在人心目中形成的影像。视觉是人类从大自然中获取信息的最主要的手段。据统计，在人类获取得信息中，视觉信息约占60%，听觉信息约占20%，其他方式获取的信息加起来约占20%。由此可见，视觉信息对人类非常重要。同时，图像又是人类获取视觉信息的主要途径，是人类能体验的最重要、最丰富、信息量最大的信息源。

一幅图像包含了它所表示的物体的有关信息，在较广的定义下，图像也包括人眼不能感知的各种“表示”。图像可根据其形式或产生方法来分类。为此，引入一个集合论的方法，将图像的类型用图3.1来表示。

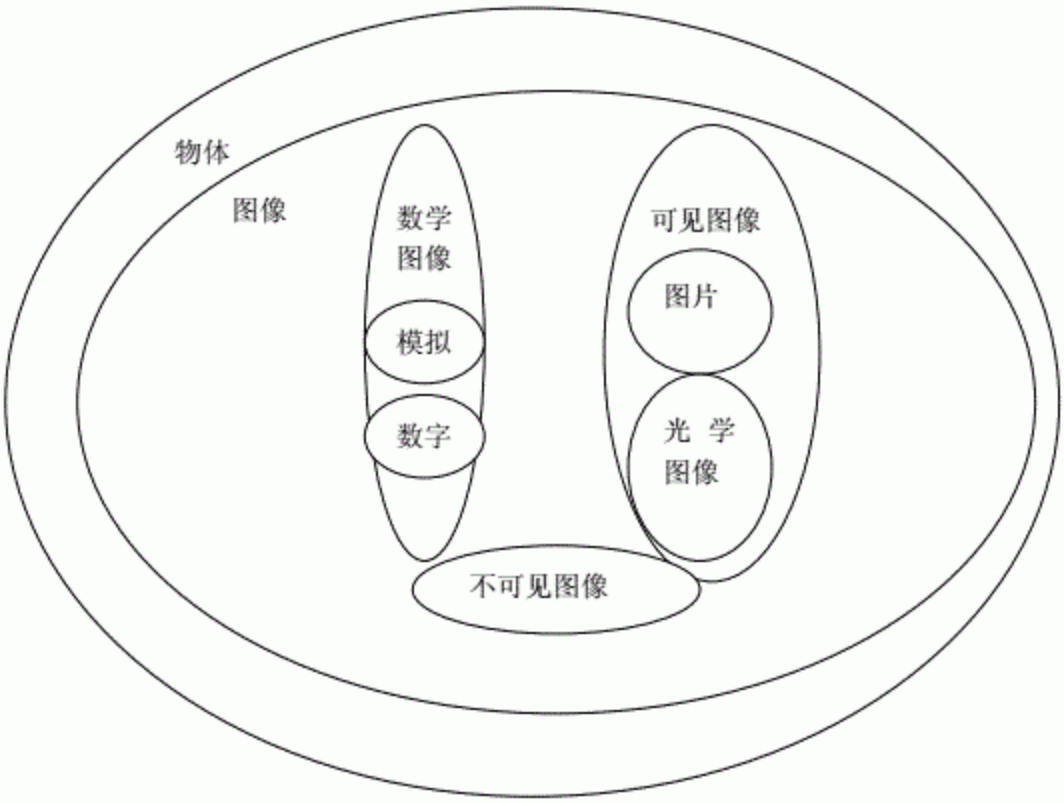

图 3.1 图像的模型

在图像集合中，包含了所有可见的图像(visible image)，即可由人眼看见的图像的子集，在该子集中又包含几种不同方法产生的图像的子集，一个子集为图片(picture)，它包括照片(photograph)、图(drawing)和画(painting)。另一个子集为光学图像(optical image)，即用透镜、光栅和全息技术产生的图像。图像的另一个子集是由连续函数和离散函数组成的抽象的数学图像，其中后一种是能被计算机处理的数字图像(digital image)。

客观世界在空间上是三维的，但一般从客观景物得到的图像是二维的。一幅图像可以用一个二维函数f(x,y)来表示，也可看作是一个二维数组，x和y表示二维空间XY中一个坐标点的位置，代表图像在点(x,y)的某种性质F的数值，例如一种常用的图像是灰度图(如图3.2)，此时f表示灰度值，它对应客观景物被观察到的亮度。

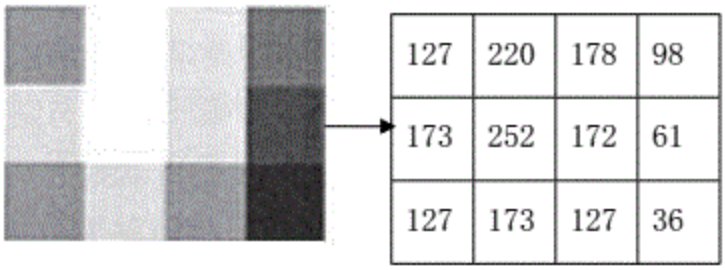

图 3.2 灰度图像及其函数表示

日常见到的图像多是连续的，有时又称之为模拟图像，即f,x和y的值可以是任意实数。为了便于计算机处理和存储，需要将连续的图像在坐标空间XY和性质空间F都离散化。这种离散化的图像就是数字图像(digital image)，可以用I(r,c)来表示。其中，r代表图像的行(row)，c代表图像的列(column)。这里I,r,c的值都是整数。在不致引起混淆的情况下我们仍用．f(x,y)表示数字图像,f,x和y都在整数集合中取值。

3.1.2 图像的数字化处理

实际的图像具有连续的形式，但必须经过数字化变成离散的形式，才能在计算机中存储和运算。数字化包括采样和量化两个步骤。采样就是用一个有限的数字阵列来表示一幅连续的图像，阵列中的每一个点对应的区域为“采样点”，又称为图像基元(picture element)，简称为像素(pixel)。采样时要满足“采样定理”。这个过程是通过扫描实现的，输出的量是连续的电平。“量化”就是对这个模拟输出量取离散整数值，这个过程用A/D器件实现。

1．图像的采样

图像采样的常见方式是均匀的矩形网格，如图3.3所示，将平面(x,y)沿x方向和y方向分别以△x和△y为间隔均匀地进行矩形的划分，采样点为x=i△x　y=j△y于是连续图像f(x,y)对应的离散图像f1(x,y)可表示为（3-1）

$$f_d(x,y)=\begin{cases} f_c(x,y), & x=i\Delta x, y=i\Delta y \\ 0 \end{cases} \tag{3-1}$$

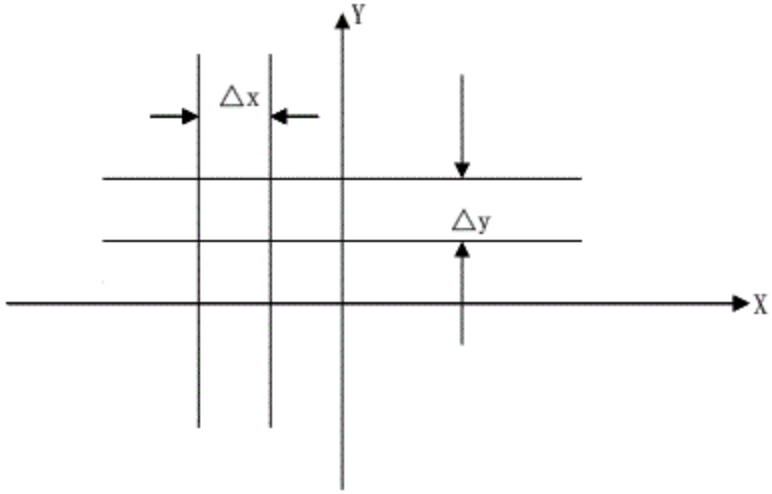

图3.3 典型的矩阵网格采样方式

2．图像的量化

经过采样后，模拟图像已被分解成空间上离散的像素，但这些像素的取值仍然是连续量。量化就是把采样点上表示亮暗信息的连续量离散化后，用数字来表示。根据人眼的视觉特性，为了使量化后恢复的图像具有良好的视觉效果，通常需要 100 多个量化等级。为了计算机的表达方便，通常取为 2 的整数次幂，如 256、128 等。图 3.4 所示是量化操作的示意图。

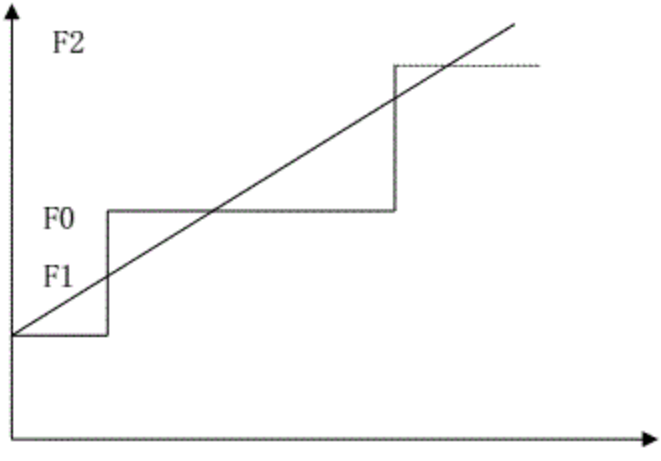

图3.4 量化示意图

将连续图像的像素值分布在[f1,f2]范围内的点的取值量化为f0，称之为灰度值和灰阶。把真实值f和量化值f0 之差称为量化误差。量化方法有两种。一般采用等间隔廊一量化，称之为均匀量化。对于像素灰度值在从黑到白的范围内较均匀分布的图像，这种量化可以得到较小的量化误差。另一种量化方法是非均匀

量化，它是依据一幅图像具体的灰度值分布的概率密度函数，按总的量化误差较小的原则来进行量化。具体做法是对图像中像素灰度值频繁出现的范围，量化间隔取小一些，而对那些像素灰度值极少出现的范围，则量化间隔取大一些。这样就可以在满足精度要求的情况下用较少的位数来表示。

3. 数字图像的表示

经过采样和量化操作，就可以得到一幅空间上表现为离散分布的有限个像素，灰度取值上表现为有限个离散的可能值的数字图像。数字化之后的图像用一个矩阵表示g=[g(x,y)]式中x、y是整数，且1≤x≤M，I≤Y≤N，表示矩阵的大小为M*N.其中M为采样的行数N为采样的列数。除了常见的矩阵形式外，在MATLAB运算等情况下，常将图像表示成一个向量：g=[g(1)g(2)…g(j)…g(N)]。式中，g(j)是行向量或列向量。向量g是把式中元素逐行或逐列串接起来形成的。

3.1.3 数字图像的灰度直方图

灰度直方图是数字图像的重要特征之一。它是关于灰度级分布的函数，反映一幅图像中各灰度级与各灰度级像素出现的频率之间的关系。灰度级为[0，L-1]的数字图像的灰度直方图通常用离散函数h(Rk)表示，定义如下：h(Rk)其中Rk为第k级灰度，Nk是图像中具有灰度级Rk的像素个数。显然0≤k≤L-1，0≤Nk≤n-1，n为图像总的像素数目。在图像处理中常用的是归一化的直方图P(Rk)。

$$p(R_k) = N_k / n \tag{3-2}$$

$$\sum_{k=0}^{L-1} P(R_k) = 1 \tag{3-3}$$

P(Rk)反映了图像中各个灰度级的分布概率，是能够反映图像整体特征的一个统计量。可以看出，直方图很直观地反映了图像的视觉效果。对于视觉效果良好的图像，它的像素灰度应该占据可利用的整个灰度范围，而且各灰度级分布均匀。值得一提的是，灰度直方图只能反映图像的灰度分布情况，而不能反映图像像素的位置，即丢失了像素的位置信息。图像的灰度直方图在信息隐藏技术中得到了重要的应用。提出了基于差分直方图实现LSB信息隐藏的可靠性检测方法，研究了一种基于频率域差分直方图能量分布的可对DFT域、DCT域和DWT域图像信息隐藏实现通用盲检测的方法。提出了基于空域直方图、频域直方图的无损数据隐藏方法。一个灰度直方图的例子如图3.5所示。

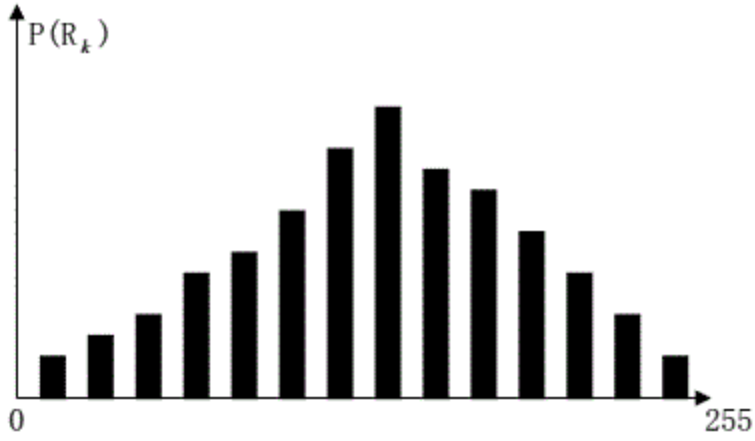

图 3.5 灰度直方图示例

3.1.4 常用颜色模型

所谓颜色模型就是指某个三维颜色空间中的一个可见光子集，它包含某个颜色域的所有颜色。常用的颜色模型可分为两类，一类面向诸如彩色显示器或打印机之类的硬设备，另一类面向以彩色处理为目的的应用。面向硬设备的最常用的模型是RGB模型，而面向彩色处理的最常用模型是HIS模型。这两种模型也是图像技术最常见的模型。

1. RGB模型

RGB颜色模型基于笛卡儿三维直角坐标系，3个轴分别为红、绿、蓝三基色，各个基色混合在一起可以产生复合色，如图3.6所示。RGB颜色模型通常采用图3.6所示的单位立方体来表示，在正方体的主对角线上，各原色的强度相等，产生由暗到明的白色，也就是不同的灰度值。(0,0,0)为黑色，(1,1,1)为白色。正方体的其它六个角点分别为红、黄、绿、青、蓝和品红。

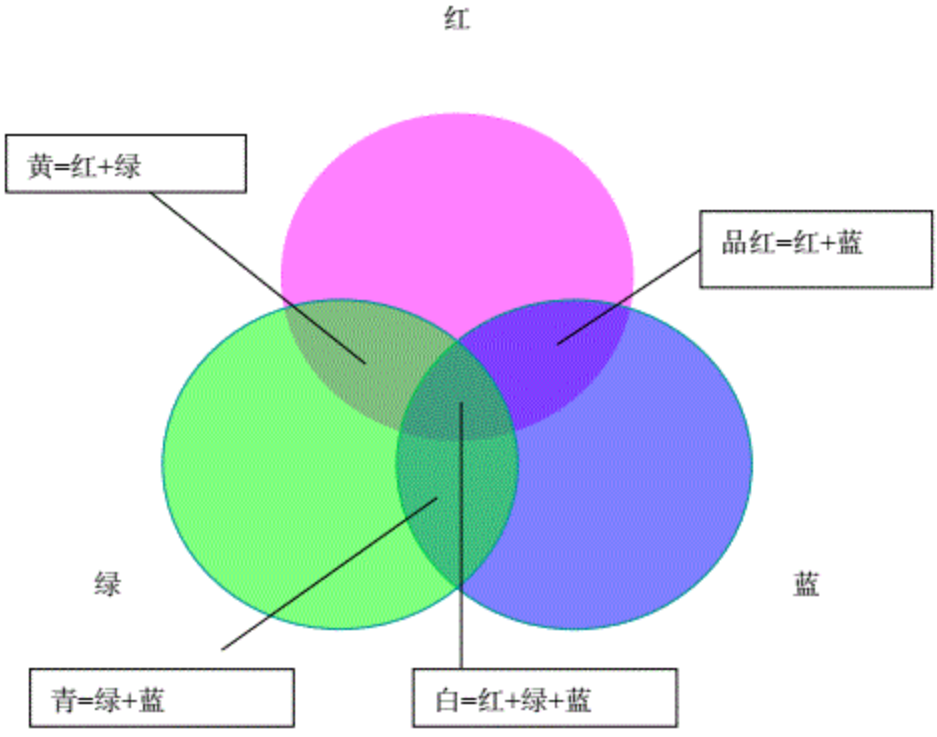

图3.6 RGB混合效果

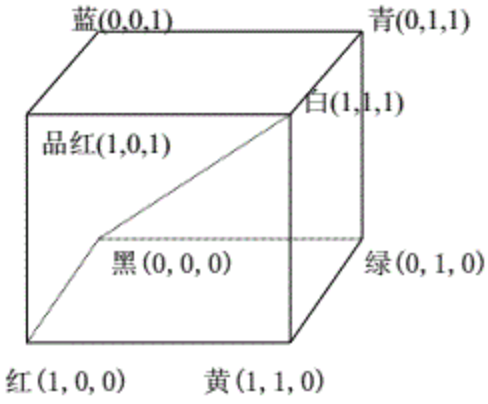

图3.7 RGB立方体

根据这个模型，一幅彩色图像每个像素的颜色都用三维空间的一个点来表示，由红、绿、蓝三基色以不同的比例相加混合而产生的。

$$C=aR+bG+cB \tag{3-3}$$

其中C为任意彩色光，a,b,c,为三基色R、G、B的权值。R、G、B的亮度值限定在[0-255]。

2．HSV模型

该模型对应于圆柱坐标系的一个圆锥形子集(图3.8)。圆锥的顶面对应于V=1，代表的颜色较亮。色彩H由绕V轴的旋转角给定，红色对应于角度0度，绿色对应于角度120度，蓝色对应于角度240度。在HSV颜色模型中，每一种颜色和它的补色相差180度。饱和度s取值从0到1，由圆心向圆周过渡。在圆锥的顶点处，V=0，H和S无定义，代表黑色，圆锥顶面中心处S=0，V=1，H无定义，代表白色，从该点到原点代表亮度渐暗的白色，即不同灰度的白色。任何V=1，S=1的颜色都是纯色。

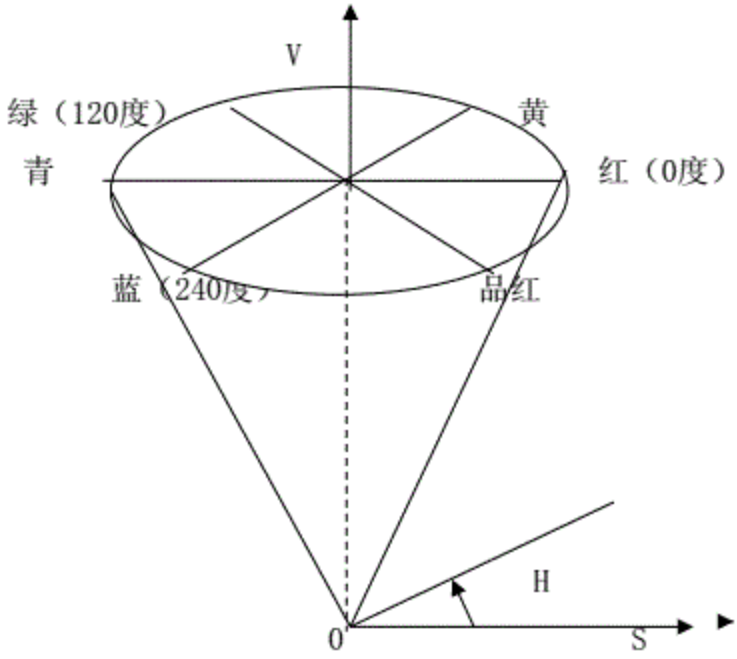

图3.8 HSV颜色模型

HSV颜色模型对应于画家的配色方法。画家用改变色浓和色深的方法来从某种纯色获得不同色调的颜色。其做法是：在一种纯色中加入白色以改变色浓，加入黑色以改变色深，同时加入不同比例的白色，黑色即可得到不同色调的颜色。如图3.9所示，为具有某个固定色彩的颜色三角形表示。

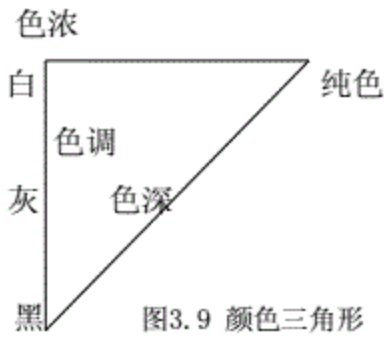

图3.9 颜色三角形

3.1.5 图像质量评价

图像质量评价的研究是图像信息工程的基础技术之一。在图像通信中，将图像传输到接收端，其中要经过采集、传输、处理、记录等过程，所有这些技术的优劣都会影响到图像质量。图像处理中的编码技术，就是在保持编码图像一定质量的前提下，以尽可能少的比特数来表示图像。以便节省信道有效带宽或存储器的容量。数字图像信息隐藏系统中也必须对隐藏算法中得到的隐密公开图像和解密算法中得到的恢复图像质量进行评价。

图像质量的含义包括两个方面，一是图像的逼真度(fidelity)，另一个是图像的可懂度(intelligibility)。逼真度是指评价图像与标准图像的偏离程度，图像的可懂度则是表示图像能向人或计算机提供信息的能力。由于人们对图像质量的评价受到诸如观察环境、观察者的视觉心理和精神状态以及观察者与视觉场景相互作用的程度等因素的影响，逼真度和可懂度的定量分析方法是个很困难的课题，虽然取得了一些进展，但是还没有很好的解决。因此，对图像质量的评价方法工程中采用的还是主观评价法，在一些特定应用背景，如图像复原中，才采用定量分析。

1．图像的客观质量评价方法

客观评价是用隐密图像(或恢复图像)偏离原始图像的误差来衡量隐密图像(或恢复图像)的质量。最常用的有均方根误差(RMSE：Root Mean Squared Error)和峰值信噪比(PSNR：Peak Signal to Noise Ratio)，它们的表达式为

$$RMSE=\sqrt{\frac{\sum_{x=1}^{M}\sum_{y=1}^{N}[g(x,y)-f(x,y)]^2}{M\times N}} \tag{3-4}$$

$$PSNR=10\lg\frac{M\times N\times 256\times 256}{\sum_{x=1}^{M}\sum_{y=1}^{N}[g(x,y)-f(x,y)]^2} \tag{3-5}$$

其中，f(x，y)和g(x，y)分别表示原始图像和隐密图像(或恢复图像)，M,N分表示图像的宽与高，且x=1,2，．．M，y=1,2，．．．，N。RMSE越小，说明两幅图像差别越小，即两者越相似。峰值信噪比PSNR越大，说明图像的保真度越好，两幅图像越相似。PSNR本质上与MSE相同，其关系表达式为式(3-4)和式(3-5)看起来直观、严格，但用它们所求得的结果常与人们的主观视觉效果不一致。这是

因为均方根误差和峰值信噪比是从总体上反映原始图像和隐密图像(或恢复图像)的差别，并不能反映一幅图像中少数像素点有较大灰度差别和较多像素点有较小灰度差别等各种情况。显然，客观质量评价采用式(3-4)和式(3-5)对图像中所有像素点同样对待，不能全面反映人眼的视觉特性。

2．图像的主观质量评价方法

主观评价方法就是让一群观察者根据一些事先规定的评价尺度或自己的经验，对测试图像按视觉效果提出质量判断，并给出质量分数，对所有观察者给出的分数进行加权平均，所得的结果即为图像的主观质量评价。

主观评价主要有两种度量尺度，即绝对尺度和相对尺度，如表3．1所示。这种测量方法虽然较好地反映出了图像的直观质量，但无法应用数学模型对其进行描述，且该方法操作复杂，在实际应用中，不能应用于实时传输的场合。在有些应用场合需要将主观评价和客观评价结合起来，后面讨论的信息隐藏系统就是如此。

表3-1 主观质量测量尺度

级别	绝对测量尺度	相对测量尺度
1	很好	一批中最好的
2	较好	比该批中平均水平好
3	一般	该批中平均水平
4	较差	比该批平均水平差
5	很差	该批中最差的

3．新的质量评价方法

随着图像处理技术的发展，图像质量评价方法的研究已从以往的简单误差统计方法发展到结合人眼视觉特性(HSV)的误差统计方法。

(1)基于视觉感知的图像质量评价方法

图像质量对人眼视觉的影响是由人眼视觉系统的灵敏度决定的，而视觉灵敏度是由人眼的视觉细胞决定的。此外，人眼视觉系统的灵敏度还受到图像局部空间频率的影响，大量实验结果证明：影响像素误差可视度的因素是误差周围的局部区域环境，而不是整个图像的背景环境。根据上述视觉特性，典型的HVS模型模拟了视觉感知的3个显著特性，即视觉非线性特性(Weber定律)、视觉敏感度带通和视觉多通道及掩盖效应。

2．基于视觉兴趣的图像质量评价方法

从视觉心理学角度看，视觉是一种积极的感受行为，不仅与生理因素有关，还在相当大的程度上取决于心理因素。人们在观察和理解图像时，往往会不自觉地对其中某些区域产生兴趣，这些区域被称为“感兴趣区”(ROI，Region Of Interest)。整幅图像的视觉质量往往取决于ROI的质量，而非ROI的降质有时不易觉察。一种基于视觉兴趣的图像质量评价方法为：通过对图像中不同区域的加权突出人眼对ROI的兴趣程度，近似认为人眼对ROI的兴趣程度与其面积成反比。

3.2 空域(Spatial Domain)隐藏算法

空域隐藏技术是指将秘密信息嵌入数字图像的空间域中，即对像素灰度值进行修改以隐藏秘密信息。

3.2.1 LSB 替换算法

最低有效位(Least Significant Bits，LSB)方法是最早提出来的最基本的空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改进扩展的，使得LSB方法成为使用最为广泛的隐藏技术之一。现在有一些简单的信息隐藏软件大多是运用LSB和调色板调整等相关技术将信息隐藏在24bit图像或256色图像中，如Hide and Seek，Stego Dos，White Noise Storm，S-tools等经典信息隐藏软件。

1．隐藏原理

LSB方法通过调整载体图像像素值的最低若干有效位来来实现数据的嵌入，使所隐藏信息在视觉上很难被发觉，而且只有知道秘密信息嵌入的位置才能正确提取出秘密信息。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24bit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。

另外，在LSB方法中，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：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. 数据嵌入量

对于24bit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，那么可以隐藏的信息率为3/24=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。

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：1/8，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. 鲁棒性分析

LSB算法具有非常弱的鲁棒性。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。因为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。

几何交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。

3.2.2. 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。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。因此，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。

Bander等人提出的Patchwork算法是一种基于统计特性的信息隐藏算法。该算法在载体图像中利用伪随机数选择N对像素点，然后针对每个像素点的亮度值，使得整幅图像的平均亮度保持不变。也就是说，该算法假设任意像素之差是零，均值随机变量，任选N对像素，增加对比度而不改变平均亮度，使该均值偏移而隐藏信息。

陈默等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，把它运用到信息隐藏过程中去，提出了基于平坦测度的隐藏方法，同样取得了较好的隐藏效果。张涛等人提出了基于图像平滑度的空域LSB嵌入的检测算法，该文献对图像像素值与邻域均值的差的分布进行建模，以该分布的方差定义了图像平滑度的概念，进而通过对消息嵌入、LSB平面取反带来的图像平滑度的变化进行分析，提出了针对空域LSB替换伪装算法的秘密消息长度估计算法，该算法可以准确地估计图像中嵌入的秘密信息数据量的大小，计算速度快，有利于实现实时检测。

此外，伪随机置换、图象降质和秘密信道、将信息编码在基十调色板图象中、量化和抖动、失真技术等也都是空域法中的主要方法。总体上来看，空间域算法简单、计算速度快、隐藏信息量大，且一般可以实现盲提取，但鲁棒性较差，对于载体图像的压缩、噪声扰动等攻击的抵抗力较弱。

3.3 变换域(Trans of Formation Domain)隐藏算法

3.3.1 变换域算法原理

变换域隐藏技术就是指将秘密信息嵌入数字图像的某一变换域中。比较常用的是离散傅立叶变换(DFT)、离散余弦变换(DCT)和离散小波变换(DWT)等，它们主要是通过修改载体图像某些指定的频域系数来嵌入数据。其基本思想是利用扩频通信原理来提高隐藏系统的鲁棒性。考虑到对低频区域系数的改动可能会影响到载体图像的感知效果，而高频系数又易被破坏，因此，信息隐藏技术一般选取载体图像中频区域上的系数来嵌入秘密数据，从而使之既满足不可感知性，又满足对诸如失真压缩等操作的鲁棒性。

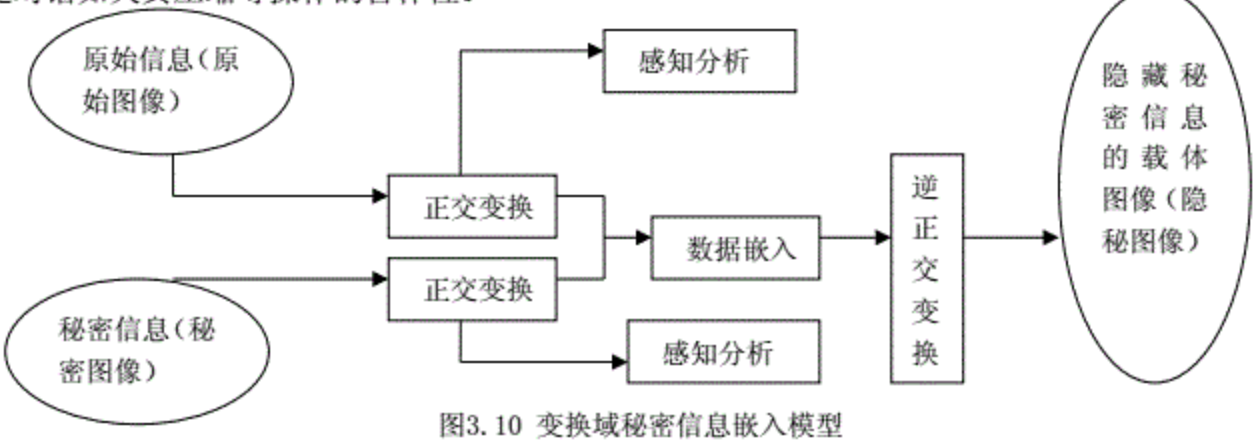

图3.10 变换域秘密信息嵌入模型

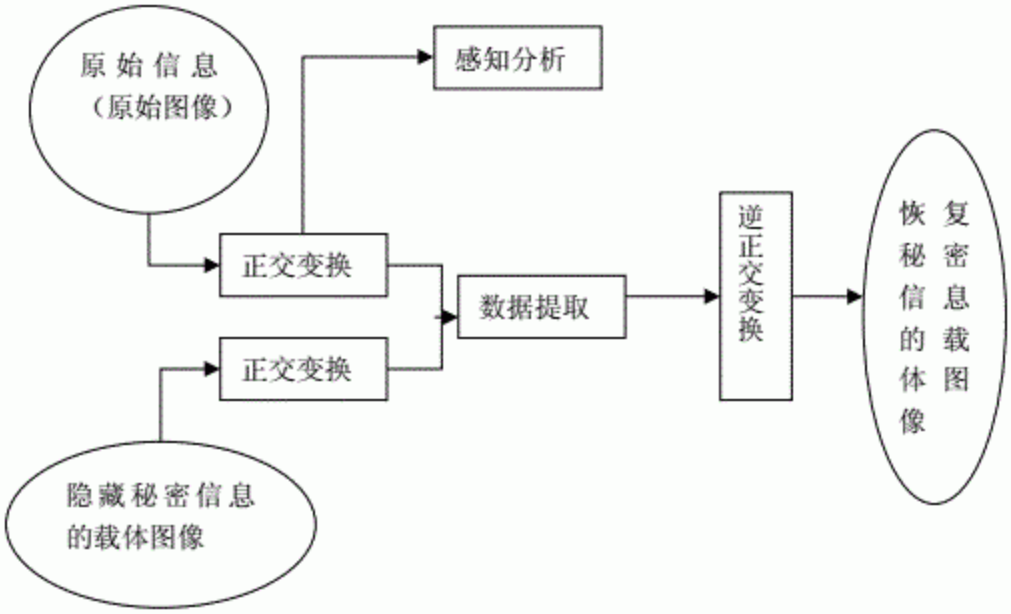

图3.11 变换域秘密信息提取模型

变换域信息隐藏算法的一般模型可用图3.10来表示，而变换域秘密信息提取算法的模型可用图3.11表示。

3.3.2 变换域算法的优点

由于变换域信息隐藏技术是在频域嵌入信息，因此它有频域所固有的抗攻击和变换的能力，使这一隐藏方案对比例变化、JPEG压缩、抖动、剪辑、打印/扫描以及合谋攻击都具有很好的鲁棒性。它的优点体现在以下几点：

(a)在变换域中嵌入的信号能量可以分布到空间域的所有像素上，有利于保证秘密信息的不可见性；

(b)在变换域中，人类视觉系统的某些特性(如频率掩蔽效应)可以更方便的结合到秘密信息编码过程中，提高算法的鲁棒性；

(c)交换域方法与大多数国际数据压缩标准兼容，从而可以直接实现压缩域内的隐藏算法，提高效率，同时，也能抵抗相应的有损压缩。

3.3.3 基于离散傅里叶变换(DFT)的图像信息隐藏算法

傅里叶(Joseph Fourier)变换是一种经典而有效的数学工具，在信号处理中有着广泛研究，在信息隐藏领域也同样得到了应用。它将图像分割成多个感觉频段，然后选择合适部分来嵌入秘密信息。提出基于原始图象的傅立叶变换，将调制后的秘密信息依次加入到某些固定位置的幅值谱上，利用傅里叶变换的可加性和图象去噪原理提出了一种基于频域的三维运动盲水印算法。傅里叶变换具有一些变

换无关的完整特性。例如：空间域的平移只引起频域上的相移，而幅度不变；空间域尺度的缩放会引起频域尺度反向的缩放；空间域旋转的角度和所引起的频域的旋转的角度是一致的。这些特点可以抵御诸如旋转、尺度、平移等几何攻击。

3.3.4 基于离散小波变换(DWT)的图像信息隐藏算法

小波分析(Wavelet Analysis)是自1986年以来由Y.Meyer S.Mattat和L.Daubechies等的奠基工作而发展起来的新兴学科，并迅速应用到图像和语音分析等众多领域的数学工具，是继110多年前建立傅立叶(Joseph Fourier)分析之后的一个重大突破。经过近二十年的努力，由多尺度分析、时频分析、金字塔算法等发展起来的小波理论基础已经基本建立并成为应用数学的一个新领域，引起了众多数学家和工程技术人员的极大关注，成为国际上科技学术界高度关注的前沿领域。图像分析和处理领域的专家认为小波分析是数字图像处理的空间一尺度分析(Space.Scale Analysis)和多分辨分析(Multiresolution Analysis)的有效工具。当前最新的图像压缩标准—JPEG2000和视频的MPEG7压缩标准都采用了小波变换。

基于压缩标准模型的信息隐藏算法可以很好的解决与这些标准的兼容问题，增强抵抗有损压缩攻击的能力。Xia Xiang.Gen等人较早地提出了基于离散小波变换(DWT)的信息隐藏方法。基于DWT域的图像信息隐藏算法的一般步骤为，首先对载体图像进行多级离散小波变换，得到不同分辨率下的细节子图和逼近子图，然后用秘密信息对DWT系数进行调制，最后对嵌入秘密信息后的小波系数进行相应级别的离散小波逆变换，完成信息隐藏过程。利用小波变换把原始图像分解成多频段的图像，能适应人眼的视觉特性且使得信息的嵌入和检测可分多个层次进行，小波变换域信息隐藏方法兼具时空域和DCT变换域方法的优点。因此，基于离散小波变换的信息隐藏算法已经成为当前研究的热点和最重要的研究方向。

目前，常见的几类小波变换域信息隐藏嵌入算法有：非自适应加性和乘性嵌入方式。例如针对JPEG2000基本压缩编码系统，通过自适应地选择嵌入点，提出一种基于冗余估算的小波域隐写算法；基于多分辨率嵌入方式。

3.4 基于离散余弦变换(DCT)的图像信息隐藏算法

离散余弦变换，简称DCT(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。早在上世纪末，COX等人较早地提出了基于DCT域信息隐藏方法。基于DCT域的图像信息隐藏算法的一般步骤为，

首先对载体图像分块进行二维DCT变换，然后用秘密信息对DCT系数进行调制，最后对新的系数作离散余弦反变换(IDCT)，即可得到隐藏图像，完成信息隐藏过程。基于DCT的信息隐藏算法因其具有较强的鲁棒性，计算量较小且与国际图像压缩标准(JPEG,MPEG,H.263,H.264等)相兼容(这些标准中均采用DCT变换)，因而具有诸多的潜在优势，成为近年来研究最多的一种信息隐藏技术，有大量的基于DCT变换域的信息隐藏算法涌现，结合DCT和DWT，提出将一幅秘密图像的DCT系数置乱后嵌入到公开图像的DWT系数中进行秘密信息的隐藏。

离散余弦变换属于正交变换图像编码方法中的一种。基于DCT的图像信息隐藏算法能够充分利用频域特性，将秘密信息分布到载体图像的各像素上，以提高算法的鲁棒性。

3.4.1 离散余弦变换(DCT)的定义

离散余弦变换是傅立叶变换的一种特殊情况。在傅里叶级数展开式中，如果被展开的函数是实偶函数，那么，其傅里叶级数中只包含余弦项，再将其离散化可导出离散余弦变换。在数字图像处理中，为了同时减弱或去除数字图像数据相关性，可应用二维离散余弦变换(2D.DCT)，将图像从空间域转换到DCT变换域。定义大小为M×N的图像f(x,y)的二维离散余弦变换F(u,v)为：

$$F(u,v)=\frac{2}{\sqrt{MN}}C(u)C(v)\sum_{x=0}^{M-1}\sum_{y=0}^{N-1}f(x,y)\cos\frac{(2x+1)u\pi}{2M}\cos\frac{(2y+1)v\pi}{2N} \tag{3-6}$$

二维离散余弦反变换(2D-IDCT)f(x,y)为：

$$f(x,y)=\frac{2}{\sqrt{MN}}\sum_{u=0}^{M-1}\sum_{v=0}^{N-1}C(u)C(v)F(u,v)\cos\frac{(2x+1)u\pi}{2M}\cos\frac{(2y+1)v\pi}{2N} \tag{3-7}$$

DCT变换相当于将图像分解到一组不同的空间频率上，F(u,v)即为每一个对应的空间频率成分在原图像中所占的比重；而反变换则是一个将这些不同空间频率上的分量合成为原图像的过程，变换系数F(u，v)在这个精确、完全的重构过程中规定了各频率成分所占分量的大小。在F(u，v)系数矩阵中，F(0，0)对应于图像f(x,y)的平均亮度，称为直流(DC)系数；其余的63个系数称为交流(AC)系数，从左向右表示水平空间频率增加的方向，从上向下表示垂直空间频率增加的方向。

3.4.2 基于 DCT 的图像信息隐藏算法流程

为了与JPEG压缩标准兼容，图像信息隐藏技术嵌入秘密信息时采用JPEG压缩标准中的DCT变换。基于图像DCT变换嵌入隐藏信息的流程如图3.12。

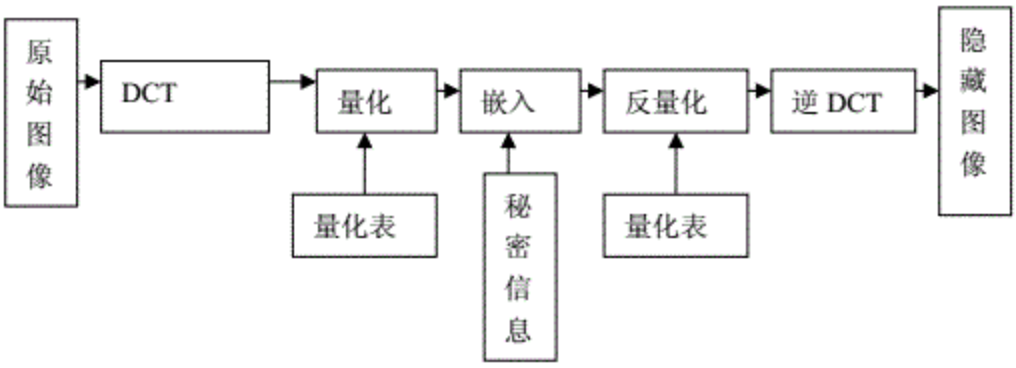

图3.12 基于图像DCT变换嵌入隐藏信息的流程图

基于图像DCT变换提取隐藏信息的流程如3.13所示。其过程为上述嵌入秘密信息算法的逆运算：先将隐密图像分割为互不重叠的8×8子块；对每一个子块进行DCT变换；然后对DCT变换后的系数进行嵌入算法的相反运算，得到提取的图像子块；最后将上面得到的所有图像子块合并成一个完整的图像。

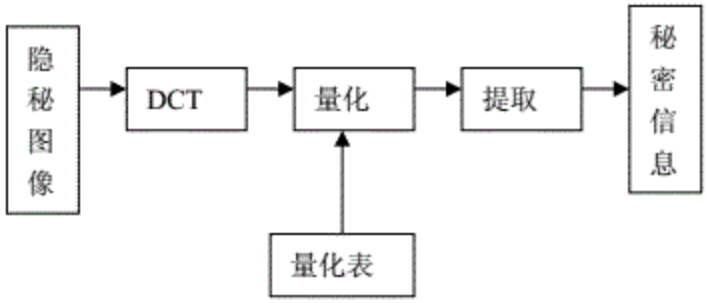

图3.13 基于图像DCT变换提取隐藏信息的流程图

3.4.3 基于 DCT 的图像信息隐藏嵌入区域的选取

DC分量，所示的DCT系数之字型排列表中第0个DCT系数。DC分量携带感知能量最大，嵌入秘密信息后，隐密图像产生强烈的块效应，隐蔽性很差。然而秘密信息嵌入在这个位置，在隐密图像受到有损压缩等攻击后，秘密信息受到的攻击很小，鲁棒性较好。总之用DCT系数嵌入秘密信息时，隐蔽性和鲁棒性是一对矛盾体，为了保证图像的质量，一般不用DC分量做嵌入位置。但大量事实证明，JPEG压缩标准中的图像经过DCT变换后再经过量化后，之字排列的0～63个DCT系数中，一般数值不为0的值多集中于左上角，DC分量一般不为0。低中频带中往往只有大约5个系数不为0，且对图像能量的影响较小。中高频带大部分系数为0。因此，兼顾嵌入秘密信息的隐蔽性和鲁棒性，低中频带可以考虑作为嵌入秘密信息的理想位置选择。中频带和高频带分量携带能量较少，从保证嵌入信息的隐蔽性角度

看是作为信息嵌入区域是好选择，但隐密图像中高频带中嵌入秘密信息很容易被有损压缩等攻击去除，鲁棒性很差。若用于数字水印，由于更注重嵌入秘密信息的鲁棒性，因此，可以利用低频带作为DCT域信息嵌入区域。若用于保密通信，由于更注重隐藏信息的隐蔽性，以及隐藏信息容量，则可以利用低中频带作为DCT域信息嵌入区域。比如选择之字型排列的0～63个DCT系数中序号为3～12的用来嵌入秘密信息。另外一种改进的方法可以考虑减小DCT变换后的量化步长，以增加AC分量中不为0的系数，增大嵌入秘密信息的容量。

4 信息隐藏实例

4.1 基于 DCT 的图像信息隐藏实例

离散余弦变换是一种实数域变换，基于 DCT 变换的编码方法是 JPEG 标准算法的核心内容，它主要包括编码和解码两个过程。

在对图像进行编码之前首先要对图像进行预处理，也就是把图像划分为数据

单元。在对图像进行处理时，有损模式下，通常 DCT 算法采用将 8×8 像素块作为一个数据单元，对 8×8 大小的图像数据块进行二维离散余弦变换。在编码器的输入端，把原始图像分割成一系列顺序排列的由 8×8 像点构成的数据子块。由于原始图像的采样数据是无符号整数，根据需要，要把其转换为有符号整数。

源图像的 8×8 数据块由 64 个像点构成，64 个像点实质上就是 64 个离散信号，输入后被分成 64 个正交基信号。每个正交基信号对应于 64 个独立二维空间频率中的一个。FDCT 即正变换输入 64 个基信号的幅值称作“DCT 系数”，即 DCT 变换系数。64 个变换系数中包括一个表示直流分量的“DC 系数”和 63 个表示交流分量的“AC 系数”。压缩数据的重要一步，就是对 DCT 系数进行量化，它是造成 DCT 编解码信号损失的根源。DCT 系数量化一般根据一张量化表提供的元素进行量化。量化表中的元素是根据人类的视觉特性制作的。

数字水印算法的实现基本上分为三个部分：水印的嵌入、水印的提取和相似度计算。

4.1.1 水印的嵌入

(1)首先对原始图像进行 DCT 变换。

(2)水印信号的产生。

Cox 等指出由高斯随机序列构成的水印信号具有良好的鲁棒性，在许多文献中也都是将高斯随机序列作为水印信号。因此本文所采用的水印信号 W 为服从正态分布 N (0, 1)，长度为 n 的实数随机序列。即:W=（Xi，0≦i≦n)。

(3)水印的嵌入。

选择将水印信号放在宿主信号的哪些位置，才能够更好的保证其具有良好的鲁棒性。Cox 等认为图像水印应该放在视觉上最重要的分量上。由于视觉上重要的分量是图像信号的主要成分，图像信号的大部分能量都集中在这些分量上，在图像有一定失真的情况下，仍然能保留主要成分，即视觉上重要的分量的抗干扰能力较强，因此将数字水印嵌入到这些分量上，可以获得较好的鲁棒性。当水印信号相对宿主信号较小时，还可以保证不可见性。所以本算法将服从 N (0, 1)分布的随机序列构成的水印序列放到 DCT 变换后图像的重要系数的幅度中，增强水印的鲁棒性。水印嵌入公式为(4-1)

$$V'=V(1+aX_k) \tag{4-1}$$

其中 V 为原始图像信息，a 为嵌入系数，X_K 为水印信息，V′为生成水印图像信息。

(4)进行二维离散余弦反变换，得到嵌入水印的图像，如图 4.1 所示。

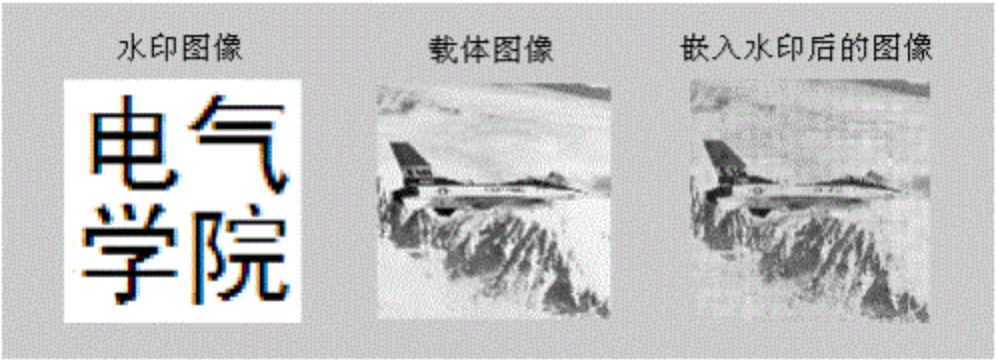

图 4.1 原始图像与嵌入水印后的图像对比

4.1.2 水印的提取

对原始图像和嵌入水印的图像分别进行离散余弦变换。利用 $X_k=(V'/V-1)/a$ 提取水印。从没有受到攻击的水印图像中提取出水印，与原始水印进行对比，如图 4.2 所示。

图 4.2 未受攻击的含水印图像提取的水印与原始水印图像比较

4.1.3 相似度和峰值信噪比计算

根据相似度的值即可判断图像中是否含有水印信号，从而达到版权保护的目的。对被恢复出的水印信号和原始水印信号的相似程度进行计算。MSE 指 Mean Square Error（均方误差，各值相差的 n 次方和的平均值的 n 次平方根）。

$$MSE = sum[(recpixel - orgpixel)^2] / ImageSize \quad (4\text{-}2)$$

PSNR 是“Peak Signal to Noise Ratio”的缩写。peak 的中文意思是顶点。而 radio 的意思是比率或比列的。整个意思就是到达噪音比率的顶点信号，PSNR 是

一般是用于最大值信号和背景噪音之间的一个工程项目。通常在经过影像压缩之后，输出的影像通常都会有某种程度与原始影像不一样。为了衡量经过处理后的影像品质，我们通常会参考 PSNR 值来认定某个处理程序够不够令人满意。

PSNR 计算公式如(4-3)所示

$$PSNR=10\times\log(255^2/MSE) \tag{4-3}$$

PSNR 的单位为 dB。所以 PSNR 值越大，就代表失真越少。

PSNR 是最普遍，最广泛使用的评鉴画质的客观量测法，不过许多实验结果都显示，PSNR 的分数无法和人眼看到的视觉品质完全一致，有可能 PSNR 较高者看起来反而比 PSNR 较低者差。这是因为人眼的视觉对于误差的敏感度并不是绝对的，其感知结果会受到许多因素的影响而产生变化（例如：人眼对空间频率较低的对比差异敏感度较高，人眼对亮度对比差异的敏感度较色度高，人眼对一个区域的感知结果会受到其周围邻近区域的影响）。

4.2 离散余弦变换阈的嵌入水印攻击实验

4.2.1 攻击实验类型及效果

数字水印技术的另一项重要指标就是考察对于已经实现水印嵌入的图象未检测时，看其对于原始的载体图象实行攻击后，水印的可承受度和载体图象以及提取水印的效果如何。就此指标，设计了如下的实验，在水印嵌入图象上，以不同的类型攻击，分析其性能。

对嵌入水印的图像进行攻击实验的菜单效果图如图 4.3：

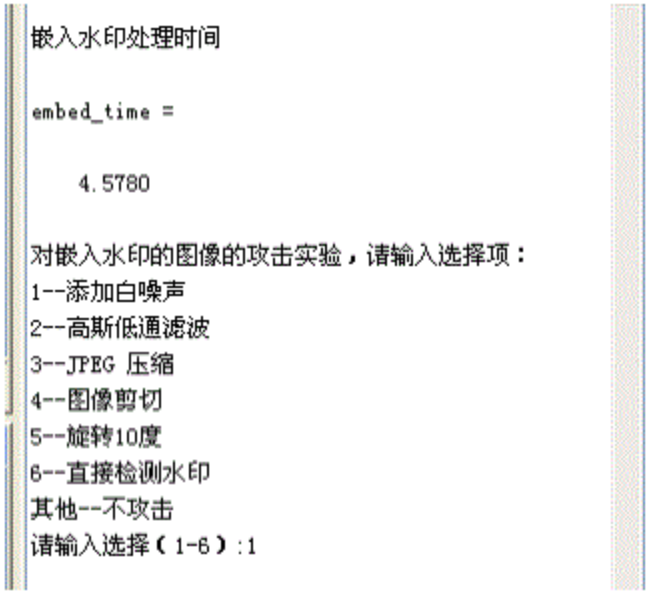

图 4.3 菜单效果图

4.2.2 添加白噪声

对水印图像进行攻击时，添加白噪声时很经常的一种攻击方式，从实验的结果可以看出，提取的水印图像很清晰，这说明水印对这种的攻击的鲁棒性很强，攻击试验效果如图 4.4 所示。

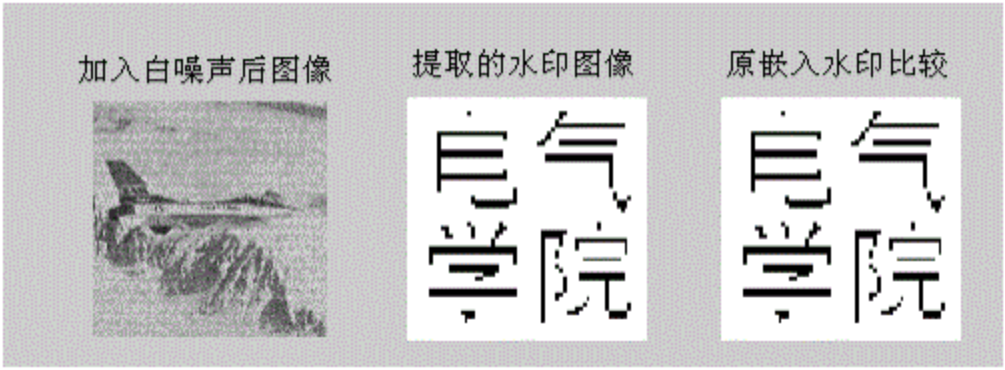

图 4.4 加入白噪声之后的图像提取出来的水印与原始水印比较

4.2.3 高斯低通滤波

对水印图像进行高斯低通滤波，图像依然清晰，这说明水印对这种攻击的鲁棒性比较强，攻击试验效果如图 4.5 所示。

图 4.5 经高斯低通滤波后的图像提取出的水印和原始水印比较

4.2.4 图像剪切

图像处理中，一个图像的不重要部分经常被剪切掉，对图像的上方进行剪切，如图 4.6，图像剪切后依然清晰，图 4.7 为提取出来的水印图像，依然清晰可见，实验结果可以看出，说明水印抵抗剪切的能力非常强，对这种攻击有着较强的鲁棒性。

图 4.6 部分被剪切过的水印图像

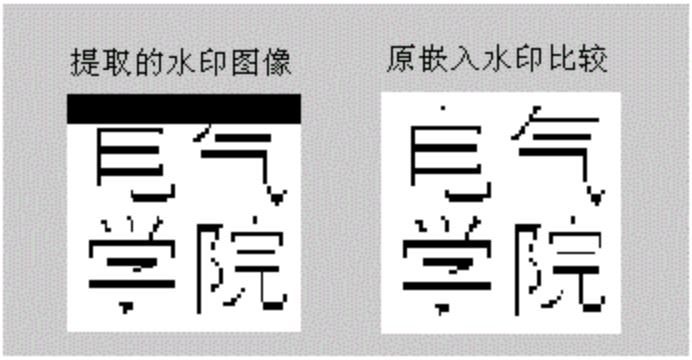

图 4.7 从部分被剪切过的水印图像中提取出的水印与原始水印对比图

4.2.5 旋转 10 度

对图像进行旋转 10 度，得到图 4.8，提取的水印图像与原始水印图像对比图如图 4.9，提取的水印图像完全变的模糊不清，可见水印对这种攻击有很差的鲁棒性。

图 4.8 经过旋转的水印图像

图 4.9 从被旋转过的水印图像中提取出水印图像与原始图像对比图

4.2.6 攻击结果数据分析

经过对含有水印的图像进行不同的攻击试验，可以得到含水印的图像在 DCT 算法下对不同的攻击的承受度，提取的水印图像与原始图像的相似度，载体图像与含水印的峰值信噪比等数据，数据在表 4-10 中有所体现。从中可以看出，含水印的图像在 DCT 算法下，对各种的攻击的抵抗性还是很高的，提取的水印图像与原始水印图像的相似度也是很高的。可见 DCT 算法还是不错的。

表 4-1 试验数据对比表

攻击图像方式	攻击与提取处理时间（attack_recover_time）	载体图像与含水印图像峰值信噪比（PSNR）	原水印图像与提取水印图像互相关系数（NC）
白噪声	8.5630	73.9134	1
高斯低通滤波	8.6410	744.0971	0.9858
JPEG 压缩	11.8440	2.9321	0.9997

剪切	8.7820	2.9272	0.8740
旋转 10 度	9.8910	2.9320	0.4685
直接检测水印	8.4690	357.9601	1

4.3 JPEG 图像压缩算法

4.3.1 JPEG 图像压缩流程

离散余弦变换(DCT)在图像压缩中具有广泛的应用，JPEG(Joint Photographic Experts Group)图像压缩算法即主要采用DCT进行变换编码。DCT变换的基本思路是将图像分解为8*8的子块或16 *16的子块，并对每一个子块进行单独的DCT变换，然后对变换结果进行量化、编码。采用较大的子块可以明显减少图像分块效应，但随着子块尺寸的增加，算法的复杂度急剧上升。因此，JPEG压缩一般把图像分解为8x8的子块进行变换。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)变换、量化、编码，压缩的具体流程如图4.10所示。

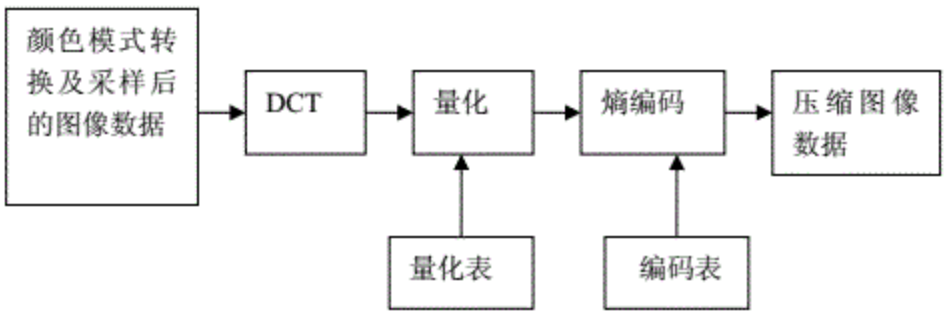

图4.10 JPEG压缩流程图

(1)颜色模式转换及采样

RGB色彩系统是最常用的表示颜色的方式，目的是为了配合计算机的输出设备，但是RGB三分量的关联性高，无形中造成存储空间的浪费。JPEG采用的是RGB

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RGB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，人眼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常用的采样方式有：YUV=4:1:1和YUV=4:2:2,YUV分别代表Y,Cb和Cr三个数据成份的采样比例。执行完这一步骤后，图像数据就压缩了50%和33%。

(2)DCT变换

交换前将图像划分为若干个8×8矩阵。这种矩阵在JPEG中被称为MCU(Minimum Code Unit)。MCU代表JPEG文件中存储压缩数据的基本单位，在每个MCU中包含一些亮度Y矩阵和色度Cb矩阵，饱和度Cr矩阵，但一个MCU中包含的矩阵数不得超过10个。例如：在采样比例为4：1：1中，每个MCU单元中含有4个亮度矩阵、1个Cb矩阵和1个Cr矩阵。

由于离散余弦公式所能接受的值的范围为-128到127之间，因此，对于MCU中每一个8x8的矩阵，首先将矩阵中64个系数减去128，然后进行DCT转换。DCT使原矩阵能量分布的范围集中，以配合接下去的量化。而经DCT后的数据仍和转换前相等，并未减少，所以DCT的步骤为无失真。JPEG使用之字型格式大致将空间频率按从低到高的顺序排列，其顺序如图4.11所示。

0	1	5	6	14	15	27	28
2	4	7	13	16	26	29	42
3	8	12	17	25	30	41	43
9	11	18	24	31	40	44	53
10	19	23	32	39	45	52	54
20	22	33	38	46	51	55	60
21	34	37	47	50	56	59	61

35	36	48	49	57	58	62	63

图4.11 8*8DCT系数之字型排列顺序

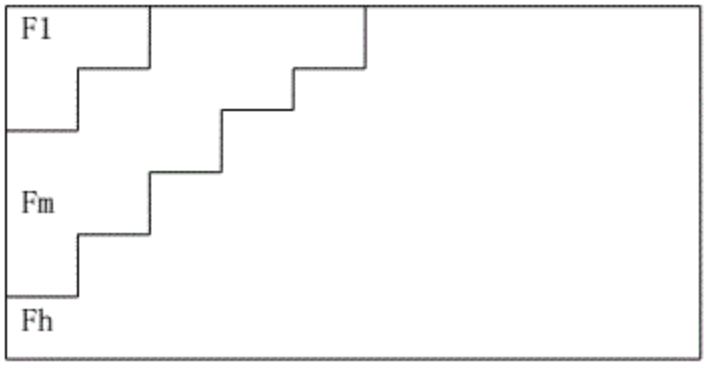

图 4.12 8*8DCT 系数频带示意图

左上角第0处的DCT系数为直流系数(集中了图像的主要能量)，其余63个为交流系数，其中靠近左上角的DCT系数为低频部分，右下角为高频部分，中间的则为中频部分，如图4.12所示。

(3)量化

对图像像素经过DCT变换后转换为频率系数进行量化，每个系数的量化步长由量化表指定，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，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。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，这有利于执行最后的编码。量化就是将DCT系数按比例缩小，取其最接近的整数值。

量化器通过JPEG提供的量化矩阵来达到目的。量化矩阵是预设的一个8*8的整数矩阵，对应DCT矩阵的64个频率系数。对亮度和色度频率系数分别需要一个量化矩阵，如表3-2和表3-3所示。

DCT中能量大的系数集中在DCT矩阵的DC系数与DC系数附近，所以量化矩阵的特色是：左上部分的系数较小，越往右下系数越大；而量化的做法是：将DCT矩阵的64个系数分别除以量化矩阵的整数，取其商的最接近的整数。此举使得原本分散的系数数值范围集中。量化矩阵中64个整数的大小取决于对应的DCT矩阵系数在图像中的重要性。如果该系数代表的是细节(高频部分)，其能量较小(如矩阵右下部分的系数)，忽略它并不会影响视觉品质，则该对应整数可以规定的大

一些，使得该系数被除后商为0，也就是此系数所代表的成分。反之，对能量大的部分除以较小的整数，保留精确的结果。

DCT矩阵量化的过程中，取商而弃余数，必然引入误差，这是JPEG中造成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。

4.3.2 JPEG 压缩试验

JPEG 压缩是图像处理中最常见的操作，该算法能有效的恢复水印。实验结果证明，在图像质量已经失真的情况下，仍然能提取出清晰的水印，可见水印具有较好的抗压缩的性能，鲁棒性很强，攻击试验效果如图 4.13 所示。

图 4.13 经过 JPEG 压缩后的图像提取出的水印与原始水印的比较

5 总结和展望

数字水印技术是信息科学中近几年来发展最为迅速的学科之一。随着多媒体技术和网络技术的飞速发展及广泛应用，对图像、音频、视频等多媒体内容的保护成为迫切需要解决的问题。多媒体内容的保护包括版权保护和内容完整性保护。由于现有计算机的计算能力不断翻番以及网络分摊计算技术的不断完善，因此传统的加密方法已受到极大的挑战，而新兴的信息隐藏技术则可以进一步增强系统的安全性与可靠性。信息隐藏技术用于多媒体保护则被称为数字水印，它是将一些标识信息直接嵌入到被保护的多媒体数据中，但是不影响原始内容的使用价值，而且不易被察觉或注意到。利用这些隐藏在多媒体数据中的信息，可以达到确认

数据拥有者、购买者或进行数据鉴定的真实性。此外，利用信息隐藏技术还可以实现电子商务中需要的匿名机制以及在军事、国防工业中实现隐藏通信.

不过，数字水印技术毕竟还是一门新兴的科学，它涉及到通信与信息理论、图像与语音处理、信号检测与估计、数据压缩技术、人类视觉与听觉系统、计算机网络与应用、电波传播等多种科学知识。虽然近几年来在理论和应用中取得了巨大的发展，但是到目前为止还尚未形成一个完整的理论体系，特别是还没有一个统一的评判标准，仍有许多的问题尚未解决。可以说，数字水印技术是一个充满活力但又垦待开拓的研究领域，而对于国内这一问题的研究正处于起步阶段。

本文主要做了以下工作：

• 系统介绍了信息隐藏与数字水印技术。归纳了信息隐藏及数字水印技术的分类、特性与应用;给出了数字水印技术的原理和基本框架以及其性能的评价方法;介绍了几种数字水印的攻击方法。

• 实现了一种数字水印的方法。使用离散余弦变换对图像进行变化后将随机序列作为水印信号嵌入到图像中，并对嵌入水印的图像进行了几种攻击以验证其鲁棒性。

信息隐藏与数字水印技术的研究目前是一个非常活跃的研究领域，应用市场前景十分广阔。本文对于信息隐藏与数字水印技术这一研究领域来说，只是一个入门，要想丰富和完善这一领域的研究，尚有大量的工作有待于在今后进一步的努力。根据对本领域的研究体会，认为以下几个方面有待于进一步的研究：

(1)水印基本原理和评价方法的进一步研究，包括水印理论模型、水印结构、水印嵌入策略、水印检测算法、水印性能评价以及水印的标准化等。现有算法的理论分析和评估。数字水印技术是直到九十年代才逐渐引起重视的，经过了近十几年的发展，涌现出了大量的算法，对这些算法的理论分析也会为我们将来在这方面的研究提供有益的帮助。这些理论可能是不成熟、不完善，但它的研究思路和技术仍给我们提供了重要的参考价值。

(2)目前其他的数字水印技术，如对基于图形、矢量图和动画等媒体的数字水印技术研究的比较少，这也是今后数字水印技术的一个研究方向。人类知觉特性的分析和研究。人类知觉包括人的视觉系统和人的听觉系统，这是我们进行信息隐藏的关键问题所在。大多数现有的数字水印算法都使在某种程度上利用人的

视觉或听觉缺陷，达到隐藏信息的目的。利用人的视觉特性的方法大多是针对图像、视频、文本等数字媒体，而利用人的听觉特性的方法大多是音频等介质。研究人的知觉特性对于如何有效地提高数字水印算法和隐藏效果都会起到十分重要的作用，这方面的研究仍是一项长期的工作。

(3)一个实用的数字水印系统的建立。开发一些具有实用价值的算法和软件不仅是信息技术发展的需要，也是数字水印技术走向实用的第一步。目前也不断有一些数字水印软件出现，但是这些隐藏算法都比较简单。今后可以把大部分的工作的重点是放在对嵌入信息的预处理上，通过这样的方法来增强系统的安全性。

参考文献

[1] 王邮锡，陈琦，邓峰森. 数字水印技术[M]. 西安: 西安电子科技大学出版社，2003.

[2] 曲丽丽. 基于数字水印的信息隐藏技术研究[J]. 光子学报，2004，20,26-27.

[3] 周亚训，叶庆卫，徐铁峰. 基于小波和余弦变换组合的图像水印方案[J]. 电子学报, 2001,29(12):1693-1695.

[4] 王志雄，王慧琴，李人厚. 数字水印的攻击和对策综述[J]. 通信学报，2002，23(11):74-79.

[5] 钟桦，焦李成. 基于特征子空间的数字水印技术[J]. 计算机学报，2003，26(3):1-6.

[6] 黄继武，Yun Q. 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 一 60.

[7] 蔡汉天，何军辉.一种能够基于 DCT 中频的数字水印技术.华南理工大学学

报.2001，(一 2):57 一 60.

[8] 程颖，张明生，王林平等.基于 DCT 域的自适应图像水印算法.计算机应用研究，2005.1.

[9] 孙圣和，王秋生.基于离散余弦变换系数分解的数字水印嵌入算法.哈尔滨工业大学学报,200l,33(5):700 一 705 北京:人民邮电出版社 2001.5.

[10] 陈明奇等.数字水印的攻击方法[J].电子与信息学报.2001，23(7):705-711.

[11] 黄继武程卫东 DCT 域图像水印:嵌入对策和算法电子学报,Vol.28,No.4,April 2000，57 一 60.

[12] Van Sehyndel R G，Tirkel A Z and Osborne C F.A Digital Watermark in Proc of the Conference on Image Proeessing.1994,(2):86 一 90.

[13] Cox1.J.，Killian J. and Leighton F.T. Secure Spread SPectrum Watermarking for Multimedia. IEEE Trans Image Proeessing.1997，6(12): 1673 一 1687.

[14] Xia 一 Xiang Gen，Boncelet C.G. and Arce G.R. Wavelet Transform Base Watermark for digital Images. Watermarking SPecial Issue of Optics ExPress.1998:497 一 511.

致谢

凝视着即将完成的论文，心中涌动着一种莫名的感受。短短的三个月时间里，在我完成毕业设计的同时，也包含了我对四年攻读学士学位所作工作的总结，包含了十几年求学生涯的经历。

我要真诚的致谢我的毕业设计指导老师——黄亚飞。在我完成设计的道路上，遇到的困难有他精心指导. 老师给我在求知、做事和为人等方面的熏陶将使我受益终身，在此，对老师表示最衷心的感谢！还要感谢其他同学对于我的帮助，感谢父母从小到大给我不断的支持是我顺利完成学业。

最后，我还要说：能进入长沙理工大学完成我的本科学业是我的荣幸！四年来能得到电子信息工程的多位老师的指导是我的幸运！在四年的学习中，老师们

渊博的学识，严谨、求是、创新的治学精神，诲人不倦的师者风范使我终生受益！

附录

```
clear all; %清除工作区所有变量
clc;%清除命令窗口所有的指令
start_time=cputime;%计 算 cpu 所 用 时 间 ， 当 前 的 时 间 赋 值 给 start——time
%%%%%%%%%%%% 读取水印图像 %%%%%%%%
I=imread('D:\毕业设计\mark.bmp');%读取水印图像
figure(1);%新建图形窗口 1 显示
subplot(2,3,1);%绘制子图 2x3 的第一个, 显示 2 行 3 列个图像
imshow(I),title('水印图像')%%显示水印图像，及其标题
I=rgb2gray(I);%将水印图形的 RGB 颜色变成灰色，把彩图转换为灰色
```

```
I=double(I)/255; %将颜色值换算成 double 型并进行归一化
I=ceil(I);% 向上取整
%%%%%%%%%%显示水印图像%%%%%%%%%%%%%
dimI=size(I);%I 的大小宽*高
rm=dimI(1);cm=dimI(2);%rm 为宽，cm 为高
%%%%%%%%%%%%%%%  以下生成水印信息 %%
mark=I; % 把 I 赋给 mark
alpha=50; %一般是幅值
k1=randn(1,8);%产生 1 行 8 列的随机数
k2=randn(1,8);%同上
a0=imread('D:\毕业设计\lena.bmp');%读取图片
psnr_cover=double(a0);%a0 变为双精度
subplot(2,3,2),imshow(a0,[]),title('载体图像');
%绘制子图 2x3 的第二个，以及图像及标题
[r,c]=size(a0);%获得 a0 的维数
cda0=blkproc(a0,[8,8],'dct2');  %对 a0 分成 8*8 的块并进行二维离散余弦变换
%%%%%%%%%%%%%%%%%%%% 嵌入 %%%%%%%%%%
cda1=cda0;     % cda1 = 256_256
for i=1:rm    % i=1:32
    for j=1:cm    % j=1:32
        x=(i-1)*8;y=(j-1)*8;
        if mark(i,j)==1
        k=k1;
        else
        k=k2;
        end
    cda1(x+1,y+8)=cda0(x+1,y+8)+alpha*k(1);
    cda1(x+2,y+7)=cda0(x+2,y+7)+alpha*k(2);
    cda1(x+3,y+6)=cda0(x+3,y+6)+alpha*k(3);
    cda1(x+4,y+5)=cda0(x+4,y+5)+alpha*k(4);
```

```
        cda1(x+5,y+4)=cda0(x+5,y+4)+alpha*k(5);
        cda1(x+6,y+3)=cda0(x+6,y+3)+alpha*k(6);
        cda1(x+7,y+2)=cda0(x+7,y+2)+alpha*k(7);
        cda1(x+8,y+1)=cda0(x+8,y+1)+alpha*k(8);

        end
end
%%%%% 嵌入水印后图像 %%%%%%%%%%%%%%
a1=blkproc(cda1,[8,8],'idct2');
a_1=uint8(a1);
imwrite(a_1,'withmark.bmp','bmp');%保存图像
subplot(2,3,3),imshow(a1,[]),title('嵌入水印后的图像');
disp('嵌入水印处理时间');
embed_time=cputime-start_time;%%%%运行时间
%%%%%% 攻击实验 测试鲁棒性 %%%%%%%%%%%
disp('对嵌入水印的图像的攻击实验，请输入选择项：');%%%disp 是输出函数
disp('1--添加白噪声');
disp('2--高斯低通滤波');
disp('3--JPEG 压缩');
disp('4--图像剪切');
disp('5--旋转 10 度');
disp('6--直接检测水印');
disp('其他--不攻击');
d=input('请输入选择（1-6）:');
start_time=cputime;
        figure(1);
                switch d
                    case 6
                subplot(2,3,4);
                imshow(a1,[]);
```

```
title('未受攻击的含水印图像');
M1=a1;
    case 1
 WImage2=a1;
 noise0=20*randn(size(WImage2));
 WImage2=WImage2+noise0;
 subplot(2,3,4);
 imshow(WImage2,[]);
 title('加入白噪声后图像');
 M1=WImage2;
 M_1=uint8(M1);%无符号取整
 imwrite(M_1,'whitenoise.bmp','bmp');

    case 2
 WImage3=a1;
 H=fspecial('gaussian',[4,4],0.2);%高斯低通滤波。hsize 表示模板尺寸，sigma 为滤波器的标准值，单位为像素
 WImage3=imfilter(WImage3,H);%%对任意功能的数组进行滤波
 subplot(2,3,4);
 imshow(WImage3,[]);
 title('高斯低通滤波后图像');
 M1=WImage3;
 M_1=uint8(M1);%%%无符号整形
 imwrite(M_1,'gaussian.bmp','bmp');

    case 4
 WImage4=a1;
 WImage4(1:64,1:512)=512;
 %WImage4(224:256,1:256)=256;
```

```
%WImage4(1:256,224:256)=256;
%WImage4(1:256,1:32)=256;
WImage4cl=mat2gray(WImage4);%把矩阵转化为灰度图像
figure(2);
subplot(1,1,1);
%subplot(2,3,4);
imshow(WImage4cl);
title('部分剪切后图像');
figure(1);
M1=WImage4cl;
%M_1=uint8(M1);
%imwrite(M_1,'cutpart.bmp','bmp');


    case 3
WImage5=a1;
WImage5=im2double(WImage5);%将输入的矩阵转化为双精
cnum=10;
dctm=dctmtx(8);%返回一个 8*8 的 DCT 变换矩阵
P1=dctm;
P2=dctm.';
imageDCT=blkproc(WImage5,[8,8],'P1*x*P2',dctm,dctm.');
DCTvar=im2col(imageDCT,[8,8],'distinct');
n=size(DCTvar,1);
DCTvar=(sum(DCTvar.*DCTvar)-(sum(DCTvar)/n).^2)/n;
[dum,order]=sort(DCTvar);
cnum=64-cnum;
mask=ones(8,8);
% mask(order(1:cnum))=zeros(1,cnum);
im88=zeros(9,9);
im88(1:8,1:8)=mask;
```

```
im128128=kron(im88(1:8,1:8),ones(16));
dctm=dctmtx(8);
P1=dctm.';
P2=mask(1:8,1:8);
P3=dctm;

WImage5=blkproc(imageDCT,[8,8],'P1*(x.*P2)*P3',dctm.',mask(1:8,1:8),dctm);
WImage5cl=mat2gray(WImage5);
%figure(2);
subplot(2,3,4);
imshow(WImage5cl);
title('经 JPEG 压缩后图像');
%figure(1);
M1=WImage5cl;
    case 5
WImage6=a1;
WImage6=imrotate(WImage6,10,'bilinear','crop');
WImage6cl=mat2gray(WImage6);
figure(2);
subplot(1,1,1);
imshow(WImage6cl);
title('旋转 10 度后图像');
figure(1);
M1=WImage6cl;
        otherwise
disp('你输入的是无效数字，图像未受攻击，将直接检测水印');
subplot(2,3,4);
imshow(a1,[]);
title('未受攻击的含水印图像');
M1=a1;
```

```
                end
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%    提取水印    %%%%%
psnr_watermarked=M1;
dca1=blkproc(M1,[8,8],'dct2');
p=zeros(1,8);
for i=1:dimI(1)
    for j=1:dimI(2)    % j=1:32
        x=(i-1)*8;y=(j-1)*8;
    p(1)=dca1(x+1,y+8);
    p(2)=dca1(x+2,y+7);
    p(3)=dca1(x+3,y+6);
    p(4)=dca1(x+4,y+5);
    p(5)=dca1(x+5,y+4);
    p(6)=dca1(x+6,y+3);
    p(7)=dca1(x+7,y+2);
    p(8)=dca1(x+8,y+1);
    %sd1=sum(sum(p.*k1))/sqrt(sum(sum(p.^2)));
    %sd2=sum(sum(p.*k2))/sqrt(sum(sum(p.^2)));
     %if sd1>sd2
     if corr2(p,k1)>corr2(p,k2),warning off MATLAB:divideByZero;
        mark1(i,j)=1;
     else
        mark1(i,j)=0;
     end
    end
end
subplot(2,3,5);
imshow(mark1,[]),title('提取的水印图像');
subplot(2,3,6);
imwrite(mark1,'getmark.bmp','bmp');
```

```
imshow(mark),title('原嵌入水印比较');
%%%% time %%%%%%%
disp('攻击与提取处理时间')
attack_recover_time=cputime-start_time,
%%%%% psnr %%%%%%%%
disp('载体图像与含水印图像峰值信噪比')
PSNR=psnr(psnr_cover,psnr_watermarked,c,r),
%%%%%%% Oringinal mark and mark test %%%%%%%%%%
disp('原水印图像与提取水印图像互相关系数')
NC=nc(mark1,mark),
```