息中判断隐藏信息是否存在,更加难以截获隐藏信息,从而保证了信息的安全。

另外,由于信息隐藏必须考虑所隐藏的信息在经历各种环境、操作之后,仍需具有免遭破坏的能力,因此,信息隐藏技术必须考虑正常的信息操作所造成的威胁,即要使秘密信息对正常的数据操作具有免疫能力。这种免疫能力的关键是要使隐藏信息部分不易被正常的数据操作(如通常的信号变换操作或数据压缩)所破坏。

3. 信息隐藏的分类和应用

本章文献[1]对信息隐藏技术进行了分类,如图 12-1 所示。

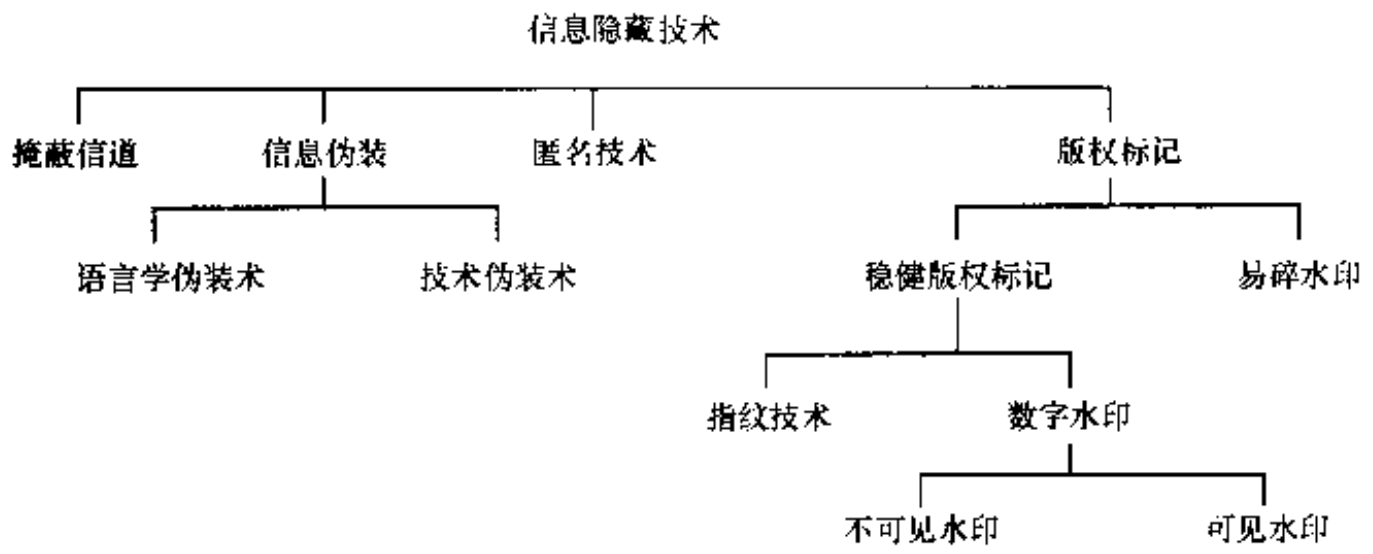

图 12-1　信息隐藏技术的分类

信息隐藏技术的一个重要应用是数字水印技术,关于该方面的应用将在 12.1.2 小节详细介绍,除此之外,还有以下应用:

(1)军事和安全部门需要不被入侵和破坏的通信信道。在现代战争中,即使秘密内容被加密编码,对信号的检测及定位也会很快导致对信号发送装置的攻击。基于这种原因军事通信可利用信息隐藏技术使得通信不被敌方检测和干扰。

(2)互联网犯罪分子在进行网络犯罪时利用这一技术,通过频繁地改变身份和使用代理服务器,并在离线时删除计算机中留下的"踪迹",以防止计算机安全部门的追查。

(3)法律和相应部门需要深入了解信息隐藏技术的原理及其弱点,以便对妨碍国家和公共安全的秘密信息传递及其他行为进行检测和追踪。

12.1.2　数字水印技术

1. 数字水印技术的发展现状

数字水印技术是 20 世纪 90 年代正式提出的,以下几个引起普遍关注的问题构成了数字水印的研究背景。

1）数字作品的知识产权保护

数字水印利用数据隐藏原理使版权标志不可见或不可听，达到既不损害原作品，又达到版权保护的目的，这种应用要求具有非常高的稳健性。包含很多图像的 Web 是数字水印应用的范畴，它所含的这些图像是可随意使用的，但是它们的所有者却要保护它们。目前，用于版权保护的数字水印技术已经进入了初步实用化阶段，IBM 公司在其“数字图书馆”软件中就提供了数字水印功能，著名的 Photoshop 软件中集成了 Digimarc 公司的数字水印插件。然而，目前市场上的数字水印产品在技术上还不成熟，很容易被破坏或破解，距离真正的实用还有很长的路要走。

2）印刷品防伪和电子商务的票据防伪

目前，许多国家都已开始研究用于印刷品防伪的数字水印技术，其中麻省理工学院媒体实验室已经开始研究在彩色打印机、复印机输出的每幅图像中加入惟一的、不可见的数字水印，在需要时可以实时地从扫描票据中判断水印的有无，进而快速辨识票据的真伪。德国也有研究单位正在研究用于护照真伪鉴别的数字水印技术。

此外，在新兴的电子商务中，各种电子票据的有效防伪是十分重要的，它们还需要一些非密码的认证方式。数字水印技术可以为电子票据提供不可见的认证标志，从而大大增加了伪造的难度。

3）声像数据的隐藏标识和篡改提示

数据的标识信息往往比数据本身更具有保密价值，如遥感图像的拍摄日期、经/纬度等。没有标识信息的数据有时甚至无法使用，但直接将这些重要信息标记在原始文件上又很危险。数字水印技术提供了一种隐藏标识的方法，标识信息在原始文件上是看不到的，只有通过特殊的阅读程序才可以读取。这种方法已经被国外一些公开的遥感图像数据库所采用。

此外，数据的篡改提示也是一项很重要的工作。基于数字水印的篡改提示可以通过隐藏在声像信号中水印的状态判断声像信号是否被篡改。

4）隐蔽通信及其对抗

数字水印所依赖的信息隐藏技术不仅提供了非密码的安全途径，更引发了信息战，尤其是网络情报战的革命，产生了一系列新颖的作战方式，引起了许多国家的重视。

网络情报战是信息战的重要组成部分，其核心内容是利用公用网络进行保密数据传送。经过加密的文件容易引起攻击者的注意。网络多媒体技术的广泛应用使得利用公用网络进行保密通信有了新的思路，利用数字化声像信号相对于人的视觉、听觉冗余，可以进行各种时(空)域和变换域的信息隐藏，从而实现隐蔽通信。

2. 数字水印原理及其通用模型

从数字信号处理的角度看，嵌入数字信号中的水印信号可以视为在强背景下迭加一个弱信号，只要迭加的水印信号强度低于人的视觉系统(HVS)或听觉系统(HAS)的感知门限，人就无法感知到水印信号的存在。HVS 或 HAS 受视觉、听觉系统的空间、时间和频率特性的影响。因此，通过对原始信号作一定的调整，就有可能在不改变视觉或听觉效果的情况下嵌入一些水印信息。

从数字通信的角度看，水印嵌入可理解为在一个宽带信道(掩体对象)上用扩频通信技术传输一个窄带的水印信号。尽管水印信号具有一定的能量，但分布到信道中任一频率上的能量是难以检测到的。水印的检测则是一个在有噪信道中进行弱信号检测的问题。

设掩体对象为 I，水印信号为 W，密钥为 K，则水印嵌入可用如下表达式来描述

$$I_w = G(I, W, K) \tag{12.1.1}$$

式中 G 表示水印嵌入算法，I_w 表示掩体对象嵌入水印后生成的隐藏对象。水印的嵌入过程如图 12-2 所示。

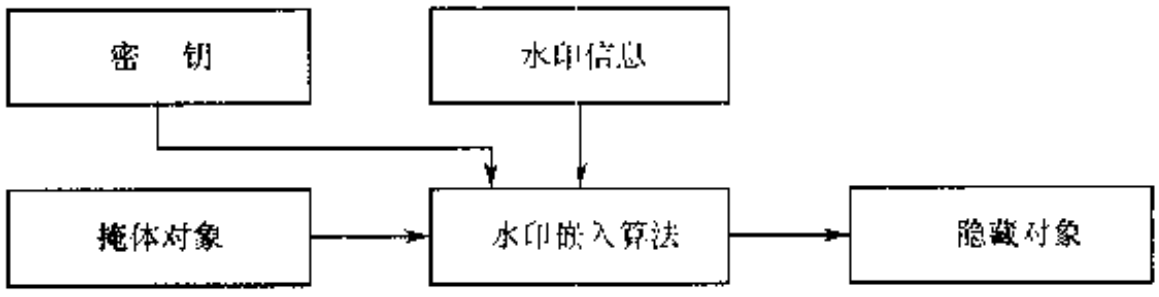

图 12-2　水印嵌入过程

图 12-3 和图 12-4 分别是水印提取与水印检测框图。图 12-3 和图 12-4 中的虚框部分表示在提取或判断水印信号时原始数据不是必要的。

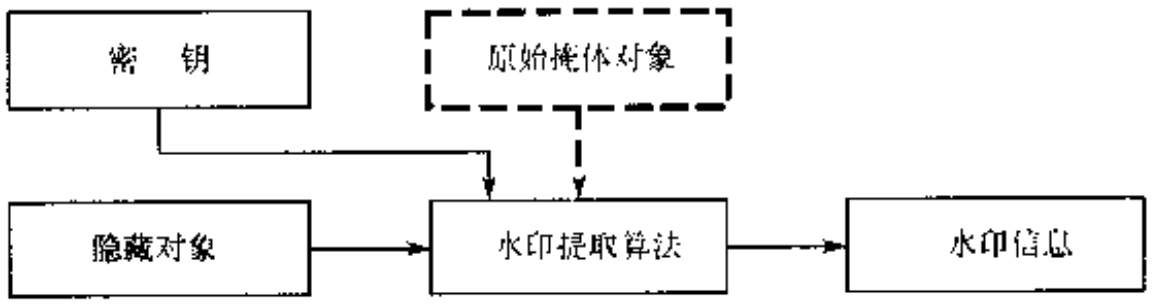

图 12-3　水印提取过程

在某些水印系统中，水印可以被精确地抽取出来，这一过程被称做水印提取(参见图 12-3)。例如在完整性确认和篡改提示应用中，必须能够精确地提取出插入的水印，并且通过水印的完整性来确认多媒体数据的完整性。如果提取出的水印发生了部分的变化，最好还能够通过发生变化的水印的位置来确定原始数据被篡改的位置。

对于稳健水印而言，使用它的目的是防止数据处理和恶意攻击对水印的破坏，而通

常对于受到某种数据处理或攻击的隐藏对象，不可能精确地从中提取出嵌入的原始水印，这时就需要一个水印检测过程(参见图 12-4)。一般来说，水印检测中首先是进行水印提取，然后是水印判决。水印判决的通行做法是相关性检测，即选择一个相关性判决标准，计算提取出的水印与指定的原始水印的相关值，如果相关值足够高，则可以基本判定被检测隐藏对象中含有指定的水印。

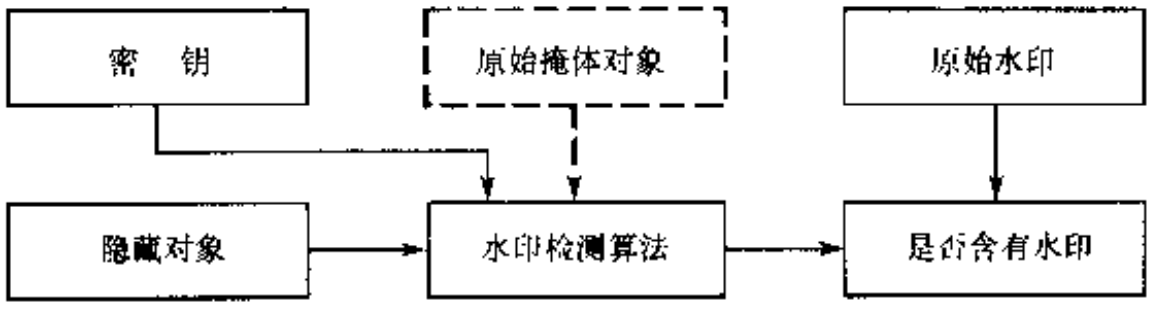

图 12-4　水印检测框图

从以上论述可以看出，水印提取的任务是从嵌入水印的数据中提取水印信号，而水印检测的任务是判断某一隐藏对象中是否存在指定的水印信号。此外，水印检测的结果依赖于一个给定的阈值，当相关性检测的结果超过这个阈值时，就给出“含有指定水印”的结论。这实际上是一个假设检验的问题。在水印检测时，会发生两类错误，一类是虚警，就是将不含有水印信号的数据误认为含有水印信号；另一类是漏报，就是未能从含有水印信号的数据中检测到水印信号。当提高相关性检测的阈值时，虚警概率降低，漏报概率升高；当降低相关性检测的阈值时，虚警概率升高，漏报概率降低。在实际的水印应用中，一般更注重对虚警概率的控制。

3. 数字水印特点及分类

在数字水印系统中，隐藏信息的丢失意味着版权信息的丢失，从而失去了版权保护的功能，这样就意味着这一系统是失败的。因此数字水印技术必须具有较强的稳健性、不可检测性和不可感知性等特点[1]。

(1) 稳健性：指抗拒各种信号处理操作和恶意攻击，在掩体对象不产生明显降质的前提下，不导致水印信息丢失的能力。信号处理操作包括：传输过程中的信道噪声、各种形式的滤波、增强、有损压缩、几何变换、D/A 或 A/D 转换等。所谓的恶意攻击包括：篡改、伪造、去除水印等。需要指出的是，稳健性只是用于版权保护的水印所必须具有的特征，而对于以保护数据完整性为目的的数字水印来说，脆弱性则是其最重要的特征。

(2) 不可检测性：指嵌入水印后的数据与原始载体数据具有一致的特性。如具有一致的统计噪声发布等，以便使攻击者无法判断其中是否有隐藏信息。

(3) 不可感知性：指向数字作品中嵌入的数字水印，是利用人类视觉或听觉系统的特性，经过一系列隐藏处理，隐藏对象必须没有明显的降质现象，而嵌入的水印不会引起人的感知。水印的不可感知性是相对于被保护数据的使用而言的。如加在图像上的水印不应干扰图像的视觉欣赏效果，但并不是说水印必须不可见。事实上，虽然目前已有的大多

数水印方案是不可见的，但也存在着可见的水印方案。

(4) 隐藏位置的安全性：指必须将水印信息隐藏于掩体对象的内容之中，而非文件头等处，这样可以防止因文件格式的变换而使水印遭到破坏。

(5) 无歧义性：恢复出的水印或水印判决的结果应该能够确定地表明所有权，不会发生多重所有权的纠纷。

(6) 计算有效性：水印处理算法应该比较容易用软、硬件实现。尤其是水印检测算法必须足够快，以满足在产品发行网络上对多媒体数据的管理要求。

数字水印的分类方法有很多种，分类的出发点不同导致了分类的不同，它们之间是既有联系又有区别的。最常见的分类方法包括以下 5 类。

(1) 空域水印和变换域水印：直接在空域中对信号采样点的幅度值作出改变，嵌入水印信息的称为空域水印；对变换域中的系数(离散傅里叶变换系数、离散余弦变换系数、离散小波变换系数等)作出改变以嵌入水印信息的称为变换域水印。一般来说变换域算法可嵌入的水印数据量大，不可感知性好，安全性高，但算法复杂度也高。

(2) 易损水印和稳健水印：易损水印很容易被破坏，主要应用于完整性验证等应用之中，它随着对象的修改而被破坏，即使对象细小的改变也会影响数字水印的提取和检测。稳健水印则应该经得起一般信号处理操作而存留下来，它的应用范围更加广泛，主要应用于版权保护中，是水印研究的重点。

(3) 非盲水印和盲水印：在提取或检测水印的过程中，如果需要用原始数据来提取水印信号，称为非盲水印算法；如果不需要原始数据参与，可直接根据含水印的数据来提取出水印信号，称为盲水印算法。通常，非盲水印比盲水印的安全性高、稳健性强，但盲水印更符合所有权验证的需要，是水印算法发展的方向。

(4) 有意义水印和无意义水印：有意义水印是指水印本身也是某个有意义数字图像或数字音频片段的编码；无意义水印则只对应于一个序列号或一段伪随机数。有意义水印的优势在于，如果由于受到攻击或其他原因致使检测到的水印有破损，人们仍然可以通过观察确认是否有水印。但对于无意义水印来说，如果检测到的水印序列有若干码元错误，则只能通过统计决策来确定信号中是否含有水印。

(5) 对称水印和非对称水印：当水印嵌入与水印提取或检测过程所使用的密钥相同时，相应的水印算法称为对称水印算法。当水印嵌入与水印提取或检测过程所使用的密钥不同时，相应的水印算法称为非对称水印算法。

4. 数字水印的主要应用领域

数字水印产品虽然只是近两年才出现，但其应用前景和应用领域将是巨大的，总的来说，数字水印技术有以下 5 个主要应用领域。

(1) 版权保护：数字作品的所有者用密钥产生一个水印，并将其嵌入原始数据，从而防止他人对该数据宣称拥有版权。当该作品被盗版或出现版权纠纷时，所有者可利用从

盗版作品或水印作品中获取的水印信号作为依据，从而保护所有者的权益。这要求水印必须有较好的稳健性、安全性和不可感知性。

(2) 图像认证：认证的目的是检测对图像数据的修改。可用易损水印来实现图像认证。为便于检测，易损水印对某些变换(如压缩)，具有较低的稳健性，而对其他变换的稳健性更低。因而在所有的数字水印应用中，认证水印具有最低级别的稳健性要求。

(3) 盗版追踪：为避免未经授权的拷贝和发行，出品人可以将不同用户的身份编码或序列号作为不同的水印嵌入到作品的合法拷贝中，以用来识别作品的单个发行拷贝。这类似于软件产品中的序列号，对监控和跟踪流通作品的非法拷贝很有用。

(4) 标题与注释：将作品的标题、注释等内容以水印形式嵌入到该作品中。例如，一幅照片的拍摄时间和地点，X 放射线相片的病人姓名和编号等。这种隐式注释可以节省带宽，且不易丢失。

(5) 使用控制：在多媒体发行体系中，人们希望有一种拷贝保护机制，即它不允许未授权的媒体拷贝。在封闭或私有系统中，可用水印来说明数据的拷贝状况。一个典型的例子是 DVD 防拷贝系统。一个符合要求的 DVD 播放器不允许播放或拷贝带有“禁止拷贝”水印的数据，而带有“一次拷贝”水印的数据可以被拷贝一次，但不允许从该拷贝再进一步制作拷贝。

12.2　基于小波变换的数字水印技术

上一节对数字水印技术进行了介绍，下面介绍小波变换在数字水印技术中的应用。由于以图像为载体对象的水印技术是当前研究的热点，因此本节的介绍以图像水印中的小波应用为重点。

在图像压缩标准“JPEG-2000”中，小波将成为一个主要的技术。因为小波变换具有良好的时频特性，所以在最近两年发表的论文中，这项技术也被用于了图像水印技术。使用小波域水印方法的优点与在 JPEC 中使用小波是类似的，主要表现在 3 个方面：一是可以保证在“JPEG-2000”有损压缩下水印不会被去除；二是可以将图像编码研究中关于视觉特性的研究成果用于水印技术；三是有可能提供在压缩域中直接嵌入水印的方法。除此之外，小波的多分辨分析与人眼视觉特性是一致的，这对根据 HVS 选择适当的水印嵌入位置和嵌入强度有很大的帮助。

和其他变换域的水印技术一样，小波变换域水印也分为水印嵌入、提取(检测)两部分，其过程可以用图 12-5 和图 12-6 来表示。图中虚线部分表示水印检测时可以不需要原始载体的参与。从图上可以清楚地看到，小波水印的嵌入和提取都是在小波域中进行的。在此过程中，小波的类型、水印的选取、水印嵌入的强度以及水印嵌入的位置都会影响到水印系统的性能，包括水印的稳健性和视觉可见性。此外，在很多情况下，提取出的水印是通过与原始水印作相关比较来判断水印的存在与否的，因此还要有一个检验阈值

的确定问题。

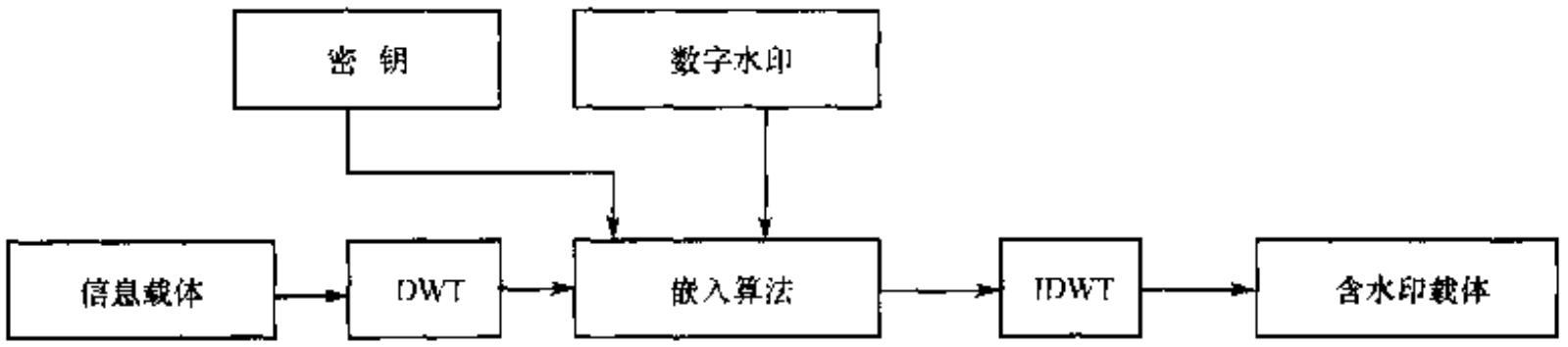

图 12-5　小波变换域水印嵌入的一般过程

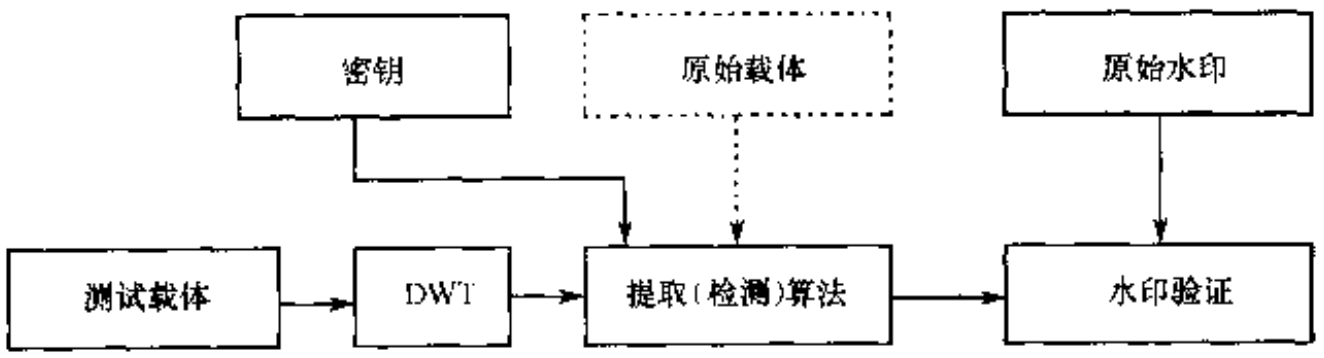

图 12-6　小波变换域水印检测的一般过程

下面分类介绍几种典型的小波水印方案。

12.2.1　基于低频子带方法

较早提出将小波变换用于水印的研究者将水印嵌入到代表载体图像的最低分辨率近似分量的系数中[2,3]。

有效搜索小波系数的多阈值小波水印编码方案是基于低频子带方法中的一种典型方案[4]。该方案选择那些在各种信号处理操作中都不会有太大变化的系数，如果这些系数明显地受到了改变，则重建图像将在视觉上与原始图像产生很大的差异。与预先确定一组系数(例如各种低频系数)的方法相反，这种方法依赖于图像本身来选择系数。因此，这种方法适合于纹理图像以及光滑图像。

本章文献[5]将一个二进制随机水印信号嵌入到一组按重要性选出的小波系数中，为了使水印具有较高的稳健性，嵌入过程将水印信号作为量化噪声嵌入到小波零树编码的数字图像中。

考虑到离散余弦变换在水印技术中的应用，有学者将离散小波变换和离散余弦变换相结合[6]，将原始图像经适当的离散小波变换分解成一个逼近子图和多个细节子图，然后对逼近子图再进行离散余弦变换，将水印嵌入到中高频段 DCT 系数中。

为了充分利用人类的视觉特性，Pereira[7]描述了一种使用 Haar 小波滤波器对非重叠 16×16 图像块进行一层分解的算法。该水印算法使用线性规划获得水印的稳健性，并使视觉失真限制在由可见性差值(JND，Just Noticeable Difference)门限映射给出的范围内。

对每一个嵌入的水印比特，从大小为 8×8 的 LL 子带中选取 2×2 的相邻系数，对嵌入的信息使用差分编码。由于该算法要求相邻系数的平均差值为 0，因而相邻系数的选择是很重要的。

本章文献[8]利用小波系数自身的特点和各层小波系数之间的树结构关系，对最低频逼近系数进行分类，一类对应于强纹理区域，另一类对应于弱纹理区域，对不同类采取不同的嵌入对策，以保证水印的不可见性。

12.2.2　细节分量方法

由于近似图像系数的分布是很均匀的，其细节分量系数的分布服从 Laplace 分布，而大多数的系数接近于 0，只有很少一部分对应于图像边缘和纹理信息的系数具有较大的峰值，含有较显著的能量。这些空间域的特征在小波域中是由不同尺度具有渐低的分辨率描述的，因而可进行多分辨率分析，以突出显示图像局部或全局的特征。

为在细节分量系数中可靠地嵌入水印，必须选择一些重要系数进行水印嵌入或者对水印能量进行加权，以便在重要系数中嵌入更多的能量。水印嵌入强度可以自适应于子带能量、分解层和子带的方向。在一些算法中，系数的重要性由系数和门限的比较而确定，即

$$T_l^o = \frac{\max\{|c_l^o|\}}{2} \tag{12.2.1}$$

该门限值由在第 l 分解层，方向为 o 的子带的系数绝对值的最大值决定。

基于小波变换的水印提取方法有不少，例如分层的水印法[9]，其优点是，如果加水印的图像失真不太严重的话，可以节省计算量。它的基本思想是，用离散小波变换将待检测的图像和原始图像分解为 4 个频段，即只作 1 级分解。然后，计算待检测图像和原始图像 HH1 段的 DWT 系数之间的差值，将它与加在 HH1 段的水印进行比较，计算它们之间的互相关函数，如果互相关函数出现了一个峰值，那么认为水印被检测到了，否则再考虑同一级的其他频段。如果水印还是没有被检测到，就计算下一级的 DWT，即 2 级分解，并且重新尝试检测水印。这个过程一直进行，直到检测到了水印为止或者已经达到了 DWT 的最后一级。该方案不足之处是，如果图像失真较大，则水印提取所需运算量就会增大；并且水印嵌入的强度较低，水印稳健性不高。因此在分层水印提取处理方法的基础上，人们又采用了包括近似分量在内的所有尺度进行水印的嵌入。使用层适应门限选取感知显著的系数以获得高的稳健性。水印能量根据分解层数进行调解，以避免产生感知失真。

Tsekeridou[11]利用小波变换域的多分辨特性，在小波分解的第一层和第二层的细节分量中嵌入一种循环自相似水印是另一种水印提取处理的方法。采用这种方法的优点是：在图像受到几何失真攻击时，在不需要原始图像的前提下，可以大大简化水印的定位步骤。

二值水印法是通过修改载体图像的同一分辨率层中 3 个不同方向的细节分量系数的

幅度关系，而嵌入的一种二值水印。该算法是对每一组选中的 3 个系数进行排序，对中间的系数进行量化以嵌入比特 0 或 1。而与此法类似的方法是将最低分辨率细节分量分割为不同区域，使每个区域含有近似相同数目的重要系数[13]。这种方法将每个区域的重要系数分量进行量化，使其代表水印信息中的一个比特。由于该方法是根据稳健性的需要确定每个区域中的重要系数的个数，并不是局限于对 3 个系数中的一个进行量化，所以，这种方法具有较强的灵活性。但是，在水印提取过程中由于需要参照数据，即前者需要 3 个重要系数的位置，后者需要细节子带的划分区域，因而这两种新算法也是半盲的。

为进一步提高细节分量小波水印算法的性能，有文献结合人类视觉系统和图像的 DWT 多分辨分解，将水印嵌入图像小波分解的各个中高频带[14]，其频带的选择和嵌入的水印由密钥确定，并可实现水印的盲检测。

Jayawardena[15]成功地应用二值小波滤波器获得了一个多分辨域。该算法选择细节分量的一个显著比特层。首先，将该层的所有比特都置为 1，并进行逆小波变换计算。得到的图像用 I_1 表示；接下来，将该层的所有比特都置为 0，同样进行逆小波变换计算，得到图像 I_0；然后，当图像受到有损压缩时，观察哪一个位置上选定的位平面的嵌入信息是固定不变的，对每个提出的比特嵌入位置考虑给定的视觉失真约束；最后将得到的这些固定不变的位置就用来直接嵌入二值水印。

12.2.3 基于图像的编码方法

零树编码是基于这样一个假设：如果近似分量的小波系数对于给定的门限 T 是不显著的，那么在同样空间区域的细节分量中，相同方向所有的小波系数对于 T 都是不显著的。如果可以用特殊的符号对一个零树根(zerotree root)进行编码，就意味着整个树是不显著的。这可导致编码空间的节省，因为在高频细节分量中，许多次要系数可以被忽略。Inoue[16]使用零树编码的方法进行水印的嵌入，他根据水印信息，用一个小的正或负值替代零树的次要系数。

较早提出将基于小波图像编码和水印结合的研究者是 Wang[17]和 Su[18]。Wang 的算法是基于多门限小波编码方法(MTWC, Multi-Threshold Wavelet Codec)，Su 则是使用利用最优化截断的嵌入块编码算法(EBCOT, Embedded Block Coding with Optimized Truncation)，该算法也是即将公布的 JPEG 2000 图像压缩标准的基础。上述两种水印算法在选中的细节子带中的重要系数上添加伪随机 Gaussian 噪声。水印的嵌入和提取在图像的压缩和解压过程中进行，这样就可以避免为水印的嵌入和提取而进行的第 2 次变换域计算。

JPEG 2000 和 EBCOT 的主要设计目标是：通过对图像块的独立处理和编码获得广泛的多应用性和灵活性。JPEG 2000 的默认设置是使用 7/9 双正交小波对图像进行 5 层小波分解，然后将变换图像分割为不超过 4 096 个系数的非重叠编码块。

为适应 JPEG 2000 的编码处理，水印算法应遵循对编码块的独立操作。设计水印算法时需要注意以下几个方面：

(1)依赖于子带间或分级多分辨率关系的算法不能直接在 JPEG 2000 的编码中应用;

(2)由于受 JPEG 2000 编码块系数个数的限制,基于相关的方法在单个独立块中无法进行可靠的水印检测;

(3)需要原始图像和参照数据的水印提取算法在这里是不合适的。

12.3　几种基于小波变换的图像水印算法

为增强读者对基于小波域的数字水印算法技术的深入理解,本节将详细分析几种有代表性的小波数字水印算法。

12.3.1　Inoue 算法

这里首先介绍由 Inoue[16]提出的使用零树编码进行水印嵌入的算法。Inoue 在该文中提出了两种水印嵌入的方法,一种是将水印嵌入到小波域的次要系数上,一种是将水印嵌入到小波域的重要系数中,嵌入的水印 W 是二值的比特序列。

1. 预备知识

1) 图像信号的多分辨小波分解

为了使嵌入的水印对有损压缩(如 JPEG)具备较强的稳健性,在水印的嵌入过程中,把原始图像通过二维小波变换分解为 3 层多分辨率塔式结构,如图 12-7 所示。其中,在多分辨率分解的第 3 层中,最低频子带 LL3 包含了原始图像的最低分辨率信息,而 HL3,LH3 和 HH3 是 LL3 的精细图像信息,第 3 层中 HL3,LH3 和 HH3 图像包含了第 2 层参考图像(HL2,LH2 和 HH2)的近似信息,而第 2 层中的图像(HL2,LH2 和 HH2)又包含了第 1 层参考图像(HL1,LH1 和 HH1)的近似信息。在以小波方式分解的图像数据中可以构成若干个如图 12-7 所示的四叉树。

2)基于零树编码的小波系数分类

在零树编码中,可以将较低精度级上的系数称为父系数,该父系数所对应的同一方向上各较高精度级的系数称为其子系数。给定一个阈值 T,如果一个近似分量中的系数 x 满足 $|x| < T$,并且它的所有各级子系数 $u, v, \cdots$,都满足 $|u| < T, |v| < T, \cdots$,则称这些系数是次要系数;如果 $|x| > T$,则称 x 是重要系数。

2. 在次要系数中嵌入水印的方法

首先对原始图像进行 3 级小波分解,选用 3 个子带组(LH3,LH2,LH1),(HL3,HL2,HL1) 和(HH3,HH2,HH1) 构造零树。保留最低频率子带(LL3) 不变。