§7.2 数字水印

对多媒体内容的保护分为两个部分：一是版权保护，二是内容完整性（真实性）保护，即认证。

数字水印技术就是将指定的数字、序列号、文字、图像标志等版权信息嵌入到数据产品中，以起到版权保护、秘密通信、数据文件的真伪鉴别和产品标识等作用。

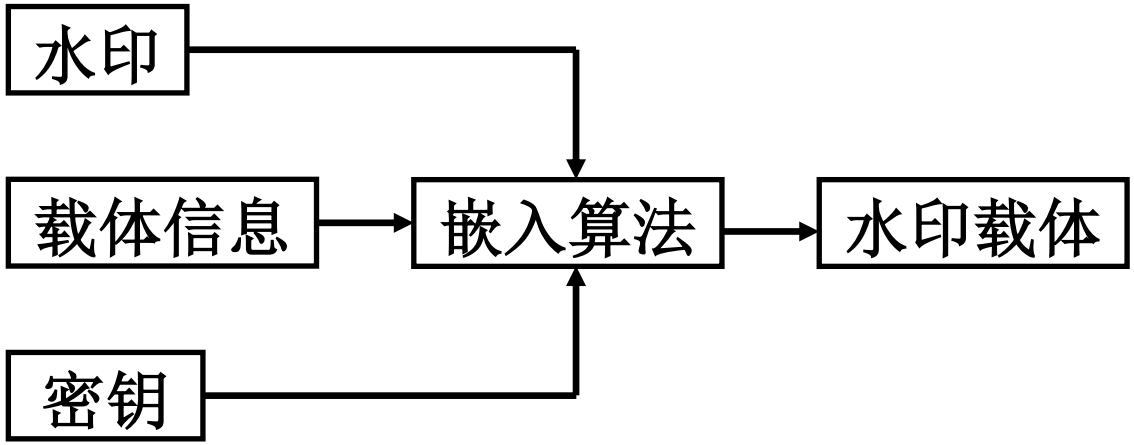
数字水印目的在检查盗版行为时，可以从数字载体中提取出有关信息，用以证明数字产品的版权，指证盗版行为。在大多数情况下，只需要证明载体中存在某一个数字水印，不需要精确地恢复隐藏的数字水印。

数字水印技术已成为多媒体信息安全研究领域的一个热点，也是信息隐藏技术研究领域的重要分支。

§7.2 数字水印

数字水印的通用模型：

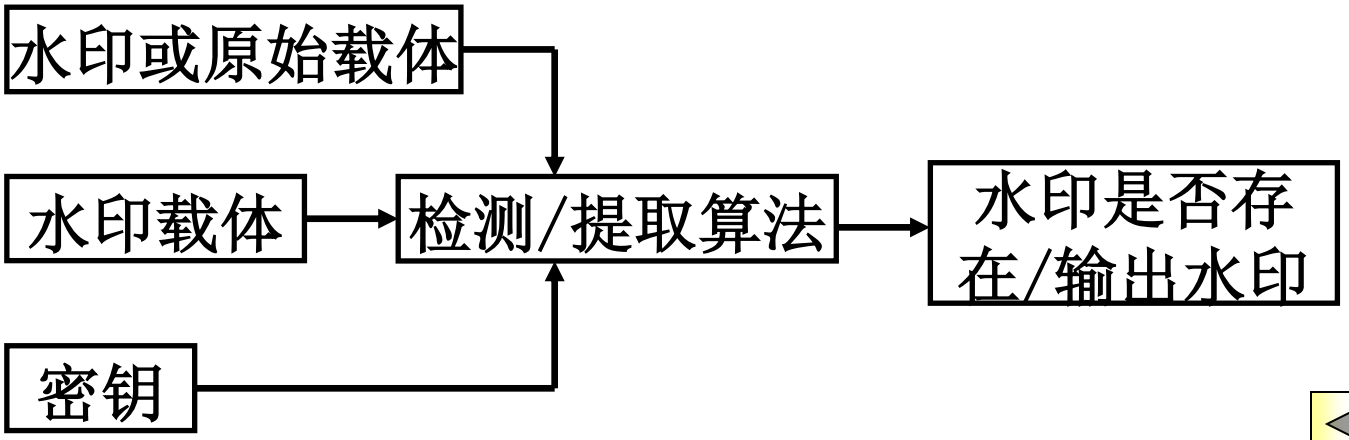
数字水印技术包括嵌入、检测和提取3个过程。嵌入模型的功能是要将水印信号加入到原始数据中，如下图所示。主要解决两个问题：一是数字水印的生成，可以是一串伪随机数，也可以是指定的字符串、图标等。二是嵌入算法，嵌入方案的目标是使数字水印在不可见性和鲁棒性之间找到一个较好的折中。



§7.2 数字水印

水印信号检测模型是用来判断某一数据中是否含有指定的水印信号，如下图所示。检测阶段主要是设计一个对应于嵌入过程的检测算法。检测的结果用来判断是否存在原水印，检测方案的目标是使错判与漏判的概率尽量小。提取时采用了密钥，只有掌握密钥的人才能读出水印。

提取数字水印设备只需要有打印机、扫描仪、计算机等设备。



§7.2 数字水印

数字水印的主要特性：

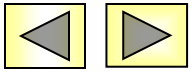
（1）鲁棒性

（2）水印容量

（3）安全性

（4）自恢复性

（5）不可见性



§7.2 数字水印

数字水印的主要特性：

（1）鲁棒性

是指水印信息能够抵抗应用过程中的各种破坏程度。比如对信息的传输、压缩、滤波、几何变换等处理后，数字水印不会被破坏，仍能从数字信息中提取出水印信息。

而用于完整性保护的水印，当内容发生改变时水印信息会发生相应的改变，从而可以鉴定原始数据是否被篡改。

（2）水印容量

（3）安全性

（4）自恢复性

（5）不可见性

§7.2 数字水印

数字水印的主要特性：

（1）鲁棒性

（2）水印容量

是指是指载体在不发生形变的前提下可嵌入的水印信息量。水印信息必须足以表示多媒体内容的创建者或所有者的标志信息或购买者的序列号，这样有利于解决版权纠纷。

水印容量和鲁棒性是相互矛盾的，水印容量的增加会带来鲁棒性的下降，鲁棒性不好就会导致检测结果的不可靠。

（3）安全性

（4）自恢复性

（5）不可见性

§7.2 数字水印

数字水印的主要特性：

（1）鲁棒性

（2）水印容量

（3）安全性

是指加入水印和检测水印的方法对没有授权的第三方应是绝对保密的，难以篡改或伪造，不可轻易破解。数字水印系统一般使用一个或多个密钥来确保水印安全。

（4）自恢复性

（5）不可见性

§7.2 数字水印

数字水印的主要特性：

（1）鲁棒性

（2）水印容量

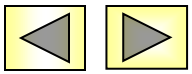
（3）安全性

（4）自恢复性

是指数字水印在原始数据经过较大的破坏或变换后，仍能从原数据中恢复出隐藏的水印。

（5）不可见性

对不可感知的数字水印来说，是指数字信息加入水印后不会改变其感知效果，即看不到数字水印的存在。



§7.2 数字水印

数字水印分类：

（1）按水印的可见性，可分为可感知的和不易感知的。

可感知水印最常见的例子是有线电视频道上的半透明标识，主要目的是明确标识版权，防止非法的使用。可感知水印应可适应各种图像显示器，对彩色和单色图像都是明显的，甚至对视觉有缺陷的人；应不特别掩盖其下的图像细节；可见水印应该是难以擦除的。

不易感知水印目的是为了将来起诉非法使用者，作为起诉的证据，以增加起诉非法使用者的成功率，保护原创造者和所有者的版权。不易感知水印往往用在商业用的高质量图像上，而且往往配合数据解密技术一同使用。

§7.2 数字水印

（2）按水印的特性，可分为鲁棒数字水印和易损数字水印。

鲁棒数字水印主要用于在数字作品中标识著作权信息，嵌入创建者或所有者的标示信息，或购买者的标示（即序列号）。发生版权纠纷时，创建者或所有者的信息用于标示数据的版权所有者，而序列号用于追踪违反协议而为盗版提供多媒体数据的用户。用于版权保护的数字水印要求有很强的鲁棒性和安全性，除在一般图像处理中生存外，还需能抵抗一些恶意攻击。

易损数字水印主要用于完整性保护，易损水印应对一般图像处理有较强的免疫能力，同时又要求有较强的敏感性，即既允许一定程度的失真又要能将失真情况探测出来。必须对信号的改动很敏感，根据水印的状态可以判断数据是否被篡改。

§7.2 数字水印

（3）按照水印的载体，可分为图像水印、视频水印、音频水印、文本水印和印刷水印等。

（4）按照检测方法，可分为明文水印和盲水印。

明文水印在检测过程中需要原始数据，而盲水印的检测只需要密钥，不需要原始数据。

一般来说，明文水印的鲁棒性比较强，但其应用受到存储成本的限制。目前学术界研究的数字水印大多数是盲水印。

§7.2 数字水印

（5）按照内容，可分为内容水印和标志水印。

内容水印是指水印本身也是某个数字图像（如商标图像）或数字音频片段的编码；标志水印则只对应于一个序列号。

内容水印的优势在于，如果由于受到攻击或其他原因致使解码后的水印破损，人们仍然可以通过视觉观察确认是否有水印。但对于标志水印来说，如果解码后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。

§7.2 数字水印

（6）按照用途，可分为版权保护水印、票据防伪水印、身份认证水印、篡改提示水印和隐蔽标识水印等。

版权标识水印是目前研究最多的一类数字水印。数字作品既是商品又是知识作品，这种双重性决定了版权标识水印主要强调隐蔽性和鲁棒性，而对数据量的要求相对较小。

票证防伪水印是一类比较特殊的水印，主要用于打印票据和电子票据、各种证件的防伪。

篡改提示水印是一种脆弱水印，其目的是标识原文件信号的完整性和真实性。

隐蔽标识水印的目的是将保密数据的重要标注隐藏起来，限制非法用户对保密数据的使用。

§7.2 数字水印

（7）按数字水印的隐藏位置，可分为时（空）域数字水印、频域数字水印、时/频域数字水印和时间/尺度域数字水印。

时（空）域数字水印是直接在信号空间上叠加水印信息，而频域数字水印、时/频域数字水印和时间/尺度域数字水印则分别是在离散余弦变换域、时/ 频变换域和小波变换域上隐藏水印。

随着数字水印技术的发展，各种水印算法层出不穷，水印的隐藏位置也不再局限于上述四种。应该说，只要构成一种信号变换，就有可能在其变换空间上隐藏水印。

§7.2 数字水印

典型数字水印算法：

（1）空域算法

首先把一个密钥输入到一个m-序列发生器来产生水印信号，再将此m-序列重新排列成2维水印信号，按像素点逐一插入到原始声音、图像或视频等信号中作为水印，即将数字水印通过某种算法直接叠加到图像等信号的空间域中。由于水印信号被安排在了最低位上，所以不会被人的视觉或听觉所察觉。

典型空域方法有最低有效位方法LSB（Least Significant Bits）、 Patchwork法和文档结构微调方法。

§7.2 数字水印

ⅰ）LSB方法是将水印直接嵌入到原始信号表示数据的最不重要的位置（最低有效位）中，这可保证嵌入的水印是不可见的。该算法的鲁棒性差，水印信息很容易被滤波、图像量化、几何变形的操作破坏。

ⅱ）Patchwork方法是一种基于统计的数据水印嵌入方案，其过程是用密钥和伪随机数发生器来选择N对像素点(a_i, b_i)，然后将每个a_i点的亮度值加δ，每个b_i点的亮度值减δ，整个图像的平均亮度保持不变，δ值就是图像中嵌入的水印信息。

该方法对JPEG压缩、FIR滤波以及图像裁剪有一定的抵抗力，但该方法嵌入的信息量有限。可以将图像分块，然后对每一个图像块进行嵌入操作。

§7.2 数字水印

iii）文档结构微调方法是在通用文档中隐藏特定二进制信息的技术。如轻微改变文档的字符或图像行距，水平间距，或改变文字特性等来完成水印嵌入。这种水印能抵御攻击，其安全性主要靠隐蔽性来保证。

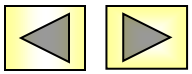
空域数字水印技术的优点是算法简单、速度快、容易实现，几乎可以无损的恢复载体图像和水印信息。其缺点是太脆弱，常用的信号处理过程，如信号的缩放、剪切等，都可以破坏水印。

（2）变换域算法

该类算法的基本思想是先对图像或声音信号等信息进行某种变换，在变换域上内嵌入水印，然后经过反变换而成为含水印的输出。在检测水印时，也要首先对信号作相应的数学变换，然后通过相关运算检测水印。这些变换包括：离散余弦变换（DCT）、小波变换（DWT）、付氏变换（FT或FFT）等。其中基于分块的DCT是最常用的变换之一，现在所采用的静止图像压缩标准JPEG也是基于分块DCT的。

（3）压缩域算法

水印检测与提取直接在压缩域数据中进行。



§7.2 数字水印

数字水印应用：

（1）数字作品的知识产权保护

将版权所有者的信息作为数字水印，嵌入在要保护的数字多媒体作品中，从而防止其他团体对该作品宣称拥有版权。此数字水印，应该具有不可察觉性、稳健性、唯一性等要求，还要能够抵抗一些正常的数据处理和恶意的攻击。

§7.2 数字水印

数字水印应用：

（1）数字作品的知识产权保护

（2）商务交易中的票据防伪

随着高质量图像输入输出设备的发展，特别是高精度彩色喷墨、激光打印机和高精度彩色复印机的出现，使得货币、支票以及其他票据的伪造变得更加容易。

传统商务向电子商务转化的过程中，大量过度性的电子文件（如各种纸质票据的扫描图像等），需要一些非密码的认证方式。数字水印技术可以为各种票据提供不可见的认证标志，从而大大增加了伪造的难度。

§7.2 数字水印

数字水印应用：

（1）数字作品的知识产权保护

（2）商务交易中的票据防伪

（3）证件的防伪

（4）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，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。

现有的信号拼接和镶嵌技术可以做到“移花接木”而不为人知，数据的篡改提示通过隐藏水印的状态可以判断声像信号是否被篡改。

§7.2 数字水印

数字水印应用：

（1）数字作品的知识产权保护

（2）商务交易中的票据防伪

（3）证件的防伪

（4）声像数据的隐藏标识和篡改提示

（5）隐蔽通信及其对抗

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。

§7.2 数字水印

数字水印应用：

（1）数字作品的知识产权保护

（2）商务交易中的票据防伪

（3）证件的防伪

（4）声像数据的隐藏标识和篡改提示

（5）隐蔽通信及其对抗

（6）使用控制

如DVD防拷贝系统，将水印信息嵌入DVD内容数据中，DVD播放机通过检测DVD数据中水印信息来判断其合法性和能否拷贝。

§7.2 数字水印

数字水印攻击方法：

（1）简单攻击

（2）同步攻击

（3）迷惑攻击

（4）删除攻击

（5）协议攻击

§7.2 数字水印

数字水印攻击方法：

（1）简单攻击

也可称为波形攻击或噪声攻击，就是通过对水印图像进行某种操作，削弱或删除嵌入的水印。

（2）同步攻击

（3）迷惑攻击

（4）删除攻击

（5）协议攻击

§7.2 数字水印

数字水印攻击方法：

（1）简单攻击

（2）同步攻击

试图使水印的相关检测失效，或使恢复嵌入的水印成为不可能。这类攻击的一个特点是水印实际上还存在于图像中，但水印检测函数已不能提取水印或不能检测到水印的存在。

（3）迷惑攻击

（4）删除攻击

（5）协议攻击

§7.2 数字水印

数字水印攻击方法：

（1）简单攻击

（2）同步攻击

（3）迷惑攻击

就是试图通过伪造原始图像和原始水印来迷惑版权保护。

（4）删除攻击

（5）协议攻击

§7.2 数字水印

数字水印攻击方法：

（1）简单攻击

（2）同步攻击

（3）迷惑攻击

（4）删除攻击

就是针对某些水印方法通过分析水印数据，穷举水印密钥，估计图像中的水印，然后将水印从图像中分离出来，并使水印检测失效。

（5）协议攻击

§7.2 数字水印

数字水印攻击方法：

（1）简单攻击

（2）同步攻击

（3）迷惑攻击

（4）删除攻击

（5）协议攻击

协议攻击的基本思想是盗版者在已加入水印版权的图像中加入自己的水印，并声称该图像的所有权是属于他的。

§7.2 数字水印

数字水印发展趋势：

- 结合智能体技术，开发水印Agent和自动追踪版权标志。
- 面向电子商务提供服务器端完整性保护和客户端数据认证。
- 建立水印认证中心，提供各种网上服务。
- 开发基于数字水印技术的数字作品电子销售系统，提供完整的安全与版权保护机制。
- 为各种付费点播服务，提供基于流技术的数字水印产品。
- 面向更广泛的数字媒体，如三维动画、数字地图等，开发基于数字水印的安全保护产品。
- 与密码尤其是数字签名技术结合，构造综合数据安全系统。
- 使用生物认证技术(如指纹、视网膜)构造专人标识水印。