1. 信息加密：

①将信息利用密钥把信息变换成密文，通过公开信道进行传输。

②信息加密通过密钥控制信息的使用权，从而隐藏秘密信息的内容，没有密钥就无法恢复明文，但没有隐藏秘密信息存在的事实

信息隐藏：

①把秘密信息隐藏于可以公开的信息中，使攻击者难以知道秘密信息的存在，从而掩盖通信过程中存在秘密信息的事实

②其主要目的并不是限制对信息的访问，而是确保宿主信息中隐藏的秘密信息不被改变或消除，从而在必要时提供有效的信息证明

2.

指载体在隐藏信息前后没有明显的差别，除非使用特殊手段，否则无法感知机密信息的存在，当然，个别场合也需要可见水印

3.

LSB：将隐秘信息嵌入到随机选择的取样点的值的最低几位上的最低有效位。该算法将隐秘信息存在最低位，相当于叠加一个能量微弱的信号，因而在视觉与听觉上很难以察觉。LSB空域算法对能隐藏较多的信息，但由于使用的不是重要的像素位，因此对信道干扰的鲁棒性较差。

DCT算法的PPT基本思想为，先计算原始图像的离散余弦变换，再将隐秘信息叠加到变换域上的系数上，这些系数通常为图像的低俗频分量。

4、

①鲁棒性水印：

鲁棒性水印是指恶意攻击下仍不能被修改，去除，主要用于版权标识，数字指纹也属于鲁棒性水印。

②脆弱性水印是指能够察觉载体信息的变化，并可根据被破坏的情况记录产品所受的攻击。通应用中还有半脆弱性水印，它对一些如压缩编码，滤波等正常信号处理具有鲁棒性。

③可见水印是指其嵌入的保护标识是可见的，最常见的可见水印为多媒体~~上的~~视频顶上的半透明图像，主要应用于标识版权，防止非法使用。

④不可见水印，是指将水印隐藏起来的水印，用于获悉窃盗版者的证据。

⑤私有水印和公有水印：

~~私有水印~~检测水印时必须采用原始数据作为参照的水印系统称为私有水印，不需要采用无原始数据进行检测称为公有水印。私有水印的缺是根据私有水印鉴别非法复制品时，必须连同原始信息作为证据。公有水印用于通过检测软件鉴别产品信息是否为盗版，应用较广　　应用较少

6.

⑥ 对称水印和非对称水印

非对称水印要求在公开水印检测算法和密钥时，任何人都能方便地检测出水印，但无法通过检测算法和密钥去除已嵌入的水印信息。

对称水印的嵌入与提取互逆，~~不知公开水印密钥，攻击者若不知道密钥，则难以删除水~~若攻击者知晓检测密钥，则都可轻易删除水印，因此水印密钥很少公开。

⑦ 多比特水印与单比特水印

单比特水印中只是表示"有水印"或"无水印"。嵌入多比特有意义的信息的水印称为多比特信息。多比特信息的应用价值更大。

5.

数字隐写的基本模型：

根据给定的算法和秘钥将秘密信息嵌入至图像、音频或视频中，等多媒体信号中，使得~~窃~~秘密信息在传输过程中不引起第三方或信道监控者的怀疑。接收方在得到载有秘密~~数字的~~信息数字的载体后，可根据算法提取和同样的密钥恢复~~出~~秘密信息。