

作业五

PB19111708 杨云皓

HWS.

1. 信息隐藏是把一个待保护的秘密信息隐藏在另一个称为载体的信息中。信息隐藏可以掩盖通信过程中存在秘密信息的事实，其主要目的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证明信息。而信息加密是利用密钥把信息变换为密文，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。

2. 透明性 (不可感知性): 载体在隐藏信息前后没有明显的差别，除非使用特殊手段，否则无法感知秘密信息的存在。

3. LSB 空域算法: 将秘密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，相当于叠加一个能量微弱的信号，因而在视觉和听觉上难以察觉。

DCT 变换域算法: 先计算原始图像的离散余弦变换，然后将秘密信息叠加到变换域中的系数上，这些系数通常为图像的低频分量。

4. 鲁棒性水印: 篡改及去除不能被修改、去除的水印，主要用于版权标识。
脆弱性水印: 能够察觉载体信息的细微变化，并可根据被破坏的情况下记录产品受到的攻击。

可见水印: 嵌入的保护标识可见；不可见水印则把水印信息隐藏起来。

私有水印: 用原始数据作为参照的水印系统，而不需要原始数据检测的是否有水印。

对称水印的嵌入与水印提供互逆；非对称水印在公开水印检测算法和密钥时，所有人可以但无法去除水印。

没有具体含义的水印信号是比特信息，而有多比特有意义信息的信号的水印是多比特水印。
空域图像水印、DCT 域图像水印

