信息安全导论第五次作业

PB17151767 焦培淇

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。
而信息隐藏则掩盖通信过程中存在秘密信息的事实，其主要目的并不是限止对信息的访问，而是确保隐藏的信息不被改变或消除，从而在必要时提供有效的证明信息。

2. ①空域算法
基本思想是由于隐秘信息在最低位，相当于叠加一个能量很弱的信号，因此在视觉和听觉上很难察觉
②变换域算法
先计算原始图像D的离散余弦变换，然后将隐秘信息叠加到变换域的系数上（不包括直流分量）
③压缩域算法
首先对DCT编码数据块中的每一个输入的Huffman编码进行解码和逆量化，以得到当前数据块的一个DCT系数。其次，把相应的隐秘信息值与其相加，从而得到隐秘信息叠加的DCT系数。再重新进行量化和Huffman编码；最后对新的Huffman码字的位数n_1与原来无隐秘信息的码字n_0进行比较，只有在$n_1 \leq n_0$时，才能传输隐秘信息。
④NEC算法
首先以密钥为种子来产生伪随机序列，其次对图像进行DCT变换，最后用该序列来调制该图像除直流分量外的1000个最大系数
⑤生理模型算法
利用视觉模型来确定与图像相关的调制掩膜，然后再利用其来嵌入隐秘信息。

3. ①鲁棒性水印和脆弱性水印：主要用于版权标识，对数字化产品实现版权认证，完整性认证和非法复制跟踪的保护功能。

②可见水印与不可见水印：主要用于明确版权标识，防止非法使用。

③私有水印与公有水印：用于鉴定非法复制品与信息产品是否为盗版。

4. 数字水印是自数字产品中嵌入版权拥有者的一些信息，当发生争议时能够有效确认出版权所属。数字指纹是在原产品中嵌入与用户有关的信息，产品提供者能够根据该信息对非法用户进行跟踪。