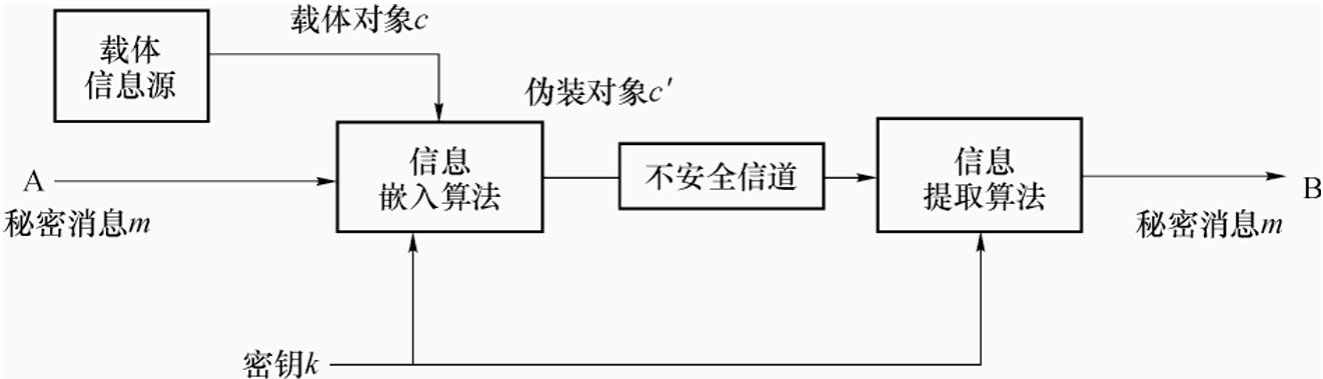


《信息隐藏技术》易错点总结

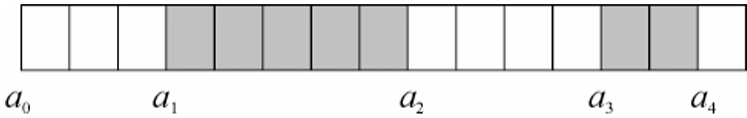
知识点

1. 信息隐藏的载体可以是**图像、音频、视频、网络协议、文本和各类数据**等。
2. **图像、视频、音频**利用了冗余来隐藏信息；而**文本、网络协议和各类数据**等无法利用冗余。
3. 隐写术考虑信息的**不可觉察性和不可检测性**，一般不考虑鲁棒性；数字水印对**鲁棒性**要求很高，但是对于容量和可不可见就随便了，两种类型都有。
4. 隐写术分类
 - 技术性的隐写术
 - 用头发掩盖信息
 - 使用书记板隐藏信息
 - 将信函隐藏在信使的鞋底、衣服的皱褶中，妇女的头饰和首饰中
 - 改变其中某些字母笔画的高度，或者在某些字母上面或下面挖出非常小的孔，以标识某些特殊的字母
 - 采用无形的墨水在特定字母上制作非常小的斑点
 - 微缩胶片
 - 化学方法的隐写术
 - 艺术作品中的隐写术
 - 语言学中的隐写术
 - 藏头诗
 - 卡登格子法
 - 乐谱
 - 应用于版权保护的隐写术
 - 核对校验图
 - 纸张中的水印
 - 纸币中的水印
5. 在图像、视频、声音中的信息隐藏和叠像术，都是利用了人类的视觉和听觉的特性来实现的。而在文本中的信息隐藏则不容易实现，由于文本的编码中没有任何冗余。
6. 数字水印和数字指纹
 - 数字水印：嵌入在数字作品中的一个版权信息，它可以给出作品的作者、所有者、发行者以及授权使用者等版权信息
 - 用于版权保护的数字水印：该具有不可察觉性、稳健性、唯一性
 - 用于盗版跟踪的数字指纹：嵌入了包含购买者信息的数字指纹
 - 用于复制保护的数字水印：对于嵌入了数字水印的产品，经正常授权的用户可以无障碍地使用，而对于非授权的用户（或非法复制、盗版的产品），该产品则无法正常使用。
 - 数字指纹：作为数字作品的序列码，用于跟踪盗版者
7. 信息隐藏三大指标——相互制约，不存在三个都很好的情况
 - 透明性：是首要特性，也称为不可感知性
 - 隐藏容量：在单位时间或一幅作品中能嵌入水印的比特数
 - 鲁棒性：也称稳健性，可以抗住对图像的修改
8. 对大多数语音信号而言，通常认为在**10-20ms**的时间范围内是**近似不变**的。因此可以确定，语音的数字模型是一个**缓慢时变**的线性系统，这个系统的参数在10-20ms的时间内是近似不变的。
9. 人耳对**频率相近**的声音无法区别，对**时间间隔太短**的声音无法区别，对**隐藏在强音后面的弱音**无法区别。
10. 人对一个声音是轻还是响的判断，与声音的**强度**有关，也与声音的**频率**甚至**波形**有关。
11. 当人耳听到两个强度不同的声音时，**强的声音的频率**成分会影响人耳对**弱的声音的频率**成分的收听，这种现象称为掩蔽效应。通常，**低音容易掩蔽高音**，而高音掩蔽低音较难。
12. 限幅的影响——**语音信号中的大部分信息都保存在其低幅值的部分**
 - 峰值削波：将幅度超过某一门限的值限制在门限上
 - 中心削波：将幅度小于某一门限的值置为零
13. 语音的质量
 - 清晰度：衡量语音中的字、单词和句子的清晰程度
 - 自然度：衡量通过语音识别讲话人的难易程度
14. 语音质量评价
 - 主观评价：**平均意见分（MOS）**——一共五个等级、音韵字可懂度测量（DRT）和满意度测量（DAM）
 - 客观评价：使用机器对语音质量进行评价
 - 基于输入——输出：就是把前后的做一下对比
 - 基于输出：就是只看后面的内容

15. **视觉范围**是指人眼所能感觉的亮度范围。这一范围非常宽，但是人眼并不能同时感受这样宽的亮度范围，当人眼适应了某一个平均的亮度环境后，它所能感受的亮度范围是**有限的**。并且，当**平均亮度比较适中时，能分辨的亮度的范围较大**；而当**平均亮度较低时，能分辨的亮度范围较小**。而即使是客观上相同的亮度，**当平均亮度不同时，主观感觉的亮度也不相同**。如同样的亮度，在白天和在黑夜，主观亮度感觉是不同的。
16. 人眼的分辨率：彩色的分辨率小于黑白的；运动速度快的小于运动速度慢的
17. 暗适应性：从亮的走到暗的；亮适应性：从暗的走到亮的。**通常亮适应性比暗适应性要快得多。**
18. 二维DWT变换：一级分解后的图像变为四部分：近似部分（LL），水平方向细节部分（HL），垂直方向细节部分（LH），对角线方向细节部分（HH），其中近似部分还可以进行下一级分解，得到图像的二级分解
19. 信息隐藏原理框图：



20. 信息隐藏的分类
- 无密钥信息隐藏：不需要预先约定密钥，事先约定嵌入算法和提取算法；为了提高无密钥信息隐藏技术的安全性，可以将秘密信息先进行加密再进行隐藏
 - 私钥信息隐藏：私钥伪装系统需要密钥的交换
 - 公钥信息隐藏：需要使用两个密钥：一个公开钥和一个秘密钥——**容易受到第三方攻击！**
21. 攻破一个信息隐藏系统可分为三个层次：**证明隐藏信息存在、提取隐藏信息和破坏隐藏的信息**
22. 判断时的四种情况：
- 准确判断隐藏有秘密信息
 - 准确判断没有隐藏信息
 - 从不含有秘密信息的载体中错误地检测出隐藏信息（称为第一类纳伪错误）
 - 在含有秘密信息的载体中错误地认为没有信息隐藏（称为第二类弃真错误）
23. 攻击情况分类
- 主动攻击：截获传递的伪装对象，修改后再发给接收方——破坏秘密信息的传递，篡改秘密信息——既看又改
 - 被动攻击：只是在监视和试图破译隐藏的秘密信息，并不对伪装对象进行任何改动——只看不改
 - 非恶意修改：这些就不是攻击了，就是一些正常的图像处理操作
24. 信息隐藏通信模型分类
- 根据噪声性质分类：加性噪声和非加性噪声信道模型
 - 主动攻击&被动攻击
 -
25. 根据信息隐藏的载体分类，可以分为**图像**中的信息隐藏、**视频**中的信息隐藏、**语音**中的信息隐藏、**文本**中的信息隐藏、**各类数据**中的信息隐藏
26. 替换技术就是利用这个原理，试图用**秘密信息比特**替换掉**随机噪声**，以达到隐藏秘密信息的目的
27. 人的**视觉和听觉系统**对于图像和声音的**最低比特位是不敏感的**
28. 回声隐藏巧妙地利用人类听觉系统（HAS）的时域掩蔽特性，隐藏时将数据文件分割，定义两种不同的时延，产生并输出回声信号；提取时利用倒谱相关测定回声间距，求出各段的倒谱自相关值
29. MP3编码算法流程大致可以分为四部分：**时频映射、心理声学模型、量化编码、帧数据流格式化**
30. MP3五种声道模式
- 单声道模式：只有一个声道的模式。
 - 双声道模式：具有两个相互独立声道的模式。
 - 立体声模式：具有两个声道且两个声道之间有一定关联的模式。
 - 强度立体声模式：是在立体声模式的基础上，对某些比例因子带的样值，仅对左右声道之和以及子带能量进行编码以获取更高的压缩率。
 - 和差立体声模式：对左右声道频域样值的和值及差值分别进行编码的立体声模式。
31. 频域样值经模式处理后，就进行量化和编码。所采用的是**非均匀量化**，量化过程处于两重迭代循环中，而且每循环一次都要对每个频域样值执行一次量化，**计算量较大**
32. 一个标准MIDI件基本上是由两部分组成：头块和音轨块。头块用来描述整个MIDI 文件基本信息。音轨块则包含一系列由MIDI消息构成的MIDI数据流。一个MIDI消息是由一个状态字节及多个数据字节构成。
33. MIDI消息分类
- 通道消息
 - 声音消息
 - 模式消息

- 系统消息
 - 公共消息
 - 实时消息
 - 专用消息
34. 改变MIDI音乐文件的部分声音消息并不影响MIDI文件的听觉效果，通过实验，改变声音开启的最低位比特、乐器编号的最低位比特和通道触动压力的低4比特位，都不会引起听觉差异，因此可在这三种声音消息中嵌入水印信息
35. 替换技术就是利用这个原理，试图用**秘密信息比特**替换掉**随机噪声**，以达到**隐藏秘密信息**的目的。
36. 对于数字图像和数字声音，其**最低比特位**或者**最低几个比特位**的改变，对整个图像或者声音没有明显的影响，因此替换掉这些不重要的部分，可以隐藏秘密信息。
37. LSB的操作方法：
- 在秘密信息嵌入结束后，再继续嵌入伪随机序列
 - 在一次嵌入之后，再重复嵌入秘密信息
 - 使用伪随机数来扩展秘密信息（比如随机间隔法）
38. 提高LSB方法的安全性
- 对秘密信息先加密后再隐藏
 - 多次重复嵌入，以提高信息的冗余度
 - 引入纠错编码技术，在秘密信息嵌入之前先进行纠错编码
39. 基于调色板的图像的LSB隐藏——鲁棒性都很差，随便修改就会出问题！
- 对调色板的颜色向量的LSB修改
 - 对图像数据（索引数据）的LSB修改
 - 调色板的排序方式对信息进行编码
 - 两个调色板索引
40. **游程编码**
- 在二值图像中，连续像素具有同种颜色的概率很高。因此，对每一行，不再直接地对每一个位置具有什么像素进行编码，而是对颜色变化的位置和从该位置开始的连续同种颜色的个数进行编码。
 - 

a_0 a_1 a_2 a_3 a_4
 - 编码： `< a 0 , 3 > < a 1 , 5 > < a 2 , 4 > < a 3 , 2 > < a 4 , 1 >`
 - 总结：就是说从什么时候开始变化了，就重新开一个新的头
 - 方法：在这样的编码中如何隐藏信息呢？仍然考虑在**最低比特位**的隐藏。现在修改二值图像的游程长度，如果第*i*个秘密信息位 m_i 是0，则令该游程长度为偶数；如果 m_i 是1，则修改游程长度为奇数。例如，可通过下面的方式进行：**如果 m_i 是0，而对应的游程长度是奇数，则把长度个数加1。另一方面，如果 $m_i = 1$ 并且长度是偶数，则把长度减1。**如果 m_i 的取值与长度个数的奇偶性相匹配，则不改变游程长度。在接收端，根据游程长度的奇偶性，就可以提取出秘密信息。
41. 在DCT域中的信息隐藏，可以有效地抵抗**JPEG有损压缩**
42. 这些DCT系数从低频到高频按照Zig-Zag次序排列，**第一个值（左上角）为直流系数，其余为交流系数**。DCT系数中，**左上角部分为直流和低频系数，右下角部分为高频系数，中间区域为中频系数**。中低频部分包含了图像的大部分能量，也可以说，对人的视觉最重要的信息部分，**都集中在图像的中低频**。
43. 经过一级小波分解后得到的四个部分，**左上为低频近似部分，右上为水平方向细节部分，左下为垂直方向细节部分，右下为对角线方向细节部分**。可以看出，图像的主要能量集中在**低频部分**
44. 数字水印的特点：
- 安全性：难以被发现、擦除、篡改或伪造
 - 可证明性：能为宿主数据的产品归属问题提供完全和可靠的证据
 - 不可感知性：在宿主数据中隐藏的数字水印是不能被感知的。一是指感观上的不可感知；二是指统计上的不可感知。
 - 稳健性：数字水印应该难以被擦除。
45. 数字水印方案包括三个要素：**水印本身的结构，水印的加载过程，水印的检测过程**。
46. 数字水印的分类：
- 从水印的载体上分类
 - 图像水印
 - 视频水印
 - 音频水印
 - 软件水印
 - 文档水印
 - 从水印的加载方法上分类
 - 空间域水印：比如LSB或者拼凑法、文档结构微调方法等等
 - 变换域水印：DCT变换、小波变换、傅里叶变换等
 - 从水印的检测方法上分类
 - 私有水印（非盲水印）和公开水印（盲水印）

■ 私钥水印和公钥水印

47. 数字水印的应用：

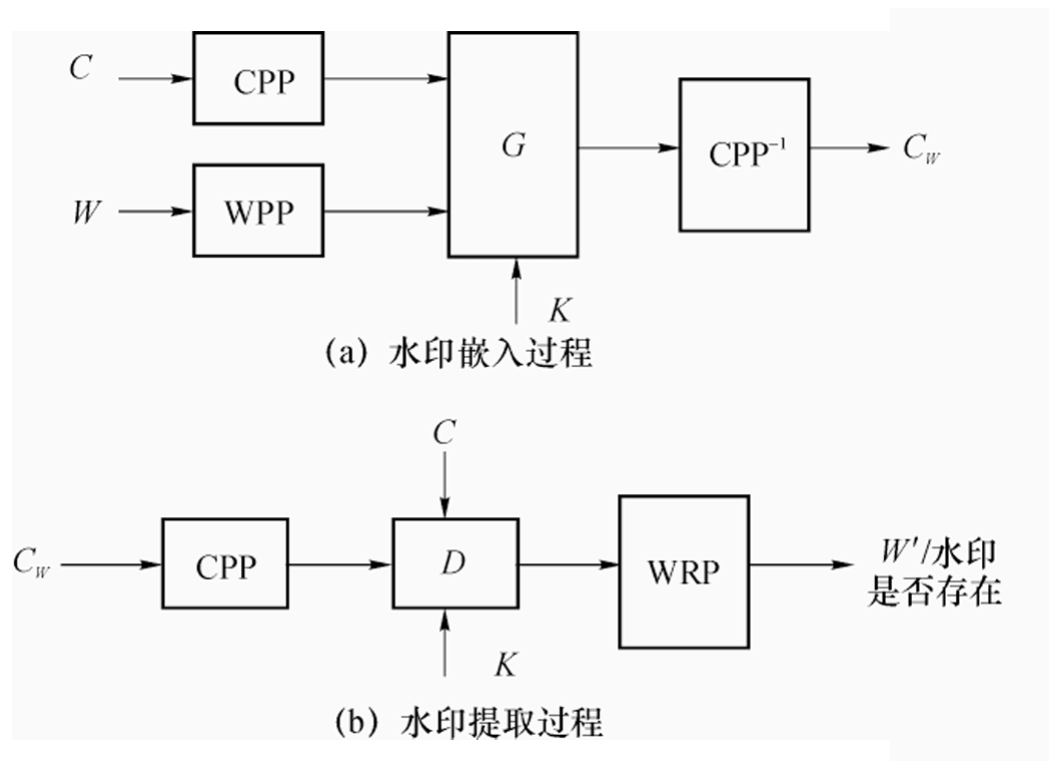
- 版权保护
- 数字指纹
- 认证和完整性校验
- 内容标识和隐藏标识
- 使用控制
- 内容保护
- 完全不可见通信

48. 数字水印从其表现形式上可以分为几大类

- 一串有意义的字符
- 一串伪随机序列
- 一个可视的图片

49. 一方面，选择水印时应该考虑水印本身能够**容忍一定的误码**，比如第二类 and 第三类水印；另一方面，设计水印算法时，要考虑水印算法的**抗攻击能力**，同时还要考虑**水印检测方式**。

50. 数字水印框架：

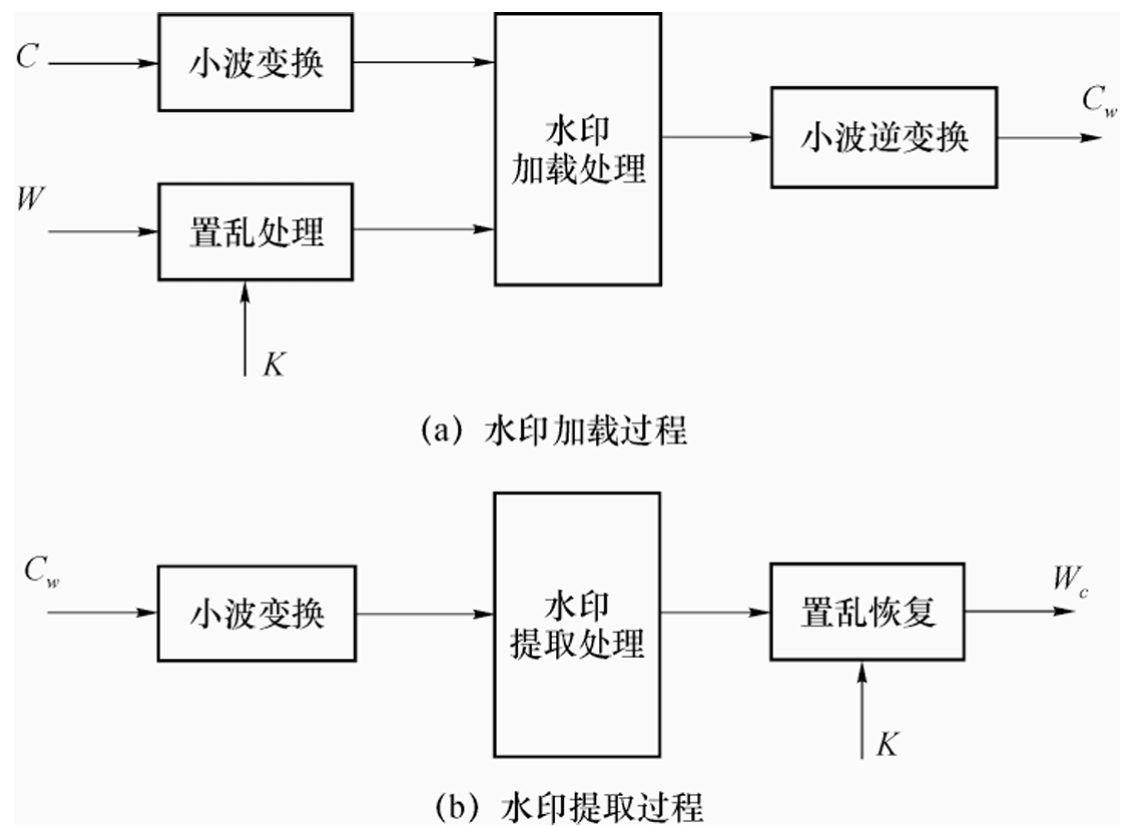


51. 水印嵌入位置的选择，考虑两个问题

- 安全性的问题
- 对载体质量的影响问题

52. 水印嵌入位置选择：在纹理较复杂的地方以及物体的边缘区域；嵌入水印不影响感观效果

53. 小波变换示意图：



54. 脆弱性数字水印的基本特征：检测篡改，稳健性与脆弱性，不可感知性与感知性，可靠性

55. 脆弱性水印划分为以下四个层次

- 完全脆弱性水印
- 半脆弱水印

- 图像可视内容鉴别
 - 自嵌入水印
56. 软件水印：
- 静态数据水印：将水印信息嵌入在程序中的一些数据中
 - 静态代码水印：利用目标代码中包含冗余信息嵌入水印
 - Easter Egg水印：一个输入产生一个输出
 - 动态数据结构水印：堆、栈或者全局变量域
 - 动态执行过程水印：在特定的输入下运行
57. 人耳听觉系统（HAS）要比人眼视觉系统（HVS）灵敏得多
58. 根据水印加载方式的不同，音频数字水印可以分为四类：**时间域数字水印、变换域数字水印、压缩域数字水印以及其他类型的数字水印**
59. 音频水印按照水印嵌入的位置也可以分为三类：
- 在原始音频信号中嵌入
 - 在音频编码器中嵌入，这种方法稳健性较高，但需要复杂的编码和解码过程，运算量大，实时性不好
 - 在压缩后的音频数据流中直接嵌入，这种方法避免了复杂的编解码过程，但稳健性不高，而且能够嵌入的水印容量不大
60. 对图像水印的分类方法原则上也可以推广到对视频水印的分类。按**嵌入策略**分，视频水印可分为**空间域和变换域**两种；按**水印特性**分，可分为**稳健性水印、脆弱性水印和半脆弱性水印**；按**嵌入位置**分，可分为**在未压缩域中嵌入、在视频编码器嵌入、在视频码流中嵌入**；按**水印的嵌入与提取是否跟视频的内容相关**分，可分为**与视频内容无关的第一代视频水印和基于内容的第二代视频水印方案**；按**视频载体采用的压缩编码标准**分，可分为**基于MPEG1或MPEG2标准的视频水印、基于MPEG4标准的视频水印和基于其他压缩标准**。
61. 视频水印根据嵌入的策略一般可以分成三种，**在未压缩域中嵌入、在视频编码器中嵌入和在视频码流中嵌入**
62. 隐写分析分类
- 根据适用性：专用隐写分析和通用隐写分析
 - 根据已知消息：唯隐文攻击 已知载体攻击 已知消息攻击 选择隐文攻击 选择消息攻击 已知隐文攻击
 - 根据采用的分析方法：感官分析 统计分析 特征分析
 - 根据最终的效果：被动隐写分析 主动隐写分析
63. 信息隐藏分析的目的有三个层次：**回答是否有隐藏 提取秘密信息 破坏秘密信息**
64. 被动隐写分析方法的评价：准确性 适用性 实用性 复杂度
65. 三种分析的详细说明
- 卡方分析：LSB隐写会使值对出现次数趋向于相等
 - RS分析：对于自然图像来说，非负和非正翻转同等程度增加图像的混乱程度；对于隐写图像来说，采用非负翻转，规则图像块的比例与不规则图像块的比例的差值随隐写率的增大而减小
 - GPC分析：对于自然图像， N_0 和 N_1 的比值近似为1；但是对于隐写图像来说，这个比例会随着隐写率的增大而增加
66. 对于数字水印的攻击，分为以下四种：
- 去除攻击：直接攻击稳健性的数字水印
 - 表达攻击：就是将水印变形，让检测器检测不出来
 - 解释攻击：就是让一个水印有两个不同的解释
 - 法律攻击：利用法律上的漏洞
67. 水印攻击软件：
- Unzign
 - StirMark
 - CheckMark
 - OptiMark

错题整理

- 人类视觉系统对于亮度变化大区域的敏感度要大于亮度变化小的区域。亮度变化大的区域称为**高信息量区域**，亮度变化小的区域称为**低信息量区域**。前者又可进一步划分为**关键区域**（亮度突然变化的区域，一般是图像中包含信息量最大，对人们的理解最为重要的部分）和**纹理区域**（具有规则变化的区域，人眼会产生一定的适应性，以至于很容易在人的意识中遗忘）
- 数字水印从特性上可以划分为**鲁棒性水印和脆弱性水印**。从检测过程中是否需要原始数据可以分为**明文检测水印和盲水印**。
- 检测经打印扫描后图像中的水印有较大难度，其中一个主要原因是：打印过程中，数字信号转变为模拟信号采用半色调处理；而扫描过程中，模拟信号转变为数字信号时引入噪声，称为**像素失真**。
- 信息隐藏的研究也分为三个层次：**应用技术研究、应用基础研究、基础理论研究**。
- 结构微调法是对文本的空间特征进行轻微调整来嵌入秘密信息的方法，一般采用的方法是**行移位编码、字移位编码和特征编码**三种方法。
- 使用FFT2对信号作离散傅里叶变换获得二维矩阵，水平方向从左至右频率逐渐**增加**。
- 一般使用倒谱自相关检测回声延迟，因为其准确度高，且算法复杂度低——是错误的
- DCT变换以小块为基本单位，高通滤波后，隐写图像小块间的不连续性更加明显——正确
- 观察隐写图像的灰度直方图可以发现值对频度趋于相等——错误

- DCT系数量化是分块进行的，不同小块之间会有一定的不连续性，F5隐写后，小块间的不连续性更明显。——正确
- 若隐写时使用的不是普通LSB算法，而是预留了部分像素用于平衡由隐写带来的直方图的变化，那么RS分析可能失效——错误
- 在二值图像中利用黑白像素的比率隐藏信息时，可以考虑引入稳健性参数，假设经过测试，已知某传输信道误码率的概率密度：误码率低于1%的概率为0.8，误码率低于5%的概率为0.9，误码率低于10%的概率为0.95，…。则：为保证隐藏信息正确恢复的概率不低于90%，稳健性参数至少为**10%**
- 对隐写图像，应用非负翻转后，规则与不规则图像块比例的差值随隐写率的增大而减小——正确
- 对隐写图像，应用非正翻转后，R-m与S-m的差值随隐写率的增大而减小——错误
- 心理声学实验表明，人耳难以感知位于强信号附近的弱信号，这种声音心理学现象称为掩蔽。强信号称为被掩蔽音，弱信号称为掩蔽音——错误，说反了
- 从语音信号中取一帧信号，称为加窗。两帧信号必须重叠，重叠的部分称为帧移，通常是帧长的1/3——错误
- 窗函数的形状和长度对语音信号分析无明显影响，常用RectangleWindow以减小截断信号的功率泄漏——错误
- 波形编码通过对语音信号特征参数的提取并编码，力图使重建的语音信号具有较高的可懂度——错误
- 语音信号的幅度值的分布满足均匀分布，对语音信号进行PCM编码时，适合采用均匀量化——错误，不是均匀量化

综合题

1. 调色板图像像素位置处存储的不是真正的颜色分量，而是颜色编号。图像中出现的颜色及其编号存储在调色板中。若用 $R、G、B$ 表示彩色图像颜色分量，则可用近似公式 $Y = 0.3R + 0.5G + 0.1B$ 来计算该颜色的近似亮度。已知某彩色图像调色板共有 4 种颜色，分别是 $(167, 142, 172)、(162, 175, 210)、(214, 167, 172)、(176, 205, 231)$ ，其序号为 $0 \sim 3$ ，请利用近似亮度计算公式并采用 LSB 算法在下列像素亮度域上隐藏秘密信息 0101。4 个像素的颜色序号为 3、2、2、0。要求写出过程及隐藏后，上述像素的颜色序号。（隐藏步骤为：根据近似亮度公式计算四种颜色所对应亮度，并按升序排列，在亮度域上进行 LSB。假设颜色序号按亮度排序为 3012，即 3 号颜色：176、205、231 的亮度序号为 0，此时，若在颜色序号为 3 的像素上隐藏秘密信息 1，由于 3 号颜色的亮度序号 0 的最低比特位与秘密信息不同，因此亮度序号替换为 1，对应的颜色编号为 0，这样隐藏信息后，样点颜色由 3 号变为 0 号。）

2. 现接收到一使用 PVD 算法隐藏秘密信息的 8 bit 灰度图像（已知灰度划分为 6 个区域： $[0, 7]、[8, 15]、[16, 31]、[32, 63]、[64, 127]、[128, 255]$ ），并且从隐藏区域计算出的相邻像素灰度差值为：13、30、129，则可从中提取的秘密信息是什么？（提示：若原始载体相邻像素灰度差值为 11，则其差值落入区间 $[8, 15]$ ，区间宽度为 8，可以隐藏 $\log_2(8) = 3$ bit 秘密信息，假设秘密信息为 $B(111) = D(7)$ ，则隐藏后像素灰度差值应该调整为 $7 + 8 = 15$ ；反之，若携密载体相邻像素灰度差值为 11，其差值也落入区间 $[8, 15]$ ，区间宽度为 8，则隐藏的消息长度为 $\log_2(8) = 3$ bit，因此秘密信息为 $D(11 - 8) = D(3) = B(011)$ 。）

3. 已知某图像轮廓的游程编码为： $\langle a_0, 5 \rangle \langle a_1, 4 \rangle \langle a_2, 3 \rangle \langle a_3, 7 \rangle$ 。现需修改游程长度以隐藏秘密信息，约定隐藏 0 时游程长度为偶数（约定长度在 $2i$ 和 $2i + 1$ 之间翻转，例如， $2 - 3, 4 - 5, \dots$ ），则隐藏秘密信息 1100 后，游程编码变为什么？

4. F5 算法对量化 DCT 系数采用类似 LSB 的技术隐藏秘密信息。

第一，F5 约定在非零系数上隐藏秘密信息，若隐藏后系数变为零，则在下一系数继续隐藏同一秘密信息。

第二，F5 算法中，正奇负偶表示 1，负奇正偶表示 0，如果要隐藏的比特与系数所表示的比特一致，则不改变系数，否则，保持该系数符号，将其绝对值减 1。

第三，F5 算法采用了矩阵编码技术。 $2^k - 1$ 个像素最多修改 1 个像素就可以嵌入 k 比特秘密信息。以 $k = 2$ 为例，用 $a_1、a_2、a_3$ 表示原始载体， $x_1、x_2$ 表示要嵌入的秘密信息。则若 $x_1 = a_1 \oplus a_3, x_2 = a_2 \oplus a_3$ ，不改变原始数据；若 $x_1 \neq a_1 \oplus a_3, x_2 = a_2 \oplus a_3$ ，改变 a_1 ；若 $x_1 = a_1 \oplus a_3, x_2 \neq a_2 \oplus a_3$ ，改变 a_2 ；若 $x_1 \neq a_1 \oplus a_3, x_2 \neq a_2 \oplus a_3$ ，改变 a_3 。

请根据以上信息求解下述问题：

(1) 定义载体数据利用率(R)为秘密信息数/隐藏秘密信息所需样点数,即,若隐藏 N 比特秘密信息所要 M 个样点,则 $R=N/M$,问: $k=2$ 时,F5 算法的载体数据利用率为多少? 普通 LSB 算法载体数据利用率为多少?

(2) 定义嵌入效率(E)为嵌入比特数/平均修改长度,则 $k=2$ 时,F5 算法的嵌入效率为多少? 普通 LSB 算法嵌入效率为多少? 试根据矩阵编码的思想,推算 $k=3$ 时的嵌入效率。

(3) 若要嵌入 010111,可用的 DCT 系数为:7,27,-1,1,-22,-14,4,8,-7,则使用 F5 算法嵌入信息后,DCT 系数为多少? 若其他步骤相同,但不采用矩阵编码,则嵌入信息 101011 后 DCT 系数为多少?

(4) 若已知系数 1,24,-1,1,-26,-14,4,2,-11 使用 F5 算法嵌入了秘密信息,则从中可提取的信息为什么?

5. 调色板图像格式可简单理解为两个逻辑区域:一个区域为“调色板”,存储颜色及颜色编号;一个区域为图像数据,存储像素值,由于“调色板”区域已经存储了所有可能出现的颜色,因此该区域不需要存储颜色,只需存储颜色在调色板中的编号。

EzStego 是一种简单有效的隐写工具,可用于调色板图像。其算法思路是在亮度域上进行 LSB。详细步骤:首先将调色板颜色按照亮度进行升序排列,然后为每个颜色分配一个亮度序号,最后在亮度域进行 LSB。例如:若编号为 3、7 的颜色其亮度相邻,得到的编号是 4、5,则在值为 3 的像素处嵌入秘密信息 1,由 3 号颜色对应的亮度号 4 可知,LSB 后,4 号亮度变为 5,5 号亮度对应 7 号颜色,所以,值为 3 的像素处嵌入秘密信息 1 后,值变为 7。

假设颜色亮度可通过近似公式为: $Y=0.3 \times R+0.6 \times G+0.1 \times B$,且已知某图像调色板为:0:<24,231,117>,1:<40,215,206>(青),2:<251,241,57>(明黄),3:<238,70,87>(桃红)。请根据算法解答下列问题。

(1) 若在值为 203231 的像素上使用 EzStego 隐藏比特“111000”,则像素值变为多少?

(2) 若已知图像经过 EzStego 处理,且像素值为 213031,则可提取秘密信息比特为多少?

6. BPCS 位平面复杂度分割算法将信息嵌入变化剧烈、复杂度较高的位平面小块,使得秘密信息可以加载在多个位平面。复杂度定义为所有相邻像素对中取值不同的像素对数目。例如, 8×8 的小块,复杂度为 0~112。嵌入信息时,将复杂度大于 αC_{\max} 的位平面小块用于负载秘密信息,将秘密信息组成位平面小块,如果其复杂度大于 αC_{\max} ,则直接替换原位平面小块;如果其复杂度小于等于 αC_{\max} ,则需要作共轭处理(将秘密信息小块与棋盘状小块作异或,共轭处理后复杂度为 $\alpha C_{\max} - c$),并记录下哪些小块经过共轭处理。现假设像素灰度值为 3 bit 量化,小块尺寸为 2×2 ,棋盘状小块比特按行优先顺序为 1001, α 为 0.45。请根据算法解答下列问题:

(1) 按行优先方式,信息序列为 1001 1111 1010,像素为 7,6,4,1,请回答这些像素能隐藏多少比特数据? 隐藏后像素值变为多少?(约定:先嵌入较低比特平面,若需共轭,请注明哪个平面作了共轭处理。)

(2) 若像素 7,6,4,1 已使用 BPCS 算法嵌入了秘密信息,并且所有平面均没有使用共轭处理,则从中能提取的秘密信息为什么?

(3) 算法要求 $\alpha < 0.5$,试分析该要求的理由。(提示:考虑共轭处理环节)并请指明调整参数 α 对算法的哪项指标有影响。为什么?

