《信息隐藏技术》课程期末复习资料

《信息隐藏技术》课程讲稿章节目录：

数字水印攻击的分类

去除攻击

表达攻击

解释攻击

法律攻击

水印攻击软件

一、客观部分：

（一）单项选择题：

1.下列关于回声隐藏算法描述不正确的是( )。

A. 回声隐藏算法利用时域掩蔽效应，在原声中叠加延迟不同的回声代表 0，1 bit。

B. 可以使用自相关检测回声提取 0、1 bit，但由于信号自身的相关性，回声延迟过小时，其相关度的峰值容易被淹没。

C. 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。

D. 回声隐藏算法的特点是听觉效果好，抗滤波重采样等攻击能力强，但嵌入容量不大。

答案：C

2.评价隐藏算法的透明度可采用主观或客观方法，下面说法正确的是( )。

A. 平均意见分是应用得最广泛的客观评价方法。

B. B. MOS 一般采用 3 个评分等级。

C. 客观评价方法可以完全替代主观评价方法。

D.图像信息隐藏算法可用峰值信噪比作为透明度客观评价指标。

答案：D

3.（）指的是同一个作品被不同用户买去，售出时不仅嵌入了版权所有者信息，而且还嵌入了购买者信息，如果市场上发现盗版，可以识别盗版者。

A. 用于版权保护的数字水印

B. 用于盗版跟踪的数字指纹

C. 用于拷贝保护的数字水印

D. （A、B、C）都不是

答案：B

4.（）是在文件格式中找到某些不影响载体文件的位置，嵌入要隐藏的数据。

A. 统计隐藏技术

B. 变形技术

C. 文件格式隐藏法

D. 扩展频谱技术

答案：C

是一种重要的信息隐藏算法，下列描述不正确的是(　)。

A. LSB 算法简单，透明度高，滤波等信号处理操作不会影响秘密信息提取。

B. LSB 可以作用于信号的样点和量化 DCT 系数。

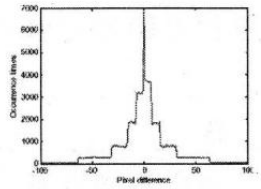
C. 对图像和语音都可以使用 LSB 算法。

D. LSB 算法会引起值对出现次数趋于相等的现象。

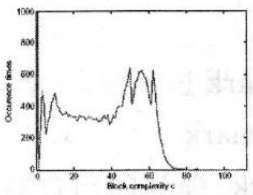
答案：A

6.通过调整相邻像素灰度差值可以隐藏秘密信息，称为 PVD 隐写算法。根据算法原理，下面哪一张直方图可能是经过 PVD 算法隐写后的图像生成的(　)。

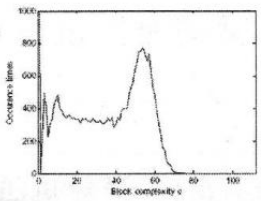
A.



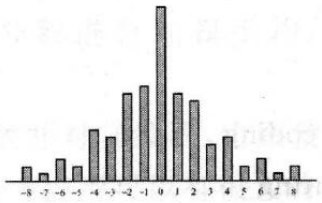
B.



C.



D.



答案：A

7. 卡方分析的原理是（ ）。

A. 利用图像空间相关性进行隐写分析。

B. 非负和非正翻转对自然图像和隐写图像的干扰程度不同。

C. 图像隐写后，灰度值为 2i 和 2i+1 的像素出现频率趋于相等。

D. 图像隐写后，其穿越平面簇 z=0. 5，2. 5，4. 5，…的次数增加。

答案：C

8. 下列描述不正确的是( )。

A. 限幅影响语音清晰度。

B. 峰值削波门限为幅值 1/3 时，语音清晰度受很大影响。

C. 中心削波门限为幅值 1/3 时，语音清晰度几乎全部丧失。

D. 语音信号大部分信息保存在幅值较低部分。

答案：B

9. 下列关于半脆弱水印的描述，不正确的是( )。

A. 半脆弱水印是特殊的水印，它的稳健性介于鲁棒水印和脆弱水印之间，可以判定图像经受的是普通信号处理操作还是图像内容篡改操作。

B. LSB 算法可作为半脆弱水印算法，对图像的操作，无论是否影响图像内容，都将导致该算法判定图像被篡改。

C. P. W. Wong 水印系统是基于公钥图像认证和完整性数字水印系统，实质是脆弱水印系统。

D. 一些半脆弱水印算法是由鲁棒水印算法演变来的。

答案：B

10. 关于 F5 算法隐写过的 JPEG 图像，下列哪种说法不正确( )。

A. 与原始图像相比，隐写图像的 DCT 量化系数直方图更"瘦"、更"高"。

B. 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。

C. 观察隐写图像的灰度直方图可以发现值对频度趋于相等。

D. 隐写图像的 DCT 量化系数直方图不会出现偶数位置色柱比奇数位置色柱更突出的现象。

答案：C

11. 下列哪些不是描述信息隐藏的特征（ ）。

A. 误码不扩散。

B. 隐藏的信息和载体物理上可分割。

C. 核心思想为使秘密信息"不可见"。

D. 密码学方法把秘密信息变为乱码，而信息隐藏处理后的载体看似"自然"。

答案：B

12. 下面哪个领域不是数字水印应用领域（ ）。

A. 版权保护

B. 盗版追踪

C. 保密通信

D. 复制保护

答案：C

13. 关于 F5 隐写算法，下列描述正确的是（ ）。

A. 算法引入了矩阵编码，提高了载体数据利用率，减少了 LSB 算法的修改量。

B. 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。

C. 隐写会导致奇异颜色数目小于与其对应的颜色数目，嵌入量越大，这种差距越明显。

D. 隐写导致值对出现次数趋于相等。

答案：B

14. 攻击者只有隐蔽载体，想从中提取秘密信息，属于（ ）。

A. Known-cover attack

B. Stego-only attack

C. Chosen-message attack

D. Known-message attack

答案：B

15. 下列关于相位隐藏算法描述正确的是（ ）。

A. 相位隐藏利用了人耳听觉系统特性：HAS 能察觉语音信号中的微弱噪声，但对其相位的相对变化不敏感。

B. 虽然样点的绝对相位发生了变化，但相邻片断间的相对相位保持不变，可以获得较好隐藏效果。

C. 采用改算法，每秒一般可隐藏 8000 bit 秘密信息。

D. 相位隐藏的原理是利用掩蔽效应，利用人耳难以感知强信号附近的弱信号来隐藏信息。

答案：B

16. 信息隐藏可以采用顺序或随机隐藏。例如，若顺序隐藏，秘密信息依此嵌入到第 1， 2，3，…个样点中，而随机方式，秘密信息的嵌入顺序则可能是第 10，2，3，129，…个载体中。 已知发送方采用随机方式选择隐藏位置，算法选择 LSB，携带秘密信息的载体在传输过程中有部分发生了变化，则下列说法正确的是( )。

A. 虽然秘密信息采用信息隐藏的方法嵌入，但嵌入位置由密码学方法确定。根据密码学特性：即使只错一个比特，信息也无法正确解码，可以判定接收方提取到的全是乱码。

B. 收发双方一般采用其他信道传输密钥，出现部分传输错误的不是密钥，因此，接收方能够正确提取秘密信息。

C. LSB 算法鲁棒性差，嵌入到传输错误的那部分载体中的秘密信息，很可能出现误码，但根据信息隐藏"误码不扩散"的特性可知，其他部分的秘密信息还是能够正确恢复的。

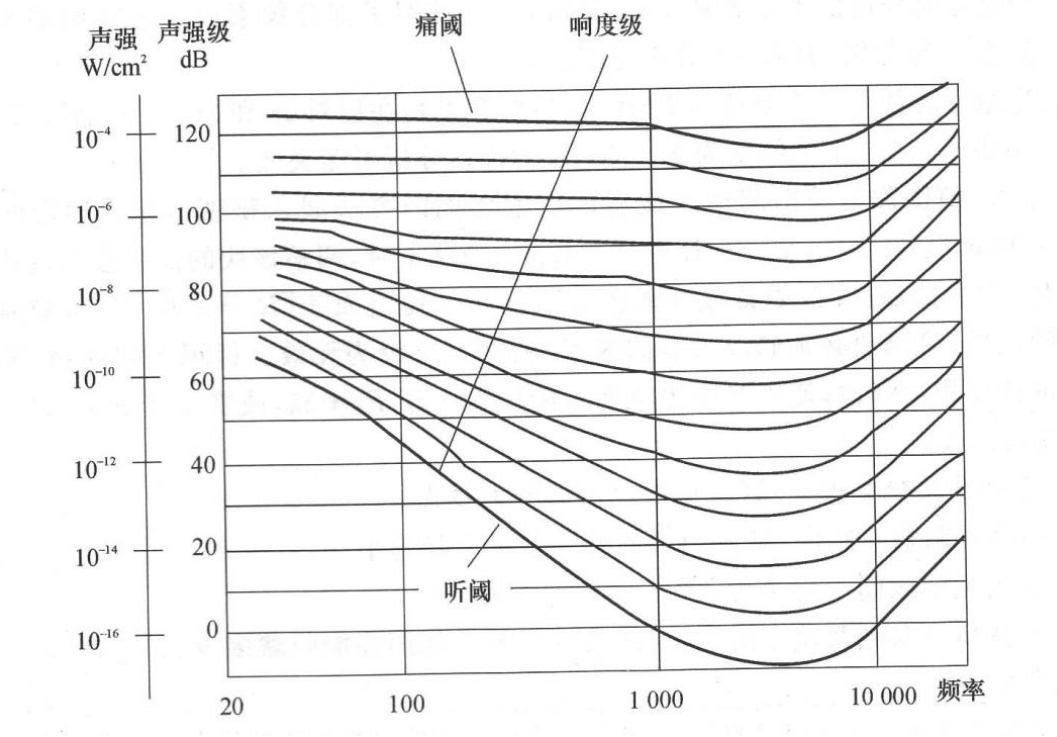
D. 信息隐藏的核心思想是使秘密信息不可见。既然采用信息隐藏的方法传输秘密信息，那么传输的安全性只取决于攻击者能否检测出载体携带了秘密信息，因此，采用随机隐藏的方式不会增强通信的安全性。

答案：C

17. 某算法将载体次低有效比特位替换为秘密信息，已知某灰度图像经过了该算法处理，其中三个样点的灰度值为 132、127 和 136，则可从中提取的秘密信息为( )。

答案：C

18. 下图为等响曲线图，其横轴表示单音的频率，单位为 Hz。纵轴表示单音的物理强度——声强，单位为 W /cm2 (纵轴左侧坐标单位) ，为便于表示，也常用声强级(10-16W/cm2 为 0dB)，单位为 dB(纵轴右侧坐标单位)。两单位可直接换算，例如，10-14W/cm2 对应 101og(10-14/10-16)dB=20dB。图中曲线为响度级，单位为方。离横轴最近的曲线响度级为 0 方，称听阈，是人在安全环境下恰好能够听见的声音;离横轴最远的曲线响度级为 120 方，称痛阈，人耳听见这样的声音会疼痛。则下列描述不正确的是( )。



A. 根据图中数据，人耳难以感知 100 Hz， 10 dB 的单音，因为其响度级在听阈之下。

B. 根据图中数据，100 Hz，50 dB 左右的单音和 1 000 Hz，10 dB 的单音在一条曲线上， 因此，人耳听来，这两个单音同等响亮。

C. 图中各条等响曲线在 20~1 000 Hz 区间内呈下降趋势，说明该区间内，人耳对频率较低的单音更加敏锐。

D. 由图可知，不同频率相同声强级的单音响度级不同，说明响度是人耳对声音强度的主观感受，而人耳对不同频率的声音的敏感程度不同。

答案：C

19. 对二值图像可采用调整区域黑白像素比例的方法嵌入秘密信息。确定两个阈值 R0<50%和 R1>50%，以及一个稳健性参数 λ。隐藏 1 时，调整该块的黑色像素的比使之属于[[R1，R1+λ]；隐藏 0 时，调整该块黑色像素的比例使之属于[R0 一 λ，R0]。如果为了适应所嵌入的比特，目标块必须修改太多的像素，就把该块设为无效。标识无效块：将无效块中的像素进行少量的修改，使得其中黑色像素的比例大于 R1+3 λ，或者小于 R0 -3 λ。则下列说法不正确的是( )。

A. 稳健性参数 λ 越大，算法抵抗攻击的能力越强。

B. 稳健性参数λ越大，算法引起的感官质量下降越小。

C. 引入无效区间主要是为了保证算法的透明性。

D. 算法所有参数都确定时，也不能准确计算一幅图像能隐藏多少比特信息。

答案：B

20. 掩蔽效应分为同时掩蔽和(　)。

A. 频域掩蔽

B. 超前掩蔽

C. 滞后掩蔽

D. 异时掩蔽

答案：D

21. 异时掩蔽可分为(　)和滞后掩蔽。

A. 同时掩蔽

B. 时域掩蔽

C. 频域掩蔽

D. 超前掩蔽

答案：D

22. 掩蔽效应分为频域掩蔽和（　）。

A. 同时掩蔽

B. 时域掩蔽

C. 滞后掩蔽

D. 异时掩蔽

答案：B

23. 掩蔽效应分为（ ）和异时掩蔽。

A. 同时掩蔽

B. 时域掩蔽

C. 频域掩蔽

D. 超前掩蔽

答案：A

24. 异时掩蔽可分为超前掩蔽和（ ）。

A. 同时掩蔽

B. 频域掩蔽

C. 滞后掩蔽

D. 异时掩蔽

答案：C

25. 某算法将载体次低有效比特位替换为秘密信息，已知某灰度图像经过了该算法处理。其中三个样点的灰度值为131、126、137，则可从中提取的秘密信息为(　)。

,0,1　　,1,0　　,1,0　　,0,1

答案：C

26. 下面哪个领域不是数字水印应用领域(　)。

A. 盗版追踪

B. 版权保护

C. 复制保护

D. 保密通信

答案：D

27. 下列哪种隐藏属于文本语义隐藏(　)。

A. 在文件头、尾嵌入数据

B. 句法变换

C. 对文本的字、行、段等位置做少量修改

D. 修改文字的字体来隐藏信息

答案：B

28. 卡方分析的原理是(　)。

A. 非负和非正翻转对自然图像和隐写图像的干扰程度不同。

B. 利用图像空间相关性进行隐写分析。

C. 图像隐写后，其穿越平面簇 z=0. 5，2. 5，4. 5，…的次数增加。

D. 图像隐写后，灰度值为 2i 和 2i+1 的像素出现频率趋于相等。

答案：D

29. LSB 是一种重要的信息隐藏算法，下列描述不正确的是(　)。

A. LSB 算法会引起值对出现次数趋于相等的现象。

B. 对图像和语音都可以使用 LSB 算法。

C. LSB 可以用于信号的样点和量化 DCT 系数。

D. LSB 算法简单，透明度高，滤波等信号处理操作不会影响秘密信息的提取。

答案：D

30. 下列说法不正确的是(　)。

A. 信息隐藏的主要分支包括:隐写术、数字水印、隐蔽信道和信息分存等。

B. 数字水印的主要应用包括:版权保护、盗版跟踪、保密通信和广播监控等。

C. 信息隐藏的主要思路是使秘密信息不可见，密码学的主要思路是使秘密信息不可懂。

D. 信息隐藏研究包括:正向研究和逆向研究，逆向研究的内容之一是信息隐藏分析。

答案：B

31.对于使用了 LSB 隐藏的灰度图，可用三种方法检测。

第一种，卡方分析。原理如下:LSB 隐写改变了原始图像的直方图统计特性，使得灰度值为 2i 和 2i+1 的像素出现频度趋于相等。

第二种，RS 分析。原理如下:对自然图像，非负和非正翻转同等程度地增加图像的混乱程度;而对于 LSB 隐写图像，使用非负翻转会导致经历两次翻转的像素的灰度值该变量为零，因此翻转后正常和异常图像块比例差值会随隐写率的增大而减小;而对 LSB 隐写图像使用非正翻转后，经历两次翻转的像素的灰度值该变量为 2，因此正常和异常图像块比例差值不会随隐写率的增大而减小。

第三种，GPC 分析。原理如下:定义两个与 XY 平面平行的且没有交集的平面簇，分别记图像穿过两个平面簇的次数为 N0 和 N1。对于自然图像，N0 近似等于 N1 ;对于 LSB 隐写图像，N1 随隐写率增大而增加。

现有一幅纹理丰富的待检测图像有可能经过了 LSB 隐写，则下面说法不正确的是（）。

A. 若秘密信息不是连续隐藏的,则卡方分析可能失效,而 RS 和 GPC 分析则不受该因素影响。

B. 图像纹理丰富时，自然图像的 N1 和 N0 很大，LSB 隐写引起的变化不明显，因此 GPC 分析可能失效。

C. 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。

D. 若隐写时使用的不是普通LSB算法,像素不是在值对2i和2i+1间翻转,2i可能变为2i-1，2i+1 可能变为 2i+2，那么 GPC 分析可能失效。

答案：C

32、使用书记板隐藏信息属于（）。

A. 技术性的隐写术

B. 语言学中的隐写术

C. 用于版权保护的隐写术

D. （A、B、C）都不是

答案：A

33、藏头诗属于（）。

A. 技术性的隐写术

B. 语言学中的隐写术

C. 用于版权保护的隐写术

D. （A、B、C）都不是

答案：B

34、在大约公元前 440 年，为了鼓动奴隶们起来反抗，Histiaus 给他最信任的奴隶剃头，并将消息刺在头上，等到头发长出来后，消息被遮盖，这样消息可以在各个部落中传递。用头发掩盖信息属于（）。

A. 技术性的隐写术

B. 语言学中的隐写术

C. 用于版权保护的隐写术

D. （A、B、C）都不是

答案：A

35、 在国际上正式提出信息隐形性研究是在（ ）年。

答案：B

36、 国际上第一届信息隐藏研讨会学术会议于（ ）年在剑桥大学举行。

答案：C

37、 在国际上正式提出信息隐形性研究是在 1992 年。国际上第一届信息隐藏研讨会学术会议于 1996 年在（ ）大学举行。

A. 哈佛　B.清华　C.北大　D.剑桥

答案：D

38. 由亮处走到暗处时，人眼一时无法辨识物体，这个视觉适应过程称为( )；由暗处走到亮处时的视觉适应过程则称为亮适应性；两者之间，耗时较长的是暗适应性。

A. 暗适应性　B.亮适应性　C.暗适应性

答案：A

39. 由亮处走到暗处时，人眼一时无法辨识物体，这个视觉适应过程称为暗适应性；由暗处走到亮处时的视觉适应过程则称为( )；两者之间，耗时较长的是暗适应性。

A. 暗适应性　B.亮适应性　C.暗适应性

答案：B

40. 由亮处走到暗处时，人眼一时无法辨识物体，这个视觉适应过程称为暗适应性；由暗处

走到亮处时的视觉适应过程则称为亮适应性；两者之间，耗时较长的是（ ）。

A. 暗适应性　　B. 亮适应性　　C. 暗适应性

答案：C

41. 下列描述不正确的是（ ）。

A. 限幅影响语音清晰度。

B. 峰值削波门限为幅值 2/3 时，语音清晰度受很大影响。

C. 中心削波门限为幅值 1/2 时，语音清晰度几乎全部丧失。

D. 语音信号大部分信息保存在幅值较低部分

答案：B

42. 有关基于格式的信息隐藏技术，下列描述不正确的是（ ）。

A. 隐藏内容可以存放到图像文件的任何位置。

B. 隐藏效果好，图像感观质量不会发生任何变化。

C. 文件的复制不会对隐藏的信息造成破坏，但文件存取工具在保存文档时可能会造成隐藏数据的丢失，因为工具可能会根据图像数据的实际大小重写文件结构和相关信息。

D. 隐藏的信息较容易被发现，为了确保隐藏内容的机密性，需要首先进行加密处理，然后再隐藏。

答案：A

43. 如果对调色板图像像素采用 LSB 方法进行处理以隐藏数据，下列描述不正确的是（ ）。

A. 索引值相邻的颜色对，其色彩或灰度可能相差很大，因此替换后图像感观质量可能会有明显下降。

B. 图像处理软件可能会根据颜色出现频率等重排颜色索引，因此隐藏的信息可能会丢失。

C. 方法的优点是可隐藏的数据量大，不受图像文件大小限制。

D. 为防止索引值相邻的颜色对色差过大，可以根据其色度或灰度预先进行排序，改变索引顺序，再对像素进行 LSB 替换。

答案： C

44. 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，误码率低于 5% 的概率为，误码率低于 10%的概率为，…。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( )。

% B. 5% C. 10% D. 50%

答案：C

45. 已知某图像轮廓的游程编码为<a0， 3><a1， 4><a2，4><a3，7>。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，…) ，则隐藏秘密信息 1100 后，游程编码变为( )。

A. <a0，3><a1 ，5><a2+1，2><a3 -1 ，8>

B. <a0，3><a1，5><a2 ，2><a3，8>

C. <a0 ，5><a1 +2，5><a2+2，4><a3+2，8>

D. <a0 ，5><a1 +2，3><a2+1，4><a3+1，8>

答案：C

46. 现接收到一使用 DCT 系数相对关系(隐藏 1 时，令 B(u1,v1)>B(u3,v3)+D，且， B (u2，v2) > B (u3，V3)+D)隐藏秘密信息的图像，已知 D=，对该图像作 DCT 变换后， 得到约定位置((u1，v1)u2,v2) (u3,v3))的系数值为(1. 6,，1. 0)，(0. 7，1. 2,,,,，则可从中提取的秘密信息是(　)。

，1，1　　B. 1，0，0　　C. 1，0，无效　　D. 0，1，无效

答案：C

47. 关于隐写分析，下列说法不正确的是(　)。

A. 设计图像隐写算法时往往假设图像中 LSB 位是完全随机的，实际使用载体的 LSB 平面的随机性并非理想，因此连续的空域隐藏很容易受到视觉检测。

B. 感观检测的一个弱点是自动化程度差。

C. 统计检测的原理:大量比对掩蔽载体和公开载体，找出隐写软件特征码

D. 通用分析方法的设计目标是不仅仅针对某一类隐写算法有效。

答案：　C

48. 卡方分析的原理是(　)。

A. 利用图像空间相关性进行隐写分析。

B. 非负和非正翻转对自然图像和隐写图像的干扰程度不同。

C. 图像隐写后，灰度值为 2i 和 2i 十 1 的像素出现频率趋于相等。

D. 图像隐写后，其穿越平面簇 z=0. 5，2. 5，4. 5，…的次数增加。

答案：C

49. 关于 RS 分析，下列说法不正确的是(　)。

A. 对自然图像，非负和非正翻转同等程度地增加图像的提乱程度。

B. 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。

C. 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。

D. RS 分析和 GPC 分析都是针对灰度值在 2i 和 2i+1 间，在 2i 和 2i-1 间翻转的不对称性进行的。

答案：C

50. 下列关于改进算法的描述，不正确的是(　　)。

A. 最小直方图失真隐写算法在尽量保持 F1 和 F-1 翻转平衡的情况下，使直方图在隐写前后变化量尽可能小，可以抵抗卡方分析。

B. 直方图补偿隐写算法确保隐写后，直方图中 2i 和 2i 十 1 的频度不再趋于相等，因此可以抵抗 RS 分析。

C. 改进 LSB 隐写算法翻转像素灰度时，2i 不仅可以变为 2i+1，也可以变为 2i-1。

D. 改进 LSB 隐写算法可以抵抗卡方、RS 和 GPC 分析。

答案：B

51、波形编码力图使重建的语音波形保持原语音信号的波形形状。其中，APC 指的是（）。

A. 脉冲编码调制

B. 自适应增量调制

C. 自适应预测编码

D. 自适应变换编码

答案：C

52、（）是对载体的某些统计特性进行明显的修改，表示嵌入信息“1”，若统计特性不变，则表示嵌入信息“0”；接收者在不知道原始载体的情况下，根据统计特性的改变，提取信息。

A. 文件格式隐藏法　B.扩展频谱技术　C.统计隐藏技术　D.变形技术

答案：C

53、在艺术作品中的隐写术属于（）。

A. 技术性的隐写术

B. 语言学中的隐写术

C. 用于版权保护的隐写术

D. （A、B、C）都不是

答案：　A

54、（）指的是将版权所有者的信息，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。

A. 用于版权保护的数字水印

B. 用于盗版跟踪的数字指纹

C. 用于拷贝保护的数字水印

D. （A、B、C）都不是

答案： A

55、判断载体中是否有秘密消息隐藏其中，可能会出现以下四种情况，其中（）属于纳伪错误。

A. 实际有隐藏，判断有隐藏

B. 实际无隐藏，判断无隐藏

C. 实际无隐藏，判断有隐藏

D. 实际有隐藏，判断无隐藏

答案： C

56、使用化学方法的隐写术属于（）。

A. 语言学中的隐写术

B. 用于版权保护的隐写术

C. 技术性的隐写术

D. （A、B、C）都不是

答案： C

57、（）指的是水印与作品的使用工具相结合（如软硬件播放器等），使得盗版的作品无法使用。

A. 用于拷贝保护的数字水印

B. 用于版权保护的数字水印

C. 用于盗版跟踪的数字指纹

D. （A、B、C）都不是

答案： A

58、（）是对载体的某些统计特性进行明显的修改，表示嵌入信息“1”，若统计特性不变，则表示嵌入信息“0”。而接收者在不知道原始载体的情况下，根据统计特性的改变，提取信息。

A. 统计隐藏技术

B. 文件格式隐藏法

C. 扩展频谱技术

D. 变形技术

答案： A

59、判断载体中是否有秘密消息隐藏其中，可能会出现以下四种情况，其中（）属于弃真错误。

A. 实际有隐藏，判断无隐藏

B. 实际有隐藏，判断有隐藏

C. 实际无隐藏，判断有隐藏

D. 实际无隐藏，判断无隐藏

答案： A

60、波形编码力图使重建的语音波形保持原语音信号的波形形状。其中，ADM 指的是（）。

A. 自适应预测编码

B. 自适应变换编码

C. 脉冲编码调制

D. 自适应增量调制

答案：D

（二）判断题

1、( )语音的质量一般从两个方面来衡量：语音的清晰度和自然度 。前者是衡量语音中的字、单词和句子的清晰程度；后者是衡量通过语音识别讲话人的难易程度。

答案：T

2、( )在国际上正式提出信息隐形性研究是在 1992 年。国际上第一届信息隐藏研讨会学术会议于 1996 年在哈佛大学举行。

答案：F

3、( )信息隐藏的研究分为三个层次，分别是应用基础研究、应用技术研究和基础理论研究。

答案：T

4、（ ）采用基于格式的信息隐藏方法，能够隐藏的秘密信息数与图像像素数目无关。

答案：T

5、（ ）主观评价方法依赖人对载体质量做出评价，其优点符合人的主观感受，可重复性强，缺点是受评价者疲劳程度、情绪等主观因素影响。

答案：F

6、（ ）人眼在一定距离上能区分开相邻两点的能力称为分辨力。当物体的运动速度大时，人眼分辨力会下降，且人眼对彩色的分辨力要比对黑白的分辨力高。

答案：F

7、（ ）动态软件水印的验证和提取必须依赖于软件的具体运行状态，与软件文件的内容或存储不相关。

答案：T

8、（ ）句法变换是一种文本语义隐藏方法。

答案：T

9、（ ）水印算法的透明度是指算法对载体的感官质量的影响程度，透明度高意味着人类感知系统难以察觉载体感官质量的变化。

答案：T

10、（ ）客观评价指标不一定与主观感受相符，对于峰值信噪比相同的图像，由于人眼关注区域不同，评价者给出的主观打分可能不同。

答案：T

11、（ ）图像的脆弱水印不允许对图像进行任何修改，任何修改都会导致图像中水印信息丢失。

答案：T

12、（ ）半脆弱水印技术主要用于内容篡改检测，因为对半脆弱水印图像进行普通信号处理。例如，JPEG 压缩、去噪等，不会影响水印的提取，但对图像内容的篡改将导致水印信息丢失。

答案：T

13、（ ）文本信息隐藏中的语义隐藏主要是通过调整文本格式来达到隐藏信息的目标。

答案：F

14、（ ）水印按照特性可以划分为鲁棒性水印和脆弱性水印，用于版权标识的水印属于脆弱性水印。

答案：F

15、（ ）增加冗余数是保持软件语义的软件水印篡改攻击方法之一。

答案： T

16、(　)图像的脆弱水印允许对图像进行普通信号处理操作，如滤波，但篡改内容的操作将导致水印信息丢失。

答案：F

17、(　)静态软件水印包括静态数据水印和静态代码水印。

答案：T

18、(　)与原始图像相比，采用 F5 算法隐写的图像，其 DCT 量化系数直方图更"瘦"、更"高" 0　(　)。

答案：T

19、(　)语音信号大部分信息保存在幅值较低部分，因此用峰值消波滤去高幅值信号对语音清晰度影响较小。

答案：T

20、(　)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。强信号称为掩蔽音，弱信号称为被掩蔽音。

答案：T

21、(　)人眼在一定距离上能区分开相邻两点的能力称为分辨力。人眼分辨力受物体运动速度影响，人眼对高速运动的物体的分辨力强于对低速运动的物体的分辨力。

答案：T

22、( )信息隐藏的核心思想是使秘密信息不可懂。

答案：F

23、( )很多隐写和数字水印算法原理相同，但算法性能指标优先顺序不同。相较而言，数字水印算法更重视透明性，隐写算法更重视鲁棒性。

答案：F

24、( )隐写分析可分为感官、特征、统计和通用分析。patchwork 算法调整图像两个区域亮度，使之有别于自然载体:即两区域亮度不相等，因此是一种感宫分析方法。

答案：F

25、( )隐写分析可分为感官、特征、统计和通用分析，RS 隐写分析是一种感官隐写分析算法。

答案：F

26、( )客观评价指标不一定符合主观感受。例如，经参数编码后重建的语音，由于波形发生较大变化，因此用客观评价指标信噪比评估的听觉效果可能很差，但实际听觉效果可能很好。

答案：T

27、( )水印按照特性可以划分为鲁棒性水印和脆弱性水印，用于版权标识的水印属于鲁棒性水印。

答案：T

28、（ ）模块并行化是保持软件语义的软件水印篡改攻击方法之一。

答案：T

29、（ ）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、文本中的信息隐藏等。

答案：T

30、（ ）数字指纹水印中需要嵌入购买者的个人信息。

答案：T

31、（ ）文本信息隐藏中的语义隐藏主要是通过调整文本格式来达到隐藏信息的目标。

答案：F

32（ ）等响曲线反映了人耳对不同频率声音的分辨能力不同。不同频率的单音，其声波幅度大小不同，但如果听起来同样响亮，那么它们在同一条等响曲线上。

答案：T

33、（ ）视频水印按照水印嵌入的策略分类，分为：在未压缩域中的嵌入水印、在视频编码器中嵌入水印、在视频码流中嵌入水印。

答案：T

34、(　)掩蔽音和被掩蔽音同时存在所产生的掩蔽效应称为同时掩蔽或时域掩蔽，否则称为异时掩蔽或频域掩蔽。

答案：F

35、(　)异时掩蔽(时域掩蔽)又分为超前掩蔽(pre-masking)和滞后掩蔽(post-masking)，超前掩蔽指掩蔽效应发生在掩蔽音开始之前，滞后掩蔽则指掩蔽效应发生在掩蔽音结束之后。产生时域掩蔽是因为大脑分析处理信号要花一些时间。

答案：　T

36、(　)MOS(MEan Opinion Score)又称为平均意见分，是应用最广泛的客观评价方法。 让试听者对语音的综合音质打分，总共划分为 3 个等级，平均所有人的打分得到的是平均意见分。

答案：F

37、(　)语音信号是平稳信号，即其参数是时不变的。语音信号同时具有短时平稳特性，在 100 ms 时间内，可以认为信号是平稳的。

答案：F

38、(　)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。

答案：F

39、（ ） 语音的数字模型是一个 缓慢时变 的线性系统，在 10－20ms 的时间内是近似不变的。

答案： T

40、（ ）常用语音处理算法有：傅立叶变换与短时傅立叶变换、小波变换、离散余弦变换。

答案： T

41、（ ）窗函数的形状和长度对语音信号分析无明显影响，常用 Rectangle Window 以减小截断信号的功率泄漏。

答案： F

42、（ ）数字水印应具有 安全性、可证明性 、不可感知性、稳健性的特点。

答案：T

43、（ ）数字水印方案包括三个要素：水印本身的结构、水印加载过程、 水印检测过程。

答案：T

44、（ ）脆弱性数字水印 就是在保证多媒体信息一定感知质量的前提下，将数字、序列号、文字、图像标志等做为数字水印嵌入到多媒体数据中，当多媒体内容受到怀疑时，可将该水印提取出来用于多媒体内容的真伪识别，并且指出篡改的位置，甚至攻击类型等。

答案：T

45、(　) 数字水印是永久镶嵌在其他数据(宿主数据)中具有可鉴别性的 数字信号或模式 ，并且不影响宿主数据的可用性。

答案：T

46、(　)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。

答案：F

47、(　) 水印嵌入位置的选择应该考虑两方面的问题：一个是安全性问题，一个是对载体质量的影响问题。

答案：T

48、(　)DCT 系数的特点： 直流　分量和　低频　系数值较大，代表了图像的大部分能量，对它们做修改会影响图像的视觉效果。

答案：T

49、(　) 二维离散小波变换处理图像，一级分解后的图像变为四个部分：近似部分、水平方向细节部分、垂直方向细节部分和对角线方向细节部分。

答案：T

50、(　) 信息隐藏的攻击者可以分为：被动攻击（监视和破译隐藏的秘密信息 ）和主动攻击（破坏隐藏的秘密信息；篡改秘密信息）。

答案：　T

51、（ ）根据噪声性质分类，信息影藏通信模型分为：加性噪声信道模型 、非加性噪声信道模型。

答案：T

52、（ ）参数编码的设计思想是使重建语音波形与原始语音信号波形基本一致，话音质量较好。

答案：F

53、（ ）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 1/30。

答案：F

(三)多选题

1、常用语音处理算法有：（ ）。

A.傅立叶变换与短时傅立叶变换

B.小波变换

C.离散余弦变换

答案：ABC

2、二维离散小波变换处理图像，一级分解后的图像变为( )等几部分。

A. 近似部分

B. 水平方向细节部分

C. 垂直方向细节部分

D. 对角线方向细节部分

答案：ABCD

3、信息隐藏技术发展到现在，可以大致分为三类（ ）。

A. 无密钥信息隐藏

B. 私钥信息隐藏

C. 公钥信息隐藏

D. 时域信息隐藏

答案：ABC

4、数字水印应具有（ ）的特点。

A. 安全性

B. 可证明性

C. 不可感知性

D. 稳健性

答案：ABCD

5、脆弱性数字水印就是在保证多媒体信息一定感知质量的前提下，将（ ）等做为数字水印嵌入到多媒体数据中，当多媒体内容受到怀疑时，可将该水印提取出来用于多媒体内容的真伪识别，并且指出篡改的位置，甚至攻击类型等。

A. 数字

B. 序列号

C. 文字

D. 图像标志

答案：ABCD

6、根据信息隐藏的载体分类，可以分为：（）等。

A. 语音中的信息隐藏

B. 图像中的信息隐藏

C. 视频中的信息隐藏

D. 文本中的信息隐藏

答案： ABCD

7、数字水印方案包括三个要素：（）。

A. 水印本身的结构

B. 水印的鲁棒性

C. 水印加载过程

D. 水印检测过程

答案：ACD

8、数字水印从其表现形式上可以分为几大类：（）。

A. 一类是一串有意义的字符

B. 一类是一串伪随机序列

C. 一类是一个可视的图片

答案： ABC

9、几何变换在数字水印的攻击中扮演了重要的角色，下列属于几何变换的有（）。

A. 水平翻转

B. 裁剪

C. 旋转

D. 缩放

E. 行、列删除

F. 打印-扫描处理

答案： ABCDEF

10、水印嵌入位置的选择应该考虑两方面的问题：（）。

A.一个是安全性问题

B.一个是鲁棒性问题

C.一个是可证明性问题

D.一个是对载体质量的影响问题

答案：AD

11. 视频水印按照水印嵌入的策略分类，分为：（ ）。

A. 在未压缩域中的嵌入水印

B. 在视频编码器中嵌入水印

C. 在视频码流中嵌入水印

答案：ABC

12、根据噪声性质分类，信息影藏通信模型分为：（）。

A. 加性噪声信道模型

B. 非加性噪声信道模型

C. 随机噪声信道模型

D. 隐蔽信道模型

答案： AB

13、对数字水印的攻击可分为（）。

A. 去除攻击

B. 表达攻击

C. 解释攻击

D. 法律攻击

答案： ABCD

14. 下列属于水印攻击软件的有（）。

A. Unzign

B. StirMark

C. CheckMark

D. OptiMark

答案：ABCD

15.数字水印技术的应用大体上可以分为（）等几个方面。

A. 版权保护

B. 数字指纹

C. 认证和完整性校验

D. 内容标识和隐藏标识

E. 使用控制

F. 内容保护

答案： ABCDEF

16. 信息隐藏的三个重要分支是（）。

A. 可视密码学

B. 隐写术

C. 数字水印

D. 隐蔽通信

答案： BCD

17. 异时掩蔽分为（）。

A. 时域掩蔽

B. 频域掩蔽

C. 超前掩蔽

D. 滞后掩蔽

答案： CD

18. 描述人对声波幅度大小的主观感受和描述人对声波频率大小的主观感受的术语是（）。

A. 响度

B. 音调

C. 听觉范围

D. 频率选择性

答案： AB

19. 信息隐藏的研究也分为三个层次，分别是（）。

A. 应用技术研究

B. 应用基础研究

C. 基础理论研究

答案： ABC

20. 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，一般采用的方法有（）。

A. 行移位编码

B. 字移位编码

C. 特征编码

答案：ABC

21. 按照嵌入位置分类，软件水印可分为（）。

A. 静态水印

B. 动态水印

C. 代码水印

D. 数据水印

答案： CD

22. 按照水印被加载的时刻，软件水印可分为（）。

A. 静态水印

B. 动态水印

C. 代码水印

D. 数据水印

答案： AB

23.一般采用（）作为隐写分析的评价指标。

A. 准确性

B. 适用性

C. 实用性

D. 复杂度

答案： ABCD

24、常用语音信号处理算法有：（）。

A. 傅里叶换与短时傅里叶变换

B. 小波变换

C. 离散余弦变换

答案：ABC

25、信息隐藏技术发展到现在，可以大致分为三类：（）。

A. 无密钥信息隐藏

B. 私钥信息隐藏

C. 公钥信息隐藏

答案：ABC

26. 在水印的每一种应用中，都存在（）三种操作。

A. 嵌入

B. 提取

C. 去除

D. 压缩

答案： ABC

27. 任何水印算法都需要在（）三者之间完成平衡。

A. 容量

B. 透明性

C. 鲁棒性

D. 随机性

答案： ABC

28.信息隐藏分析包括三个层次，分别是（）。

A. 发现

B. 提取

C. 破坏

答案：ABC

29 数字水印在数字作品版权保护方面的应用可以分为（）等几个方面。

A. 用于版权保护的数字水印

B. 用于盗版跟踪的数字指纹

C. 用于拷贝保护的数字水印

答案：ABC

30.衡量一个水印算法的稳健性，通常使用（）处理。

A. 数据压缩处理

B. 滤波、平滑处理

C. 量化与增强

D. 几何失真

答案： ABCD

31. 水印从外观上可分为两大类：（）。

A. 可见水印

B. 不可见水印

C. 图像水印

D. 视频水印

答案： AB

32. 根据水印加载方法的不同，可分为两大类：（）。

A. 空间域水印

B. 变换域水印

C. 静态水印

D. 动态水印

答案： AB

33. 根据识别篡改的能力，可以将脆弱性水印划分为以下四个层次：（）。

A. 完全脆弱性水印

B. 半脆弱水印

C. 图像可视内容鉴别

D. 自嵌入水印

答案： ABCD

34. 软件水印是（）等学科的交叉研究领域。

A. 密码学

B. 软件工程

C. 算法设计

D. 图论

E. 程序设计

答案： ABCDE

35. 根据采用的分析方法，信息隐藏分析可分为：()。

A. 感官分析

B. 统计分析

C. 特征分析

D. 已知隐文分析

答案： ABC

36. 隐写分析根据最终效果可分为：（ ）。

A. 特征分析

B. 已知载体攻击

C. 被动隐写分析

D. 主动隐写分析

答案：　CD

（四）　填空题

1. 掩蔽效应分为频域掩蔽和##，或##和异时掩蔽，后者又分为##和滞后掩蔽。

答案：时域掩蔽、同时掩蔽、超前掩蔽

2. 任何水印算法都需要在##、容量和鲁棒性三种性能参数之间完成平衡。

答案：透明度

3. 任何水印算法都需要在透明度、##和鲁棒性三种性能参数之间完成平衡。

答案：容量

4. 掩蔽效应分为频域掩蔽和##，或##和异时掩蔽，后者又分为超前掩蔽和##。

答案：时域掩蔽、同时掩蔽、滞后掩蔽

5. 任何水印算法都需要在透明度、容量和##三种性能参数之间完成平衡。

答案：鲁棒性

6. 根据水印被加载的时刻，软件水印可分为静态水印和##水印；按照嵌入位置分类，软件水印可分为##水印和数据水印。

答案：动态、代码

7. 在无符号 8 比特量化的音频样点序列 00010011、0011 0110、0101 0010 使用 LSB 嵌入 010，则样点序列变为##。

答案：00010010　00110111　01010010

8、 古代的隐蔽信息的方法可以分为两种基本方式：一种是将机密信息进行各种变化，使它们无法被非授权者所理解，另一种是以隐蔽机密信息的存在为目的。它们的发展可以看成两条线，从古典密码术，发展到##；从古典隐写术，发展到现在的##、信息隐藏和数字水印。

答案：现代密码学、伪装式信息安全

9、 在国际上正式提出信息隐形性研究是在##年。国际上第一届信息隐藏研讨会学术会议于1996 年在剑桥大学举行。中国于##年召开了第一次全国信息隐藏学术研讨会。

答案：1992、1999

10、 语音的数字模型是一个缓慢时变的线性系统，在 10－20ms 的时间内是##的。

答案：近似不变

11、 语音的质量一般从两个方面来衡量：语音的清晰度和##。前者是衡量语音中的字、单词和句子的清晰程度；后者是衡量通过语音识别讲话人的难易程度。

答案：自然度

12、 语音信号的编码方式可以分为两类：一类是波形编码，一类是##。

答案：参数编码

13、 根据噪声性质分类，信息隐藏通信模型分为：加性噪声信道模型和##噪声信道模型。

答案：非加性

14、替换技术就是试图用秘密信息比特替换掉## ，以达到隐藏秘密信息的目的。

答案：随机噪声

15、##就是在保证多媒体信息一定感知质量的前提下，将数字、序列号、文字、图像标志等做为数字水印嵌入到多媒体数据中，当多媒体内容受到怀疑时，可将该水印提取出来用于多媒体内容的真伪识别，并且指出篡改的位置，甚至攻击类型等。

答案：脆弱性数字水印

16、 数字水印是永久镶嵌在其他数据（宿主数据）中具有可鉴别性的数字信号或模式，并

且不影响宿主数据的##性。

答案：可用

17.让观察者根据一些事先规定的评价尺度或自己的经验，对测试对象感官质量作出判断，并给出质量分数，对所有观察者给出的分数进行加权平均。这种评价方法称为##。

答案：平均意见分

18、数字水印应具有 安全性 、可证明性、不可感知性、##的特点。

答案：健壮性

19、 数字水印从其表现形式上可以分为几大类：一类是一串有意义的字符，一类是一串伪随机序列，一类是一个##。

答案：可视的图片

20、 水印嵌入位置的选择应该考虑两方面的问题：一个是安全性问题，一个是 ##问题。

答案：对载体质量的影响

21、 DCT 系数的特点：直流分量和低频系数值较大，代表了图像的大部分能量，对它们做修改会影响图像的视觉效果；高频系数值很小，去掉它们基本不引起察觉。因此最好的水印嵌入区域就是在##频部分。

答案：中

22、 视频水印按照水印嵌入的策略分类，分为：在##中的嵌入水印、在视频编码器中嵌入水印、在视频码流中嵌入水印。

答案：在未压缩视频数据

23、 传统的图像质量评价方法可分为： ##和客观评价。

答案：主观评价

24、 传统的图像质量评价方法可分为：主观评价和##。

答案：客观评价

25、语音的数字模型是一个##的线性系统，在 10－20ms 的时间内是近似不变的。 **答案：缓慢时变**

26、语音的质量一般从两个方面来衡量：语音的##和自然度 。前者是衡量语音中的字、单词和句子的清晰程度；后者是衡量通过语音识别讲话人的难易程度。 **答案：清晰度**

27、语音信号的编码方式可以分为两类：一类是##，一类是参数编码。

答案：波形编码

28、替换技术就是试图用##替换掉随机噪声 ，以达到隐藏秘密信息的目的。

答案：秘密信息比特

29、 在多级安全水平的系统环境中，那些根本不是专门设计的也不打算用来传输消息的通信路径称为##。

答案：隐蔽信道

30、 数字水印是永久镶嵌在其他数据（宿主数据）中具有可鉴别性的数字信号或##，并且不影响宿主数据的可用性。

答案：模式

31、 信息隐藏的攻击者可以分为：##（监视和破译隐藏的秘密信息 ）和主动攻击（破坏隐藏的秘密信息；篡改秘密信息）。

答案：被动攻击

32. 信息隐藏的原理是利用载体中存在的##来隐藏秘密信息。

答案：冗余信息

33. 掩蔽效应分为##和时域掩蔽。

答案：频域掩蔽

34. 在无符号 8 比特量化的音频样点序列 0001 1011、0011 1110、0101 1010 使用 LSB 嵌入 001，则样点序列变为##，如果接收到上述样点序列，则可以提取的秘密信息为##。

答案：00011010　00111110　01011011、100

35. 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##，亮度变化小的区域称为##。前者又可进一步划分为##(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##(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)。

答案：高信息量区域、低信息量区域、关键区域、纹理区域

36、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、##。

答案：水印检测过程

（五）简答题

1.信息隐藏最重要一种特征不可感知性(透明性)表示的大致含义是什么

答:不可感知性包含两个方面的含义。

第一是指隐藏的秘密信息不对载体在视觉或者听觉上产生影响。隐藏的信息附加在某种数字载体上，必须保证它的存在不妨碍和破坏数字载体的欣赏价值和使用价值，即不能因在一幅图像中加入秘密信息而导致图像面目全非，也不能因在音频中加入秘密信息导致声音失真。

第二是要求采用统计方法不能恢复隐藏的信息，如对大量的用同样方法隐藏信息的信息产品采用统计方法也无法提取隐藏的秘密信息。

2.简述什么是回声隐藏算法。

答:回声信息隐藏是利用人类听觉系统的一个特性:音频信号在时域的向后屏蔽作用， 即弱信号在强信号消失之后变得无法听见。弱信号可以在强信号消失之后 50~200 ms 的作用而不被人耳觉察。音频信号和经过回声隐藏的秘密信息对于人耳朵来说，前者就像是从耳机中听到的声音，没有回声。而后者就像是从扬声器中听到的声音。

3. 简述什么是音频文件的相位信息隐藏算法。

答：相位编码是利用人类听觉系统对声音的绝对相位不敏感，但对相对相位敏感的特殊进行数字水印嵌入的。在相位编码中，载体信号首先分成若干个短序列，然后进行 DFT 变换，修改所有信号片段的绝对相位，同时保存它们的相对相位差不变，然后通过 IDFT 得到伪装信号;在恢复秘密信息之前，必须采用同步技术，找到信号的分段。已知序列长度，接收者就能计算 DFT，并能检测出相位 $\Phi_0 k$;该算法对载体信号的再取样有鲁棒性，但对大多数音频压缩算法敏感。由于仅在第一个信号片段进行编码，数据传输率很低。

4.简述无密钥信息隐藏系统。

答:如果一个信息隐藏系统不需要预先预定密钥，称为元密钥信息隐藏系统。在数学上，信息隐藏过程可以称为一个映射 E:CXM→C'，这里 C 表示所有可能载体的集合，M 表示所有可能秘密消息的集合，C'表示所有伪装对象的集合。信息提取也是一个映射过程， D:C'→M。发送方和接收方事先约定嵌入算法和提取算法，但这些算法都是要求保密的。

5.简述半脆弱和脆弱水印的主要区别。

答:脆弱水印对各种图像信号处理操作都敏感，载体数据发生改变时，水印信息就丢失了。有的场合要求只要图像内容没有发生变化，就应该依然能够检测水印。例如，使用 JPEG 压

缩图像后，图像内容没有发生变化，此时应该能够检测水印，因此产生了半脆弱水印算法。这种算法能够抵抗普通信号处理操作，如去噪、压缩等，但对内容篡改操作敏感。

6.简述密码学和信息隐藏的主要区别。

答:密码学的主要思路是使秘密信息"不可懂"，秘密信息加密后变成乱码，容易引起攻击者怀疑。密码学方法产生的签名及秘密信息分别存储在不同的数据结构中，物理上可以剥离，攻击者甚至不需要改写信息，只要删除签名，就能使接受者无法使用没有篡改的秘密信息。密码学方法加密的秘密信息，哪怕错 1 bit，其他信息都无法恢复。

信息隐藏的主要思路是使秘密信息"不可见"，携带秘密信息的隐蔽载体与普通载体相似，不引起攻击者怀疑。秘密信息是掩蔽载体的一部分，在保证掩蔽载体使用价值的情况下，难以去除秘密信息，部分区域的秘密信息不能正确提取不会影响其他区域的信息提取。

7.简述保持软件语义的篡改攻击。

答:保持软件语义的篡改攻击主要分为两大类：控制流程变换和数据变换。

控制流程变换又包括:插入支路、增加冗余操作数、模块并行化、简单流程图复杂化、环语句变换和内嵌技术。

数据变换又包括:数据编码、改变变量的存储方式和生存周期、拆分变量。

8.简述水印攻击算法中的马赛克攻击。

答:马赛克攻击的方法是将图像分解成为许多个小图像，每一块小到不能进行可靠的水印检测，拼接后的图像与原始图像在感知上相同。马赛克攻击的目标是使得水印检测器检测不到水印的存在，因为马赛克攻击不改变图像的质量，但是水印的检测失效了。

9.简单描述一种在 BMP 图像格式位图文件的两个有效数据结构之间隐藏信息的方法。

答:每种格式化的文件都有自己的文件结构，比如 BMP 图像就是由文件头、信息头、调色板区和数据区四个部分组成;BMP 图像可在 BMP 调色板和实际数据区之间隐藏秘密信息。

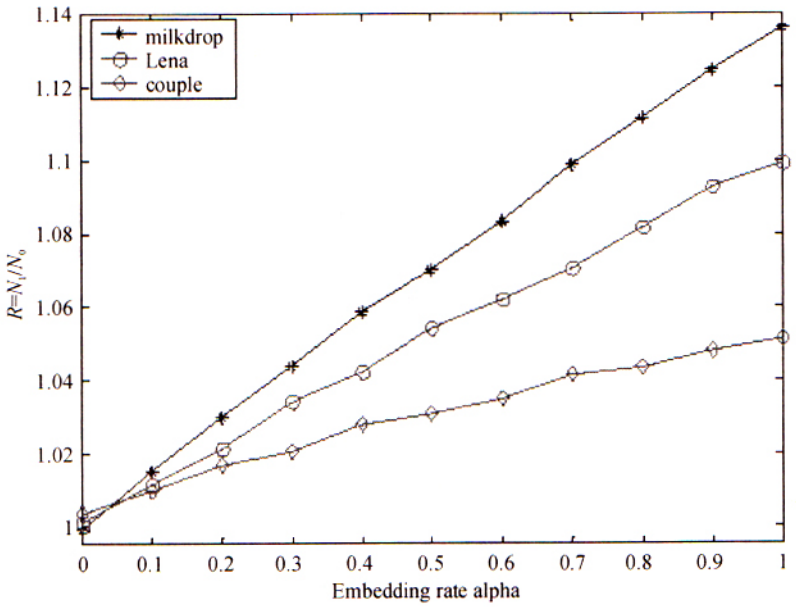
10.结构微调法是对文本的空间特征进行轻微调整来嵌入秘密信息的方法，一般采用的方法是行移位编码、字移位编码和特征编码三种方法，简述以上三种方法。

答:行移位编码就是在文本的每一页中，每间隔一行轮流地嵌入水印信息。但嵌入信息的行的相邻上下两行的位置不动，作为参考，需嵌入信息的行根据水印数据的比特流进行轻微的上移和下移。在移动过的一行中编码一个比特信息，如果这一行上移，则编码为 1，如果这一行下移，则编码为 0。

字移位编码是通过将文本某一行中的一个单词进行水平移位。通常在编码过程中，将某一个单词左移或者右移，而与其相邻的单词并不移动，这些不动的单词作为解码过程中的参考位置。

特征编码是通过改变文档中某个字母的某一特殊特征来嵌入标记。在这种编码中，水印信息作为可见的噪声叠加到字母笔画的边缘和文本中图像的边界上，对噪声图像进行二值编码，从而达到嵌入水印的目的。比较典型的方法是设计两种字体。

11. 下图是 GPC 分析方法数据图，横轴表示嵌入率，纵轴表示特定嵌入率下计算所得的 N_1 与 N_0 的比值，不同曲线是对光滑程度不同的图像作分析得到的结果(星形点折线由最光滑的图像分析而得，菱形点折线由纹理最复杂的图像分析而得)。分析从图像中可以得到两个结论。



答:第一，随着嵌入率的增加，N_1与 N_0的比值越来越大，因此越容易准确判断图像是否经过 LSB 类算法处理。第二，相同嵌入率情况下，图像越光滑，N_1与 N_0的比值越大，这是因为原始图像基数较小，所以比值对算法处理敏感，相对应地，嵌入秘密信息时，应尽可能选择纹理丰富的载体，以增加安全性。

12.在隐写分析中，要在原始载体、嵌入信息后的载体和可能的秘密信息之间进行比较。和密码学相类似，隐写分析学也有一些相应攻击类型根据已知消息的情况，参考密码分析的分类方法，对信息隐藏检测的分类，可以分为几类简单描述这几种类型。

答:

(1)仅知掩蔽载体攻击:分析者仅持有可能有隐藏信息的媒体对象,对可能使用的隐写算法和隐写内容等均全然不知，是完全的盲分析。

(2)已知载体攻击:将不含密的已知原始媒体与分析对象比较，检测其中是否存在差异。

(3)已知隐藏消息:分析者知道隐蔽的信息或者它的某种派生形式。

(4)可选隐藏对象:在已知对方所用隐写工具和掩蔽载体的基础上提取信息。

(5)可选消息:分析者可使用某种隐写工具嵌入选择的消息产生含密对象,以确定其中可能涉及某一隐写工具或算法的相应模式。

(6)已知隐藏算法、载体和伪装对象。

13.简述嵌入效率和载体数据利用率的含义，嵌入效率高意味着什么（从透明度和容量两方面分析。）

答:嵌入效率(嵌入比特数/平均修改长度)指平均每修改 1 个样点可以嵌入多少比特秘密信息,载体数据利用率(秘密信息总数/样点总数)指平均每个样点可以隐藏多少比特秘密信息。嵌入效率高意味着同样嵌入量，对图像的修改少，失真小。但与此同时，载体数据利用率下降，隐藏相同的秘密信息需要更多的像素。

14.简述信息隐藏算法的三个主要性能评价指标及其含义。

答:信息隐藏算法的主要性能评价指标是指:透明性、容量、鲁棒性、安全性和可检测性。其中:

透明性描述算法对载体感官质量造成的影响，算法应该不显著影响载体感官质量。

容量指在载体中能够嵌入的秘密信息总量，通常将之除以样本总数得到平均每样本嵌入量。

鲁棒性指算法抵抗普通信号处理操作的能力。

15. 简述卡方分析、RS 分析和 GPC 分析的原理。

答:

(1)卡方分析原理:LSB 隐写会使值对出现次数趋于相等，据此采用大数定理可以构造服从卡方分布统计量，计算待检测图像的该统计量可以判定图像是否经过 LSB 隐写。

(2) RS 分析原理:对自然图像，非负和非正翻转同等程度地增加图像的混乱程度。而对隐写

图像，采用非负翻转后，规则图像块比例和不规则图像块比例的差值随隐写率的增大而减小，采用非正翻转却不会出现上述情况。

(3) GPC 分析原理:GPC 分析也利用图像空间相关性进行隐写分析。对于自然图像，N_0（图像的三维曲面穿越平面簇 z=,,...,的次数)近似等于 N_1(图像的三维曲面穿越平面簇 z=,,...,的次数）;而对于隐写图像，N_1与 N_0的比值随隐写率增大而增加。

16.根据攻击者掌握信息的不同，隐写分析可分为哪五类，请简单介绍。

答:

(1)仅知掩蔽载体攻击:分析者仅持有可能有隐藏信息的媒体对象，对可能使用的隐写

算法和隐写内容等均全然不知，是完全的盲分析。

(2)已知载体攻击:将不含密的已知原始媒体与分析对象比较，检测其中是否存在差异。

(3)已知隐藏消息:分析者知道隐蔽的信息或者它的某种派生形式。

(4)可选隐藏对象:在已知对方所用隐写工具和掩蔽载体的基础上提取信息。

(5)可选消息:分析者可使用某种隐写工具嵌入选择的消息产生含密对象，以确定其中可能涉及某一隐写工具或算法的相应模式。

17.根据嵌入码流类型的不同可将视频水印方案分为三类，请简要介绍这三种类型的

水印方案。

答:

根据嵌入码流类型的不同可将视频水印方案分为三类，分别是基于原始视频的水印方案、基于视频编码的水印方案和基于压缩视频的水印方案。

基于原始视频的水印方案是将水印信息直接嵌入到原始的图像码流中，形成含有水印的原始视频信息，然后进行视频编码。这种方案可以充分利用静止图像的水印技术，结合视频帧的结构特点，形成适用于视频水印的方案。

基于视频编码的水印方案是在编码时嵌入水印。当前视频的基本编码思想是运动补偿预测和基于块的编码。在编码压缩时嵌入水印，可以直接与视频编码器相结合。 水印的嵌入和提取过程是在视频编解码器中进行。

基于压缩域的水印信息是将水印信息直接嵌入到编码压缩后的比特流中，这种方案适用于不能直接介入视频编码过程、只能得到编码视频流的场合。

18.隐写术与数字水印的区别。

答:

隐写术与数字水印存在密切联系，特别是不可见水印和隐写术更难彼此区分。但是，隐写术和数字水印确实各有特点。首先是它们的目标不同，隐写术的主要目标是使得对手不能确认信息隐藏是否存在，而水印的主要目标是保护数字产品的知识产权。其次是评价标准不同，隐写术最重要的评价标准是透明性，数字水印最重要的评价标准是鲁棒性。

19.隐写分析的目标是什么

答:隐写分析技术是对表面正常的图像、音频等载体进行检测，以判断载体中是否隐藏有秘密信息，甚至只是指出媒体中存在秘密信息的可能性。另外，隐写分析还可以对看似可疑的载体实施主动攻击，即删除或者破坏嵌入的秘密信息以达到阻止隐蔽通信的目的。

20.简述什么是针对水印鲁棒性的几何攻击。

答:水印信息的几何攻击包括:时间上和空间上的延迟（平移）、缩放和剪切。图像水印还包括:仿射变换。载体遭受几何攻击后，会失去水印的同步。

21.信息隐藏评价的指标有三个，分别是不可感知性、鲁棒性和容量，但是这三个性能指标之间相互制约，请简单介绍这三种性能指标，并简要描述这三种性能指标之间的关系。

答:信息隐藏的不可感知性、鲁棒性和容量是信息隐藏系统评价的三个主要特征，三者相互影响制约。

不可感知性是指隐藏后的载体和隐藏前的载体之间感知相似度。

信息隐藏的容量是指在单位时间或者在某一个作品中，隐藏的信息的数量。

信息隐藏的鲁棒性是指隐藏信息的载体经过某些信号处理或者信道攻击后,隐藏的信息依然存在。

水印嵌入强度是提高鲁棒性的重要因素，即嵌入水印能量越大，鲁棒性越强，而水印的不可感知性将随之降低，不可感知性、鲁棒性和容量三者之间的矛盾是由信息隐藏系统的基本设计思路来决定的，不同的信息隐藏系统会在鲁棒性、不可感性和容量之间寻求一个平衡点。

22.隐写分析中的正确性一般采用虚警率和漏检率来表示，请简单描述什么是虚警率和漏检率。

答:虚警率是把非隐藏信息误判为隐藏信息的概率。漏检率是把隐藏信息错误判为非隐藏信息的概率。

23.信息隐藏的研究也分为三个层次，分别是基础理论研究、应用基础研究和应用技术研究，简述每个研究层次的研究内容。

答:基础理论研究主要针对感知理论、信息隐藏及其数字水印模型、理论框架和安全性理论等;应用基础研究的主要针对图像、声音、水印等载体，研究相应的数字水印隐藏算法和检测算法;应用技术研究以实用化为主要目的，研究各种多媒体格式的信息隐藏和数字水印技

术在实际中的应用。

24、密码学的目标是让秘密信息看不懂，信息隐藏的目标是秘密信息看不见。简述密码学和信息隐藏的主要区别。

答：

密码学:乱码、签名和消息分离、雪崩效应。

信息隐藏:自然载体、不易隔离、影响范围小。

25、什么是被动隐写分析什么是主动隐写分析它们各有什么特点

答：

被动隐写分析:判断是否隐写及隐写使用的算法。特点:判断。

主动隐写分析:判断是否隐写，估计隐藏秘密信息的位置与数量，推算出所使用的密钥，并提取出秘密信息。特点:通过分析判断并提取信息。