信息对抗技术练习

Chap 1 概论

1.信息隐藏算法三个性能指标（透明性、鲁棒性、隐藏容量）之间相互制约，不存在能让这三个性能指标同时达到最优的算法。（T）

2.____指在单位时间或一幅作品中能嵌入水印的比特数。

A 透明性

B 鲁棒性

C 隐藏容量

3.____也称稳健性，是指隐藏的秘密信息抵抗各种信号处理和攻击的能力，这类水印通常不会因常见的信号处理和攻击而丢失隐藏的水印信息。

A 透明性

B 鲁棒性

C 隐藏容量

4.__是指嵌入的秘密信息导致隐写载体信号质量变化的程度。即在被保护信息中嵌入数字水印后应不引起原宿主媒体质量的显著下降和视听觉效果的明显变化，不能影响隐写载体的正常使用。

A 透明性

B 鲁棒性

C 隐藏容量

5._____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。

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 用于复制保护的数字水印

6.___同一个产品被多个用户买去，在每一个用户买到的复件中，都预先被嵌入了包含购买者的信息，这对跟踪和监控产品在市场上的非法复制是非常有用的。

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 用于复制保护的数字水印

7.数字作品极易无失真地复制和传播，容易修改，容易发表。这些特点对数字作品的版权保护提出了技术上和法律上的难题，包括:

A 如何鉴别一个数字作品的作者。

B 如何确定数字作品作者的版权声明。

C 如何公证一个数字作品的签名与版权声明。

D 在采用登记制的情况下，怎样确认登记的有效性。

8.《世界知识产权组织版权公约》已规定了计算机软件作为文字作品予以保护，数据库作为文字汇编作品予以保护。（T）

9.数字作品符合著作权法对作品的定义，应该受到版权保护。（T）

10.知识产权主要包括_____。

A 版权

B 专利权

C 商标权

11.关于叠像术，以下论述正确的有：____。

A 产生的每一张图像不再是随机噪声图像，而是正常人能看懂的图像：图像上有不同的文字或图画。

B 只要将一定数量的图像叠加在一起，则原来每一张图像上的内容都将消失，而被隐藏的秘密内容出现。

C 单个图像无论是失窃还是被泄露，都不会给信息的安全带来灾难性的破坏。

D 由于每一张图像的“可读性”，使其达到了更好的伪装效果。

12.可视密码学的思想是：把要隐藏的密钥信息通过算法隐藏到两个或多个子密钥图片中，每一张图片上都有随机分布的黑点和白点，把所有的图片叠加在一起，则能恢复出原有的信息。（T）

13.可视密码学的主要特点是：恢复秘密图像时不需要任何复杂的计算，直接以人的视觉系统就可以将秘密图像辨识出来 。（T）

14.信息隐藏研究分支有：____。

A 隐写术

B 数字水印

C 信息分存

D 隐蔽信道

E 数字图像取证

15.__年国际上正式提出信息隐形研究。

A 1992

B 1996

C 1999

D 2002

16.____无法利用冗余度来隐藏信息，因此在这些没有冗余度或者冗余度很小的载体中隐藏信息，就需要采用其他方法。

A 网络协议

B 图像

C 文本

D 视频

E 音频

17.《全国信息隐藏暨多媒体信息安全学术大会》（CIHW）开始于___年。

A 1992

B 1996

C 1999

D 2002

18.卡登格子法属于___。

A 技术性的隐写术

B 语言学中的隐写术

C 保护版权的隐写术

19.制作特殊的雕塑或绘画作品，使得从不同角度看会显出不同的印像。在一些变形夸张的绘画作品中，从正面看是一种景象，侧面看又是另一种景象，这其中就可以隐含作者的一些政治主张或异教思想。这类方法 属于_____。

A 技术性的隐写术

B 语言学中的隐写术

C 保护版权的隐写术

20.使用隐写墨水和显影剂的方法属于__。

A 技术性的隐写术

B 语言学中的隐写术

C 保护版权的隐写术

21.被人们誉为历史学之父的古希腊历史学家希罗多德(Herodotus, 486—425)，在其著作中讲述了这样一则故事：公元前480年，一个名叫希斯提乌斯（Histaieus）的人筹划着与他的朋友合伙发起叛乱，里应外合，以便推翻波斯人的统治。他找来一位忠诚的奴隶，剃光其头发并把消息刺在头皮上，等到头发又长起来了，把这人派出去送"信"，最后叛乱成功了。这种方法属于____。

A 技术性的隐写术

B 语言学中的隐写术

C 保护版权的隐写术

22.信息隐藏的载体可以是：__。

A 网络协议

B 图像

C 文本

D 视频

E 音频

23.数字信号处理和网络传输技术可以对数字媒体的原版进行无限制的任意_____。

A 编辑

B 修改

C 拷贝

D 散布

24.隐写分析(Steganalysis)是__隐写对象中秘密信息的技术。

A 检测

B 提取

C 破坏

25.信息隐藏的携密载体是“普通”数字媒体，秘密信息___。

A 不可懂

B 不可见

Chap 2 基础知识

1.常用图像处理方法有（ ）。

A 二维离散傅里叶变换DFT

B 二维离散余弦变换DCT

C 二维离散小波变换DWT

2.主观评价是比较准确的评价图像质量的方法，但是它往往受到观察者本身的( )等因素的影响。

A 知识背景

B 情绪

C 疲劳程度

3.人眼对彩色的分辨力要比对黑白的分辨力高。（F）

4.对语音信号做小波分解，每分解一次，都得到一个近似分量和一个细节分量。（T）

5.常见的波形编码：主要有 （ ）。

A 脉冲编码调制（PCM）

B 自适应增量调制（ADM）

C 自适应差分编码（ADPCM）

D 自适应预测编码（APC）

E 自适应子带编码（ASBC）

F 自适应变换编码（ATC）

6.参数编码的优点是编码速率低，它可以达到2.4kbit/s甚至更低，能够达到听懂话音，但是它的主要问题是语音的自然度较低。（T）

7.语音信号的编码方式可以分为两大类，一类是波形编码，一类是参数编码。（T）

8.一般认为MOS分为（ ）称为通信质量，能感觉到语音质量有所下降，但不妨碍正常通话。

A 4.0~4.5分

B 3.5分左右

C 2.5~3.0分

D 2.0分以下

9.基于输出的评价方法是根据原始语音和经过处理后的语音信号之间的误差大小来判别语音质量的好坏，是一种误差度量。（F）

10.语音质量评价是一个极其复杂的问题，语音质量评价一般可以分为两大类：主观评价和客观评价。（T）

11.目前使用较多的主观评价方法包括：（ ）。

A 平均意见分（Mean Opinion Scorer，MOS）

B 音韵字可懂度测量（DRT）

C 满意度测量（DAM）

12.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。（ ）是衡量语音中的字、单词和句子的清晰程度。

A 自然度

B 清晰度

13.研究结果表明，对于低通滤波而言，

去掉( )Hz以上的频率成分清晰度不受影响；

滤掉( )Hz以上的成分清晰度约下降一半，

而当滤掉( )Hz以上的成分时，清晰度降为零。

A 1.5k 5k 200k

B 5k 1.5k 200（有k吗）

C 200 1.5k 5k

D 1.5k 5k 200

14.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

15.掩蔽效应分为( )和时域掩蔽。

A 同时掩蔽

B 滞后掩蔽

C 频域掩蔽

D 超前掩蔽

16.掩蔽音和被掩蔽音同时出现所产生的掩蔽效应称为同时掩蔽或频域掩蔽。（T）

17.对于鼻音和摩擦音，（ ）不能很好地符合语音的特点。

A 全极点模型

B 零极点模型

18.声道模型中，声管是一个变截面积的声管，而声道的频率特性主要取决于声道截面的最小值出现的位置。(T)

19.语音的产生和语音的感知方面的研究与（ ）密不可分。

A 语音学

B 语言学

C 认知学

D 心理学

E 神经生理学

20.人类对于语音的研究包括两个方面:一方面是从语音的产生和语音的感知来研究,另一方面是从信号处理的角度来研究。（T）

Chap 3 信息隐藏的通信模型

1.实现信息隐藏的基本要求有哪些?

A 载体对象是正常的，不会引起怀疑

B 伪装对象与载体对象无法区分，无论从感观上，还是从计算机的分析上

C 不可视通信的安全性取决于第三方有没有能力将载体对象和伪装对象区别开来

D 对伪装对象的正常处理，不应破坏隐藏的信息

2.设C是一个非空集合，一个函数 sim：$C^2 \rightarrow (-\infty, 1)$，对x，y∈C，若满足：

$$sim(x,y)\begin{cases} =1 & x=y \\ <1 & x\neq y \end{cases}$$

则sim称为C上的相似性函数。（T）

3.隐藏模型根据载体对信息提取时的贡献可分为以下两类：

第一类模型将载体图像与信号处理、攻击同等对待。

第二类模型把载体图像视为信道边信息。

（T）

4.与通信系统不同的还有，隐藏系统能够知道更多关于信道的信息，因为在信息隐藏端完全知道载体信号，充分利用这些已知信息可以提高隐藏和提取的性能。（T）

5.通信系统和信息隐藏系统：可以将信息隐藏的载体看作通信信道，将待隐藏信息看作需要传递的信号，而信息的嵌入和提取分别看作通信中的调制和解调过程。（T）

6.一个系统抵御载体修改的鲁棒性越强，则系统的安全性就越低。（T）

7.信息隐藏的安全性和鲁棒性之间存在一个平衡。一个安全性很高的系统，其鲁棒性较差，安全性高，说明隐藏了信息后的伪装对象与载体对象从概率分布上无法区别，因此信息的隐藏必须利用载体的随机噪声，而随机噪声是载体的冗余信息，通过普通的有损压缩，或者攻击者在伪装对象中加入随机噪声，就可以抹去隐藏信息。因此其鲁棒性是比较差的。（T）

8.除了主动攻击者对伪装对象的破坏以外，伪装对象在传递过程中也可能遭到某些非恶意的修改，如：（）。

A 图像传输时，为了适应信道的带宽，需要对图像进行压缩编码。

B 图像处理技术(如平滑、滤波、图像变换等)

C 数字声音的滤波

D 多媒体信号的格式转换

9.与密码学一样，信息隐藏系统也存在攻击者，他们可以分为被动攻击者和主动攻击者。（）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。

A 主动攻击者

B 被动攻击者

10.与密码学一样，信息隐藏系统也存在攻击者，他们可以分为被动攻击者和主动攻击者。

（ ）是要截获传递的伪装对象，修改后再发给接收方。

A 主动攻击者

B 被动攻击者

11.当载体在W监视的信道上经过时，w对它们进行归类，判断是否有秘密消息隐藏其中。这时有以下几种情况，分别是：（ ）

A 准确判断隐藏有秘密信息

B 准确判断没有隐藏信息

C 从不含有秘密信息的载体中错误地检测出隐藏信息

D 在含有秘密信息的载体中错误地认为没有信息隐藏

12.在含有秘密信息的载体中错误地认为没有信息隐藏，称为（ ）。

A 纳伪错误

B 弃真错误

13.从不含有秘密信息的载体中错误地检测出隐藏信息，称为（ ）。

A 纳伪错误

B 弃真错误

14.攻破一个信息隐藏系统可分为三个层次: 证明隐藏信息的存在、提取隐藏信息和破坏隐藏的信息。（T）

15.对一个六元组Σ=〈C，M，K，C′，DK，EK〉，其中C是所有可能载体的集合，M是所有可能秘密消息的集合，K是所有可能密钥的集合，EK：C×M×K→C′是嵌入函数，DK：C′×K→M是提取函数，若满足性质：对所有m∈M，c∈C和k∈K，恒有：DK (EK (c，m，k)，k)=m，则称该六元组为（ ）系统。

A 无密钥信息隐藏

B 私钥信息隐藏

C 公钥信息隐藏

16.隐藏信息时，应该选择一个合适的载体，使得载体对象与伪装对象之间的相似性函数达到最大值。（T）

17.对一个五元组∑=〈C,M,C',D,E〉，其中

C是所有可能载体的集合，

M是所有可能秘密消息的集合，

C'是所有可能伪装对象的集合。

E：C X M→C'是嵌入函数，

D:C'→M是提取函数，

若满足性质对所有m∈M和c∈C,恒有D(E(c,m))=m，则称该五元组为无密钥信息伪装系统。（T）

18.如果一个信息隐藏系统不需要预先约定密钥，称其为无密钥信息隐藏系统。（T）

19.把需要秘密传递的信息m隐藏到载体对象c中，此时，载体对象c就变为伪装对象c'。（T）

20.A打算秘密传递一些信息给B，A需要从一个随机消息源中随机选取一个无关紧要的消息c，当这个消息公开传递时，不会引起怀疑，称这个消息c为（）。

A 伪装对象

B 载体对象

C 伪装密钥

Chap 4 音频信息隐藏

1.改变（），都不会引起听觉差异，因此可在这几种声音消息中嵌入水印。

A 声音开启的最低比特位

B 乐器编号的最低位比特

C 通道触动压力的低4比特位

2.一个标准MIDI文件基本上是由两部分组成：头块和音轨块。头块包含一系列由MIDI消息构成的MIDI数据流。原则上，可为某种声音、某种乐谱或某种乐器等分配一个音轨块。（F）

3.MIDI全称是musical instrument digital interface，即乐器数字接口，也是一种专用于乐器的接口标准。（T）

4.目前，已经有一些专家学者对mp3信息隐藏进行了研究，提出了一些隐藏算法。根据这些算法的嵌入时间的特点对其分为三类：压缩编码前嵌入、压缩编码中嵌入、压缩编码后嵌入。（T）

5.MP3编码算法流程大致可以分为哪几部分?

A 时频映射

B 心理声学模型

C 量化编码

D 帧数据流格式化

6.回声隐藏算法的最大难点在于秘密信号的提取，其关键在于回声间距的确定。（T）

7.回声隐藏巧妙地利用人类听觉系统(HAS)的频域掩蔽特性，通过向音频信号中引入回声来完成隐藏秘密信息的一种技术方法。（F）

8.音频信号和经过回声隐藏的携密数据对于人耳来说，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里听到的声音，有所处空间诸如墙壁、家具等物体产生的回声。（T）

9.回声和原声间的延迟在一定范围内人耳都难以察觉，亦即可以人为添加不同延迟的回声。（T）

10.强信号的存在会使其附近的弱信号难以被感知。（T）

11.在数字声音信号中引入回声，可根据引入回声的位置不同来隐藏秘密信息。（T）

12.LSB算法性能有（ ）。

A 透明度高

B 容量大

C 鲁棒性差

13.LSB算法参数包括( )。

A 比特位置的选取

B 样点位置的选取

14.幅值为6(110B)的样点，哪怕（噪声干扰）幅度仅变化1，则可能会影响不止一个比特位发生变化。（T）

15.数字化音频中，低有效比特对音质贡献弱。改变低有效比特不会显著影响音质。（T）

16.对音频信息隐藏技术的要求有（ ）。

A 透明性

B 鲁棒性

C 同步要求

D 盲检测

17.人眼视觉系统（HVS）比人耳听觉系统（HAS）灵敏得多。（F）

18.音频信号是二维信号。（F）

19.任何数字多媒体信息，在扫描和采样时，都会产生物理随机噪声，而人的感观系统对这些随机噪声是不敏感的。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。（T）

20.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等。（T）

Chap 5 图像信息隐藏

1.格式化文本中的信息隐藏，这一类隐藏属于变形技术，主要是利用文本的排列或者文档的布局来隐藏信息。例如，可以调节行间距、宇间距，以及在文本中加入适当的空格等等 。（T）

2.变形技术是对载体进行某种修改，其修改方式与需要嵌入的秘密信息比特相关联，通过比较修改后的载体与原始载体的差别来提取隐藏信息。而对载体的修改应该是不易察觉的。（T）

3.所谓的统计隐藏技术，就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"。而接收者应能够在不知道原始载体的情况下，区分出哪些进行了修改，哪些没有修改。（T）

4.使用文件格式来进行信息伪装，可以在一个文件中隐藏任意多的数据。 文件的拷贝并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。（T）

5.如果将秘密数据放在文件头与图像数据之间，则至少需要修改文件头中文件长度、数据起始偏移地址这两个域的值。（T）

6.图像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。图像的主要能量集中在低频部分。为了分析方便，还可以对图像的近似部分再进行下一级小波分解。（T）

7.提取秘密信息时，（）需要原始图像。

A 修改系数的方法

B 系数比较的方法

8.在中频系数中,以一定的方式挑选一些隐藏位置。可以选择所有中频系数,也可以选择固定位置的中频系数,还可以随机挑选中频系数，或者根据中频系数的大小排序,选择最大的几个系数。（T）

9.为了将隐藏的信息与载体图像的视觉重要部分绑定，一般都将隐藏信息嵌入在载体的（）部分，达到既不引起视觉变化，又不会被轻易破坏的目的。

A 高频

B 中频

C 低频

D 直流

10.低频部分代表图像中的噪声部分，这些部分容易通过有损压缩或者滤波等处理被去掉。（F）

11.DCT变换首先需要把图像分为8×8的像素块，然后进行二维DCT变换，得到8×8的DCT系数，最左上角的那个系数为（），其余为（）。DCT系数中，左上角部分为（）和（），右下角部分为（），中间区域为（）。

A 交流系数、直流系数、直流、低频系数、中频系数、高频系数

B 交流系数、直流系数、交流、低频系数、高频系数、中频系数

C 直流系数、交流系数、直流、低频系数、中频系数、高频系数

D 直流系数、交流系数、直流、低频系数、高频系数、中频系数

12.变换域技术就是在载体的显著区域隐藏信息，它比LSB方法能够更好地抵抗攻击，而且还保持了对人类感官的不可察觉性。目前主要使用的变换域方法有：（）。

A 离散余弦变换（DCT）

B 离散小波变换（DWT）

C 离散傅里叶变换（DFT）

13.基于调色板的信息隐藏，其鲁棒性都较差，攻击者只要对调色板重新排序或者对图像的格式进行变换，就很有可能破坏秘密信息。（T）

14.因为在图像的存储中，调色板不需以任何方式排序，所以在以调色板保存颜色时，可以选择对信息进行编码。（T）

15.基于调色板的图像由两部分组成：一部分是调色板数据，它定义了N种颜色索引对（i,c_i)列表，它为每一个颜色向量c_i指配一个索引 i ;另一部分是实际图像数据，它保存每一个像素的调色板索引，而不是保存实际的颜色值。（T）

16.利用奇偶校验位的方法，把载体划分成几个不相重叠的区域，在一个载体区域中存储一比特信息。选择 L(m)个不相重叠区域，计算出每一区域I的所有最低比特的奇偶校验位(即“1”的个数奇偶性）, bi(i=1,2, … ,n)。

$$b_i = \sum_{j \in I} LSB(c_j) \bmod 2$$

嵌入信息时，在对应区域的奇偶校验位上嵌入信息比特mi，如果奇偶校验位bi与mi不匹配，则将该区域中所有元素的最低比特位进行翻转，使得奇偶校验位与mi相同，即bi=mi 。（T）

17.为了提高LSB方法的安全性，可以采取一些有效的措施：（ ）。

A 对秘密信息先加密后再隐藏。

B 在隐藏信息时，可以多次重复嵌入

C 引入纠错编码技术，在秘密信息嵌入之前先进行纠错编码，再进行隐藏，这样，即使出现少量的干扰，也可以正确恢复出秘密信息。

18.图像在扫描和采样时,都会产生物理随机噪声,而人的视觉系统对这些随机噪声是不敏感的。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。（T）

19.（ ）是信息隐藏领域研究时间最长、研究成果最多的载体类型之一。

A 图像

B 音频

C 视频

D 文本

20.信息隐藏的载体可以是（ ）。

A 图像

B 音频

C 视频

D 文本

Chap 6 数字水印与版权保护

1.客观评价方法的缺陷是:客观指标难以准确反映主观感受。（T）

2.（ ）水印又称为基于数据目的的水印，主要包含数字作品的版权信息、购买者的个人信息，可以用于防止数字产品的非法拷贝和非法传播。

A 版权标识

B 数字指纹

3.（ ）主要用于完整性保护，与稳健性水印的要求相反，脆弱性水印必须对信号的改动很敏感，人们根据脆弱水印的状态就可以判断数据是否被篡改过。它的特点是：载体数据经过很微小的处理后，水印就会被改变或毁掉。脆弱性水印通常是用在证明图像的真实性、检测或确定图像内容的改动等方面。例如，如果图像中的水印被发现受到了破坏，则可证明图像遭到了篡改。

A 健壮性数字水印

B 脆弱性数字水印

4.在检测水印时，如果需要参考未加水印的原始载体(图像、声音等)，则这类水印方案被Cox等人称为私有水印方案，或者称为（ ）。

A 非盲水印方案

B 盲水印方案

5.与空间域水印方法比较，变换域水印方法具有如下优点：（ ）。

A 在变换域中嵌入的水印信号能量可以散布到空闻域的所有位置上，有利于保证水印的不可察觉性。

B 在变换域、人类视觉系统和听觉系统的某些特性(如频率掩蔽效应)可以更方便地结合到水印编码过程中。

C 变换域的方法可与数据压缩标准相兼容，从而实现在压缩域内的水印算法，同时，也能抵抗相应的有损压缩。

6.基于变换域的技术可以嵌入水印数据而不会引起感观上的察觉，这类技术一般基于常用的变换，如DCT变换、小波变换、傅里叶变换，Fourier-Meilin变换或其他变换。（T）

7.文档水印利用文档所独有的特点，水印信息通过轻微调整文档中的行间距、字间距、文字特性(如字体)等结构来完成编码。（T）

8.（ ）依赖于软件的运行状态，通常是在一类特殊的输人下才会产生，水印的验证也是在特定的时机下才能完成。

A 静态水印

B 动态水印

9.（ ）不依赖于软件的运行状态，可以在软件编制时或编制完成后被直接加入。

A 静态水印

B 动态水印

10.根据水印的生成时机和存放的位置，软件水印可以分为静态水印和动态水印两类。（T）

11.软件水印是近年来提出并开始研究的一种水印，它是镶嵌在软件中的一些模块或数据，通过这些模块或数据，可以证明该软件的版权所有者和合法使用者等信息。（T）

12.加载数字水印的数字产品，可以是任何一种多媒体类型。根据载体类型的不同，可以把数字水印分为:（）。

A 图像水印

B 视频水印

C 音频水印

D 软件水印

E 文档水印

13.对于假设检验的理论框架,可能的错误有如下两类。

第一类错误:实际不存在水印但却检测到水印,该类错误用（）(误识率)P_{fa}衡量。

第二类错误:实际有水印但是却没有检测出水印,用（）P_{rej}表示。

总错误率为$P_{err}=P_{fa}+P_{rej}$。

A 虚警率 漏检率

B 漏检率 虚警率

14.数字水印本身可分为两种：一种包含了版权所有者、合法使用者、日期等具体信息；另一种采用伪随机序列作为水印，检测时只需判断水印是否存在。（T）

15.（）是指数字水印应能为宿主数据的产品归属问题提供完全和可靠的证据。

A 安全性

B 可证明性

C 不可感知性

D 稳健性

16.数字水印应该难以被擦除，指的是（）。

A 安全性

B 可证明性

C 不可感知性

D 稳健性

17.不同的应用对数字水印的要求是不尽相同的，一般认为数字水印应具有如下特点（ ）。

A 安全性

B 可证明性

C 不可感知性

D 稳健性

18.数字水印不需要精确地恢复隐藏的数字水印，数字水印要求更高的稳健性。（T）

19.在现代，纸张的水印被广泛用于货币、各种银行和证券的票据以及各种需要标识的纸张中，起到防伪、标识的作用。（T）

20.版权标识水印又称为基于数据源的水印，水印信息标识（ ）等，并携带有版权保护信息和认证信息，用于发生版权纠纷时的版权认证，还可用于隐藏标识、防拷贝等。

A 作者

B 所有者

C 发行者

Chap 7 数字水印技术

1.通过分析现有的数字视频编解码系统，视频水印根据嵌入的策略一般可以分成（）。

A 在未压缩域中嵌入

B 在视频编码器中嵌入

C 在视频码流中嵌入

2.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。（T）

3.视频和图像有相类似的地方，但是视频水印和图像水印又有一些重要差异:（ ）。

A 视频信息作为大容量、结构复杂、信息压缩等特征的载体，调整给定水印的信息和宿主信号的信息之间的比率，变得越来越不太重要了。

B 可用信号空间不同。

C 视频作为一系列静止图像的集合，会遭受一些特定的攻击，如帧平均、帧剪切、帧重组、掉帧、速率改变等。

D 虽然视频信号空间非常大，但视频水印经常有实时或接近实时的限制，与静止图像水印相比，降低复杂度的要求更重要。

4.水印容量也常称为数据嵌入量，指单位长度的音频中可以隐藏的秘密信息量，通常用比特率来表示，单位为bit/s,即每秒音频中可以嵌入多少比特的水印信息。（T）

5.音频水印算法性能好坏一般使用（ ）指标来衡量。

A 透明性

B 容量

C 鲁棒性

6.动态数据结构水印的机制是，输入特定信息激发程序,把水印信息隐藏在堆、栈或者全局变量域等程序状态中。当所有信息都输完之后，通过检测程序变量的当前值来进行水印提取。可以安排一个提取水印信息的进程或者是在调试器下运行程序查看变量取值。（T）

7.根据水印被加载的时刻，软件水印可分为静态水印和动态水印。（ ）是保存在程序的执行状态中，而不是程序源代码本身。

A 静态水印

B 动态水印

8.根据水印被加载的时刻，软件水印可分为静态水印和动态水印。（ ）存储在可执行程序代码中，比较典型的是把水印信息放在安装模块部分，或者是指令代码中，或者是调试信息的符号部分。

A 静态水印

B 动态水印

9.根据水印的嵌入位置，软件水印可以分为代码水印和数据水印。（ ）隐藏在程序的指令部分中，而（ ）则隐藏在包括头文件、字符串和调试信息等数据中。

A 代码水印、数据水印

B 数据水印、代码水印

10.为了使软件水印能够真正发挥保护软件所有者的知识产权的作用，一般要求软件水印具有以下特征：（ ）

A 能够证明软件的产权所有者。

B 具有鲁棒性。

C 软件水印的添加应该定位于软件的逻辑执行序列层面而不依赖于某一具体的体系结构。

D 软件水印应该便于生成、分发以及识别。

E 对软件已有功能和特征的影响在实际环境下可以忽略。

11.软件水印就是把程序的版权信息和用户身份信息嵌入到程序中。（T）

12.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：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。其中，（）：即把图像本身作为水印加入，这不仅可以鉴别图像的内容，而且可以部分恢复被修改的区域，如图像被剪掉一部分或被换掉一部分，就可以利用这种水印来恢复原来被修改的区域，但这种水印可能是脆弱的或半脆弱的。

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

13.根据识别篡改的能力，可以将脆弱性水印划分为四个层次：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。其中，（）：指的是水印能够检测出任何对图像像素值进行改变的操作或对图像完整性的破坏，如在医学图像数据库中，图像的一点点改动可能都会影响最后的诊断结果，因此此时嵌入的水印就应当属于完全脆弱性数字水印。

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

14.所谓（）技术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、图像标志等作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 稳健性数字水印

B 脆弱性数字水印

15.对于图像取值比较均匀的光滑区域，人眼对这些地方的失真非常敏感，因此这些地方不适合嵌入水印。（T）

16.在设计稳健性的数字水印算法时，通常需要找到在某一种变换下的相对不变量，将水印嵌入在这些相对不变量中，这样，就可以在一定程度上抵抗相应的攻击或破坏。（T）

17.水印提取的输出结果可以是水印本身，也可以是判断水印是否存在的判决结果，这取决于水印提取算法。（T）

18.设C为被保护的数字产品，W为水印信息，K表示数字水印嵌入算法的密钥，CW 表示嵌入数字水印后的数字产品。则数字水印的嵌入过程包括四个部分:

( )：对被保护的数字产品C进行的预处理。此预处理可以是任何一种变换操作，如DCT变换、DFT变换、小波变换、傅里叶一梅林变换等；也可以是一些变换操作的组合还可以是空操作(这时嵌入的水印就成了空间域水印)。

( )：对数字水印W进行的预处理。WPP也可以是任何一种变换操作，与CPP类似。另外还可以包括诸如置乱处理等操作。

( )：数字水印嵌入算法。

( )：CPP的逆操作。

A CPP　WPP　G　CPP^{-1}

B WPP　G　CPP　CPP^{-1}

C G　CPP^{-1}　CPP　WPP

D CPP　G　CPP^{-1}　WPP

19.水印的稳健性包含两个方面的含义，从选用水印的形式上以及水印算法上都要考虑。（T）

20.第三类数字水印是一种可视图像，它可以是一个人的手写签名或者是一些字符，以一个二值图像的形式保存，也可以是一个徽标形式，以二值图像(或灰度图像)的格式保存。（T）

Chap 8 信息隐藏分析

1.目前对于图像LSB信息隐藏主要分析方法有（ ）等。

A 卡方分析

B RS分析法

C GPC分析法

2.被动隐写分析方法的评价,一般采用准确性、适用性、实用性和复杂度四个指标来衡量。其中，（ ）是针对隐写分析算法本身而言的，可由隐写分析算法实现需要的资源开销和软硬件条件来衡量。

A 准确性

B 适用性

C 实用性

D 复杂度

3.被动隐写分析方法的评价,一般采用准确性、适用性、实用性和复杂度四个指标来衡量。其中，（）是指分析算法可以实际推广应用的程度，可由实现条件是否允许、分析结果是否稳定、自动化程度的高低和实时性等进行衡量。

A 准确性

B 适用性

C 实用性

D 复杂度

4.被动隐写分析方法的评价,一般采用准确性、适用性、实用性和复杂度四个指标来衡量。其中，（）是指分析算法对不同的隐写算法的有效性。

A 准确性

B 适用性

C 实用性

D 复杂度

5.被动隐写分析方法的评价,一般采用准确性、适用性、实用性和复杂度四个指标来衡量。其中，（）是指检测的准确程度，是衡量隐写的一种评价指标。

A 准确性

B 适用性

C 实用性

D 复杂度

6.被动隐写分析方法的评价,一般采用（）等指标来衡量。

A 准确性

B 适用性

C 实用性

D 复杂度

7.隐写分析属于（）。

A 主动攻击

B 被动攻击

8.隐写载体经过不安全的信道, 可能会遭受蓄意和非蓄意攻击。非蓄意攻击包括信道噪声,传输过程编码转换引入的噪声等。蓄意攻击包括主动和被动攻击。（T）

9.讨论破坏隐藏信息的方法,不是有意提倡非法破坏正常的信息隐藏,它主要有两个方面的作用。

一方面,用于国家安全机关对违法犯罪分子的信息监控过程中,为了对付犯罪分子利用信息隐藏技术传递信息,可以采用破坏隐藏信息的手段。

另一方面,是用于合法的信息隐藏技术的辅助手段,作为一个评估系统,来研究一个隐藏算法的稳健性。（T）

10.对于用变换域技术进行的信息隐藏,采用叠加噪声和有损压缩的方法一般是不行的。 可以采用的有效的方法包括（ ），将以上这些技术结合起来使用,可以破坏大部分的变换域的信息隐藏。

A 图像的轻微扭曲、裁剪、旋转、缩放

B 滤波、模糊化

C 数字到模拟和模拟到数字的转换(图像的打印和扫描,声音的播放和重新采样)等

D 采用变换域技术再嵌入一些信息

11.信息隐藏分析的目的有三个层次：发现、提取、破坏。（T）

12.隐藏分析的目的：

（1）防止隐写术的滥用；

（2）寻找隐藏算法的漏洞，促进研制安全性更高的隐藏算法。（T）

13.隐写分析根据最终效果可分为两种: 被动隐写分析(PassiveSteganalysis)、主动隐写分析(Active Steganalysis)。其中，（ ）的目标是估算隐藏信息的长度、估计隐藏信息的位置、猜测隐藏算法使用的密钥、猜测隐藏算法所使用的某一些参数，其终极目标是提取隐藏的秘密信息。

A 被动隐写分析

B 主动隐写分析

14.隐写分析根据最终效果可分为两种: 被动隐写分析(PassiveSteganalysis)、主动隐写分析(Active Steganalysis)。其中，（ ）仅仅是判断多媒体数据中是否存在秘密信息，或尝试判断携密载体所采用的算法。

A 被动隐写分析

B 主动隐写分析

15.根据已知消息，隐写分析可分为以下几种：（）。

A 唯隐文攻击(Stego-only Attack)：只有隐写对象可用于分析。

B 已知载体攻击(Known Cover Attack)：可利用原始的载体对象和隐写对象。

C 已知消息攻击(Known Message Attack)：攻击者 可以获得隐藏的消息。即使 拥有消息，这也是很困难的，其难度甚至等同于唯隐文攻击。

D 选择隐文攻击(Chosen Stego Attack)：知道隐写工具(算法)和隐秘对象。

E 选择消息攻击(Chosen Message Attack)：隐写分析研究者用隐写工具或算法,对一个选择的消息产生伪装对象。这种攻击的目标是确定隐写对象中相应的模式。这些模式可能揭示所使用的特定的隐写工具或算法。

F 已知隐文攻击(Known Stego Attack)：知道隐写工具(算法)，可利用原始对象和隐写对象。

16.隐写分析根据隐写分析算法适用性,可分为两类：专用隐写分析(Specific Steganalysis)和通用隐写分析(Universal Steganalysis)。

( )，就是不针对某一种隐写工具或者隐写算法的盲分析。通用隐写分析方法在没有任何先知条件的基础下，判断载体中是否隐藏有秘密信息。

A 专用隐写分析

B 通用隐写分析

17.隐写分析根据隐写分析算法适用性,可分为两类：专用隐写分析(Specific Steganalysis)和通用隐写分析(Universal Steganalysis)。其中， （ ）是针对特定隐写技术对象的特点进行设计，这类算法的检测率较高，针对性强，但这类隐写分析算法只能针对某一种隐写算法。

A 专用隐写分析算法

B 通用隐写分析算法

18.隐写分析是针对图像、视频和音频等多媒体数据,在对信息隐藏算法或隐藏的信息一无所知的情况下,仅仅是对可能携密的载体进行检测或者预测,以判断载体中是否携带秘密信息。 （T）

Chap 9 数字水印的攻击

1.对水印的攻击可分为（ ）。

A 去除攻击

B 表达攻击

C 解释攻击

D 法律攻击

2.下列属于水印攻击软件的有： （）。

A Unzign

B StirMark

C OptiMark

D CheckMark

3.（）既不试图擦除水印,也不试图使水印检测无效,而是使得检测出的水印存在多个解释。

A 去除攻击

B 表达攻击

C 解释攻击

D 法律攻击

4.几何变换在数字水印的攻击中扮演了重要的角色，而且许多数字水印算法都无法抵抗某些重要的几何变换攻击。常见的几何变换如下：（）。

A 水平翻转、裁剪

B 旋转、缩放

C 行、列删除、 普通几何变换

D 打印-扫描处理、随机几何变形

5.表达攻击与去除攻击的不同之处在于，它并不需要去除载体中的水印，而是通过各种办法使得水印检测器无法检测到水印的存在。（T）

6.水印攻击中，信号处理技术也是最常用到的攻击手段，它们有可能是非恶意的攻击，但是也有可能被用来做恶意的攻击。这类技术有：（）。

A 低通滤波、添加噪声

B 锐化、直方图修改

C Gamma校正、颜色量化

D 修复、统计均衡和共谋攻击

7.常见的稳健性攻击可以分为有损压缩和信号处理技术两个方面。（T）

8.去除攻击是研究稳健性数字水印算法的一个重要的辅助手段。通常设计一个稳健的数字水印，都要检验其能够抵抗哪些稳健性攻击，或者各种攻击的组合（T）

9.恶意攻击是以去除水印为目的,它们是在保证数字载体仍然能够使用的情况下，尽可能的消除水印。（T）