**信息隐藏技术概论**

**（一）绪论**

1.基本概念

简要阐述信息隐藏的概念、掌握信息隐藏的基本思想；

信息隐藏就是将秘密信息隐藏于另一公开载体中，而不引起检查者的注意。

信息能隐藏的原因：多媒体信息本身就有很大的冗余性；人眼或人耳本身具有掩蔽效应，对边缘附近的信息不敏感。

信息隐藏算法的评价系统

透明性、鲁棒性、隐藏容量、安全性、不可检测性、自恢复性。

2.了解信息隐藏的组成及其分类；

广义的信息隐藏技术包括：隐写术、数字水印技术、数字指纹技术、隐蔽信道、阀下信道、低截获概率通信和匿名通信。

按照载体类型分类，信息隐藏技术可以基于文本、图像、音频、视频、三维模型和动画等各种不同媒体的信息隐藏技术（文本信息隐藏，基于图像的信息隐藏、音频信息隐藏）

按密钥对称分类可以分为无密钥信息隐藏、对称信息隐藏和非对称信息隐藏

按嵌入域分类可以分为原始域（包括空域、时域和时空域）、变换域和压缩域

按秘密信息提取时是否需要原始载体对象的参与可以分为非盲隐藏和盲隐藏

按可逆性进行分类可以分为可逆信息隐藏和不可逆信息隐藏

按鲁棒性分类可以分为鲁棒信息隐藏、脆弱信息隐藏和半脆弱信息隐藏

按要保护的对象分类，可以分为隐写术和版权标记技术

重点理解鲁棒水印脆弱水印区别。

脆弱水印是在保证原始载体对象和伪装对象感知相似的条件下，不管遭受恶意或无意的攻击，隐藏的秘密信息都会丢失。

鲁棒水印是在保证原始载体对象和伪装对象的感知相似条件下，在各种恶意或无意的攻击下，秘密信息都不能修改或移除。

了解信息隐藏安全性的概念，掌握度量安全性的指标。

信息隐藏安全性是指算法具有一定的抗恶意攻击能力，能承受一定程度的人为攻击，而嵌入的秘密信息不被破坏。

3. 重点难点：掌握信息隐藏与密码学之间的联系与区别。

密码术仅仅隐藏了信息的内容，信息隐藏不仅能隐藏信息的内容，还可以隐藏信息的存在。

破解密码术，相当于攻击者破解了加密信息，获取了原始信息的内容。

破解隐写术有两个步骤，检测到伪装对象中包含了隐藏信息，获取或破坏隐藏信息。

**（二）多媒体基础知识**

1.主要内容

多媒体图像与语音信号处理的基本知识，以及图像与语音处理的质量评价

2. 基本要求

(1)了解多媒体图像处理的基础知识，了解图像处理的质量评价，掌握图像变换的基本思想。

通过对DC系数的移位实现信息的嵌入

(2)了解音频和语音信号处理的基础知识，了解音频处理的质量评价，掌握音频变换的基本思想。

3.重点难点

多媒体图像处理中变换域的知识。

**（三）隐写术**

1.隐写术的应用举例、图像与语音信号的隐写方法（隐秘地传递密钥、数字签名、私密信息等）

2. 基本要求

(1)了解适用于图像的隐写方法的基础知识，了解并掌握图像LSB隐写方法、DCT隐写方法等的基本思想。

(2)了解音频隐写方法的基础知识，了解并掌握音频LSB隐写方法的基本思想，了解回声隐藏方法的基本思想。

3.重点难点

图像隐写方法，如LSB隐写方法、DCT隐写方法的基本思想和实现方式。

（四）隐写分析

1.主要内容

隐写术与隐写分析的关系、隐写术的隐写分析方法

关系：

隐写分析是根据可疑隐写对象的某一特性或统计特性来检测是否嵌入秘密信息，若有，则尽可能提取隐藏信息。

方法：

感官检测；统计检测；特征分析。

2. 基本要求

(1)了解隐写分析的基本概念和思想，了解并掌握隐写分析方法的分类。

分类：

根据隐写分析达到的效果或目标可以分为：被动攻击、主动攻击、提取攻击；

根据隐写分析者能够获得的信息可以分为：唯隐写对象分析、已知载体对象分析、已知秘密消息分析、选择秘密信息攻击、选择隐写对象攻击、已知隐写攻击；

根据分析过程中所采用的方法可以分为：感官检测、统计检测和特征分析。

(2)了解隐写分析方法的关键，了解并掌握可视攻击和卡方分析。

3.重点难点

对信息隐藏方法进行有针对性的隐写分析。

（五）数字水印技术

1.主要内容

数字水印的概念、原理与实现方法

数字水印的基本思想是在图像、音频、视频等数字产品中嵌入秘密信息以便于保护数字产品的版权、证明产品的真实可靠性、跟踪盗版行为或者提供产品的附加信息。

2. 基本要求

(1)了解数字水印技术的基本概念，了解并掌握数字水印技术的基本原理，掌握数字水印的分类及相关模型。

从含水印图像中的水印是否可见可以分为：可见水印和不可见水印

从水印生成是否依赖于原始载体可以分为：非自适应水印和自适应水印

从水印载体的抗攻击能力可以分为：脆弱水印、半脆弱水印和鲁棒水印

从水印检测是否需要原始图像参与可分为：明检测水印和盲检测水印

(2)了解数字水印的常用实现方法，了解并掌握DCT数字水印、扩频水印的方法原理，了解数字水印技术的攻击技术。

攻击技术：

JPEG压缩攻击；几何失真攻击；增强处理攻击；加噪攻击；打印扫描攻击；统计平均和共谋攻击；嵌入多重水印攻击；Oracle攻击。

(3)数字水印技术的应用

广播监控(broadcast monitoring)、所有者识别(owner identification)、所有权验证(proof of ownership)、交易跟踪(distribution tracing)、内容真伪鉴别(proof of authenticity)、复制控制(copyright control)和设备控制。

3.重点难点

数字水印与隐写术的联系与区别。

两者的基本思想都是在载体对象中嵌入秘密信息。

隐写术中的秘密信息是重要保护对象，至于用什么载体对象进行传输无关紧要。

数字水印中，载体对象通常是版权保护对象，秘密信息是与该载体对象相关的版权标志、购买者或其他相关信息。

（六）数字指纹技术

1.主要内容

数字指纹的概念、原理与应用

2. 基本要求

(1)了解数字指纹概念、特性及应用

概念：

数字指纹技术是在数字内容中嵌入与用户有关的信息，分别向不同用户复制中嵌入不同的信息，嵌入的指纹对不同的购买者是不同的。

特性：

鲁棒性；不可感知性；抗共谋攻击；嵌入容量；唯一性；准确性；安全性；效率；其他要求；设计目标（捕获共谋者，停止非法拷贝）

应用：

内容识别；盗版者/叛逆者追踪；版本控制；内容过滤；广播监控

(2)了解并掌握数字指纹的分类。

按照协议类型分类可以分为：对称指纹、非对称指纹和匿名指纹；

按照基于加入指纹的产品可以分为：数字指纹和物理指纹；

按照基于对侵害的检测灵敏度可以分为：完美指纹、统计指纹和门限指纹；

按照基于嵌入指纹的方法可以分为：识别指纹、删除指纹、添加指纹和修改指纹；

按照生成的指纹可以分为：离散指纹和连续指纹。

3.重点难点

数字水印与数字指纹的联系与区别

数字水印技术把相同的、标记版权的特殊信息嵌入到所有的数字产品中，相同的数字产品拥有相同的水印信息，主要用于版权证明。

数字指纹技术把不同的指纹信息（序列码）嵌入到不同消费者所购买的数字产品中，不同消费者所得到的是内容相同、但嵌入不同指纹信息的指纹复制，主要用于盗版者追踪，多用于网络服务中的版权保护。

两者都是信息隐藏技术，数字指纹技术以数字水印技术为基础，都需要较高的鲁棒性。

**Part I: True or false, with explanations (20 points total)**

This part comprises 5 statements. You should mark each statement as true or false; in addition, you should provide a one or two line justification of your answer. The true/false part of each statement is worth 1 point, while the justification is worth 3 points. (It is possible to get full credit for the justification even if you miss the true/false part.)

1. *True or False. LSB information hiding method performs better than DCT based information hiding method.*
2. *True or False. LSB method and DCT based information hiding method are both fragile.*

**Part II: Reading Comprehension (25 points total)**

This part comprises five questions. You should answer each question in about a paragraph in Chinese. Each question is worth five points.

*Basic concepts, differences, relationship etc.*

**Part III: Short Answer (55 points total)**

This part comprises five questions. You should answer each question in about a paragraph in Chinese. Each question is worth five points.

*LSB, DCT, Visual Attack Steganalysis*