数字内容安全

\*\*问题驱动

1.什么是数字内容

2.存在哪些安全问题

3.在哪些领域存在

4.相关技术

5.未来趋势

1. 数字内容

1.1 数字内容概述

1.1.1 数字内容内涵

1. 信息最早出现在通信领域
2. 信息内涵的演变

①1948年，信息论创始人香农提出：信息是用来消除随机不确定性的东西（使熵减少）

②计算机出现后，信息被看做数据

③二战后，信息是经验、知识和资料，泛指一切能够处理的数值、文字、符号、语音、图形等

1. 信息与内容

①相同点：在信息科技中是等价的，均指与具体表达形式、编码无关的知识、事物、数据等含义。

②不同点：

\*内容：轮廓性、主观性，与语义相关，不同的信息可能被认为是相同的内容

\*信息：细节性、客观性，一般不认为一个信息可以在主观感知下对应多个含义。具有互信息（I(x,y)=H(x)-H(x|y)）、自信息（I(x)=E(p(x))）、熵等概念，可以用比特（BIT）、奈特（NAT）、哈特（HART）等单位衡量数量的多少

1. 数字内容（信息的主要表现形式）

①定义：数字内容生成后，以数字形式存在的文本、图像、声音、视频等信息，可以存储在光盘、硬盘等数字载体上，并通过网络等手段传播。

②与其他表现形式的区别：以数字化方式存在

③组成要素：来源、归宿、传播信道

④应用：产业化，数字影像、科学出版、动漫游戏

1.1.2 数字内容产业

1. 数字内容产业定义

数字内容产业是生产数字信息内容产品和提供相应服务的产业，生产过程包括信息的收集、处理、加工、存储、交易、服务。以内容为核心，以信息或数字为纽带，强调内容与其他行业的交叉和融合。

1. 信息产业

凡是以内容加工为对象，产品形式表现为信息形式的，都属于信息产业。数字内容产业属于信息服务业。

1. 数字内容产业分类

数字传媒、数字娱乐、数字学习、数字出版、面向专业应用

1.2 新媒体数字内容发展

1.2.1 新媒体的基本概念与特点

1. 媒体：一般意义上的媒体都包含内容和载体两方面（内容和内容的载体、传输和传输的载体），媒体是内容信息表示和传输的载体
2. 内容表示载体：记载和表达信息的载体（文字、声音...）。内容的形态由内容载体所决定，内容载体的性质决定了内容的表现形式与创作形式。
3. 传输载体：决定如何将创作的内容传递给用户（图像、音频、视频、文本）
4. 新媒体创新
5. 内容载体：相较传统媒体内容载体的单一性，新媒体能够覆盖多种展现手段，被称为多媒体或富媒体。
6. 传输载体：基于互联网、有线、无线移动等多种形式，可使用多种终端来接收和展现信息。
7. 交互方式：提供双向传输，支持互动

\*\*新媒体是通过网络传输，并且具有交互能力的丰富媒体系统

1.2.1 三网融合

电信网、广播电视网、计算机通信网

1.2 数字媒体内容分类

1. 数字广播媒体内容

\*广播分类

1. 传播手段：无线广播、有线广播
2. 传播媒介：声音广播，电视广播
3. 网络电视媒体内容

互动电视、互联网电视、移动电视、OTT电视

1. 数字电影媒体内容
2. 数字游戏媒体内容
3. 数字音乐媒体内容
4. 数字出版媒体内容
5. 网络社区媒体内容

1.4 数字内容产业的问题

1、产业政策协调不够

2、产业结构发展不均

3、版权保护措施不足

4、技术能力有差距（存储空间、压缩

1.5 数字内容关键技术

1、图像采样与量化。 图的子标题

光学成像 —> 数字化

传感器阵列：记录光信号颜色、强度，光电转换，量化（除以量化步长）把连续的信号转化为离散数字图像

模数转换：电压信号 —> 数字信号

2、数字图像的表示

f (x) I(x) 下标注意

图像矩阵表示：A=[ ]

3、数字图像的空间分辨率

32x32 pixel

与距离有关

4、数字图像的灰度分辨率

5、离散傅立叶（DFT）变换

幅度谱、相位谱（f（0，0）在中间，直流分量，存在突变高频更大，什么方向存在突变，什么方高频有值）

1. 消息认证与数字签名
2. 密码学基础知识
3. 密码学分类

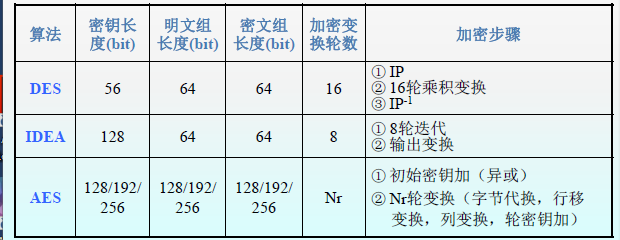
\*按操作分：代换密码、置换密码

\*按使用密钥数量：对称密码（序列，分组）、公钥密码

1. 典型对称密码算法

\*序列密码（流密码）：RC4

\*分组密码：DES，AES，IDEA



1. 典型公钥密码算法



1. 两种密码体制优缺点

\*对称：效率高、算法简单、适合加密大量数据

密钥的安全传输困难

\*公钥：密钥管理方便

加解密速度慢

1. 消息认证概念
2. 信息安全基本属性

保密性Confidentiality、完整性 Integrity、可用性 Availability、不可抵赖性、可控性

1. 消息认证

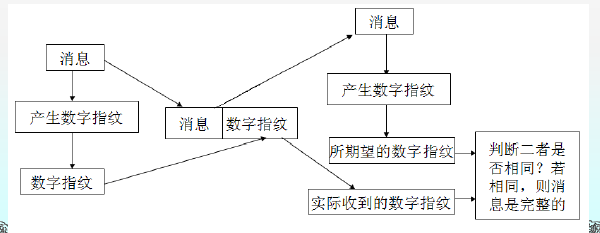
\*概念：指通过对消息进行加密或签名变换而实现的认证

\*目的：防止传输和存储的消息被篡改

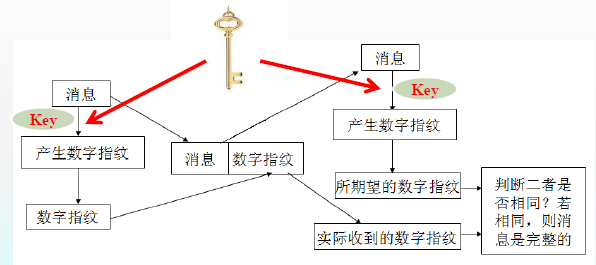
\*组成：消息内容认证（完整性）、消息源宿认证（身份认证）、消息的序号和操作时间认证

1. 消息认证的两层含义
2. 检验消息的完整性：验证消息在传送或存储过程中未被修改
3. 验证消息来源的真实性：身份认证
4. 消息完整性检验

\*基本思想：数字指纹比对



\*一般方法：单向hash函数（MD5、SHA）

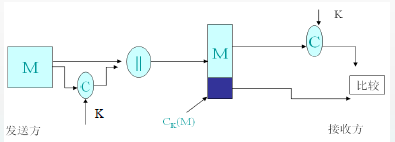


1. 消息认证技术
2. 消息认证码（MAC=CK(M)）

\*组成：M：可变长消息，K：收发双方共享的密钥，CK(M)：定长的密码校验和

\*原理：用公开函数和密钥产生一个固定长度的值作为认证标识，用这个标识鉴别消息的完整性。接收方利用共享密钥进行身份认证。

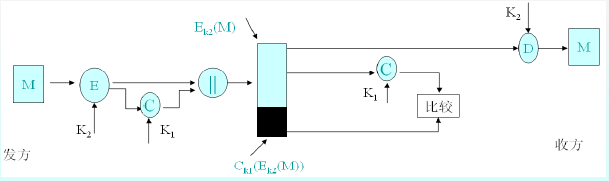
\*过程：



\*得到结论：

1. 验证完整性：接收方确信消息M未被篡改
2. 验证消息源：除收发双方没有人知道这个共享密钥。
3. 消息认证与保密

\*既加密又认证



1. 感知哈希（2001提出）
2. 传统哈希的局限

\*典型：RSA数字签名算法（matlab实现）

1. 定义：哈希函数不可逆的提取原始数据的数字摘要，具有单向性、脆弱性等特点，可保证原始数据的唯一性与不可篡改性。
2. 局限：

\*无法满足多媒体信息管理和保护的需求

\*仅具有数据压缩性，不能消除多媒体感知内容上的冗余

\*\*将图片由png压缩到jpeg：Q越低压缩越严重

\*多媒体数字化表示与该媒体内容之间存在多对一映射，要求内容摘要具有感知鲁棒性，二传统哈希对任何数字表示改变是脆弱的。

\*\*PSNR值越大，两幅图片越相似（）

1. 优点：比特级别完整认证

\*\*比较内容篡改：

Hash

A ——> b1b2b3...b128（128位摘要）

Hash

A’——> b1’b2’b3’...b128’（128位摘要）

统计匹配成功百分比：

随机变化，因为每位比特为0、1值，所以每位变化的概率为50%。

1. 感知哈希概念
2. 定义：能将大数据量的多媒体对象映射为长度较小的比特序列，将感知想进的媒体对象映射成数学相近的哈希值。基于心理学的信息加工理论，由多媒体数据集到多媒体感知摘要集的一类单向映射，将具有相同感知内容的多媒体谁表示唯一的映射为一段数字摘要，能够满足感知安全性。
3. 应用场景：基于内容的媒体访问（识别、检索、认证），多媒体信号处理，多媒体安全
4. 提出与发展：研究满足多媒体内容压缩性、感知鲁棒性的多媒体单向摘要算法与技术。
5. 理论基础：认知心理学

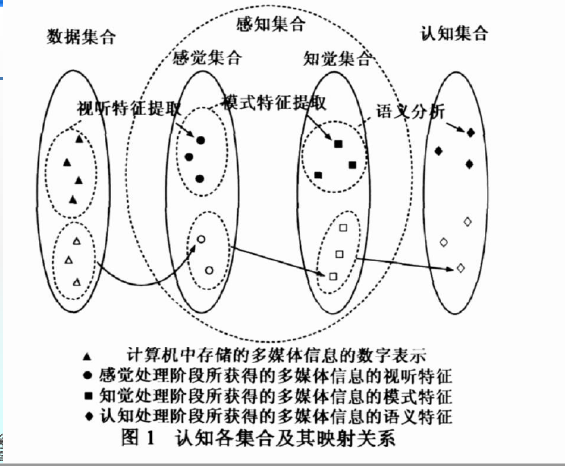


\*模式识别：总结出类

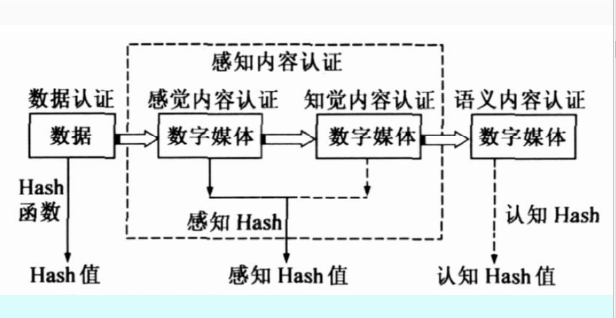
场景——>事件

\*物体识别：物体

分类（纹理、颜色、边缘）



1. 感知哈希函数：PH：M——>Hp（Hp为感知数字摘要集合）
2. 与传统哈希区别（发展）



1. 性质（6）

\*抗碰撞性（内容敏感性）

\*感知鲁棒性

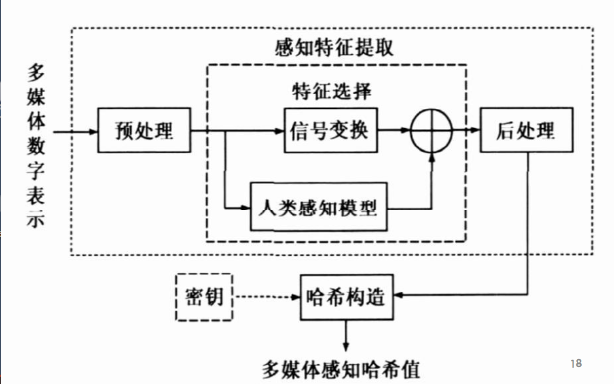
\*单向性

\*随机性

\*摘要性

\*易于实现，计算效率高

1. 感知哈希技术



1. 预处理：分帧**（抽取出一帧一帧的图片）**、滤波，提高特征选择的准确性
2. 感知特征提取：以人类感知模型为基础，得到多媒体对内容保持操作的感知不变性**（通过特征选择描述当前物体，通过纹理、边缘、颜色等特征）**

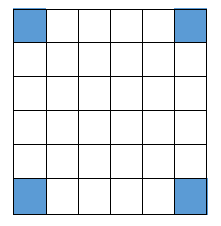
**\*方法：① 边缘检测（matlab实验）**

**② 分块（8x8等），对每个小分块求均值（亮度分布感知向量），每个图像提取出的结果都是不同的，能够抵抗压缩攻击**

1. 特征选择：通过与人类感知模型一致的各种信号处理方法，去除感知冗余，选择最具有感知意义的特征参数。**（例：选取分块中最重要的特征）**
2. 后处理：对选择的特征参数进行量化以及编码等后处理。**（量化后取整等操作）**
3. 哈希构造：对感知特征进一步降维**（0~255转化为二进制比特流）**，并输出最终结果，即感知哈希值**（通过最后的输出结果能够比较相似度）**。**（长度不是固定的，因其具有感知鲁棒性，所以内容相同时哈希值也应相同）**

\*满足抗碰撞性、单向性、随机性等安全性要求

**\*方法：**

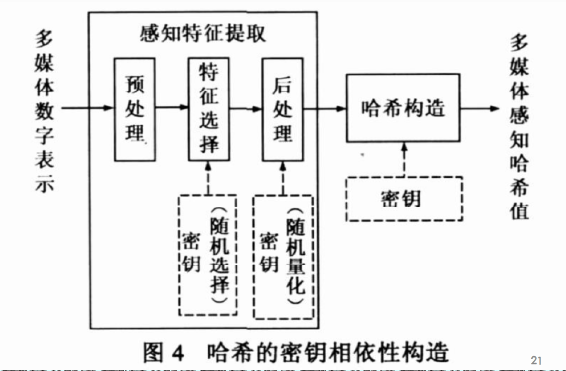


**1 分块>整体+阈值**

**0 分块<整体-阈值**

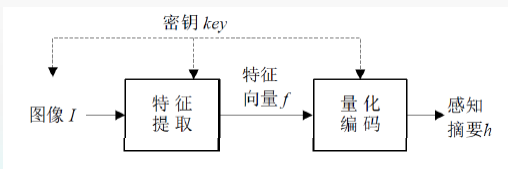
**每个分块求均值，而后比较各分块与整体的均值大小，决定提取出的是0还是1。**

1. 密钥相依性：针对应用的不同安全需求，可选择在不同阶段使用密钥实现密钥相依性**（每个阶段都可以引入密钥机制）**



**\*加密方法举例：**

1. **每个分块均值的排列顺序可以打乱**
2. **图像像素位置的置乱与反置乱（经典：Arnold公式**）
3. **局部置乱：进行分块平滑操作（例：马赛克）**
4. 感知哈希算法
5. 生成算法



**\* 特征向量：二维或一维的特征数组组成。**

**\*量化编码：R—（q）—>Z——>B（应用：DCT变换等）**

**优点：具有一定的鲁棒性，x在小范围内抖动时x’不变**

  **（q为量化步长）**

1. 匹配算法：对比两个感知摘要
2. 感知哈希算法分类
3. 基于空域特征：亮度、图像分块
4. 基于变换域特征：DFT、DCT、DWT、Fourier-Mellin**（对几何变换具有鲁棒性）**
5. 矩阵分解：SVD**（奇异值分解）**、NMF**（非负分解）**
6. 细节特征：特征点**（角点—两边缘角点、SIFI—广泛应用于人脸识别..）**

1、基于图像统计特性的特征：利用了图像块直方图**（即概率分布，x轴为取值范围，y轴为频次，，E[x]为直方图，h(i)为均一化的直方图）**的均值、方差和高次惯量等统计不变性属性

2、基于关系的特征：基于DCT、DWT等变换系数之间的相对大小关系

3、原始图像粗略特征（利用其对感知的显著性）：粗略特征包括低频DCT系数**（平均亮度，反映大体轮廓）**、低分辨率的小波系数、SVD的最强奇异矢量、Fourier-Mellin变换的旋转不变性

4、基于边缘或特征点的低层**（低层：像素、中层：物体、高层：场景）**图像特征

\*\*补充

内容改变型操作：删减、替换、合成 => 哈希摘要完全不同

内容保持型操作：滤波、压缩、几何变换 => 应具有感知鲁棒性，哈希摘要相同

xx操作：改动（≠ 篡改）多媒体文件

\*\*考点：名词解释——内容、语义、认知、感知、鲁棒性

1. 感知哈希技术异同比较
2. 与鲁棒哈希技术

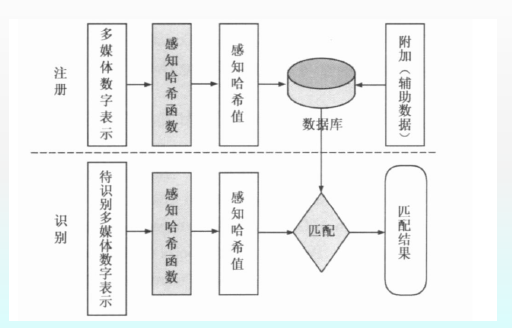
\*鲁棒哈希是以任意不变量的选择为建立映射的基础

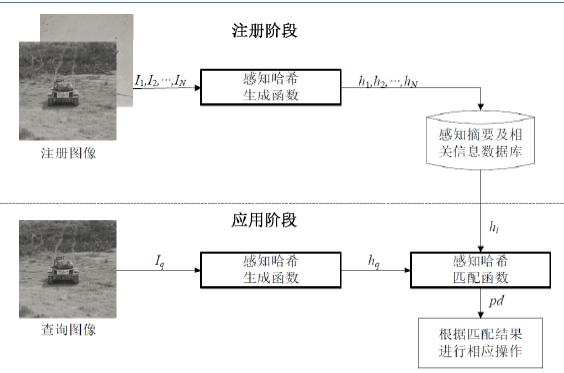
\*感知哈希技术是以多媒体感知特征为不变量

1. 与数字指纹技术

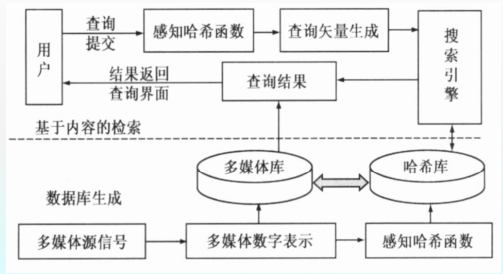
\*数字指纹主要分为用于版权保护的数字水印技术和应用于媒体内容识别的媒体摘要技术

1. 典型应用
2. 识别

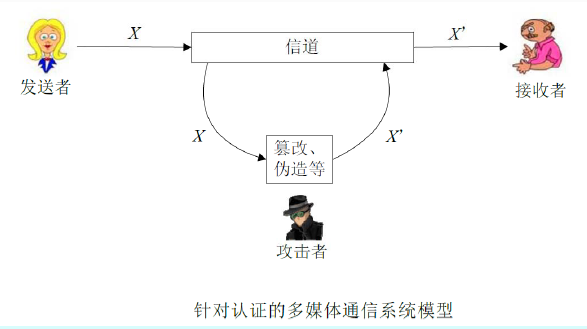


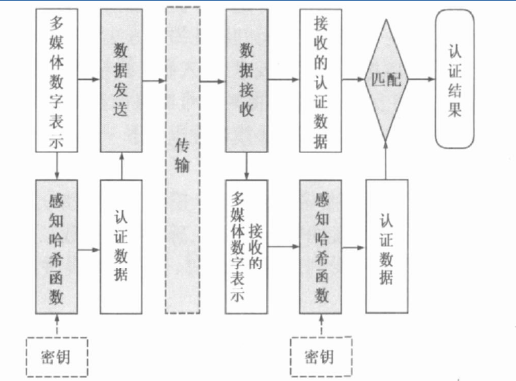


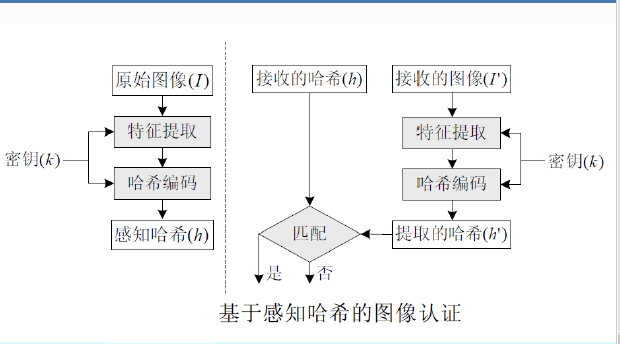
1. 检索

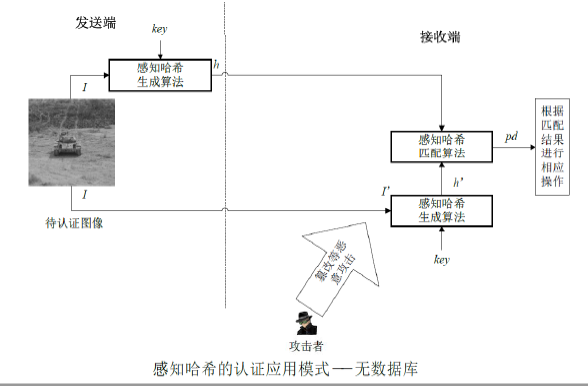


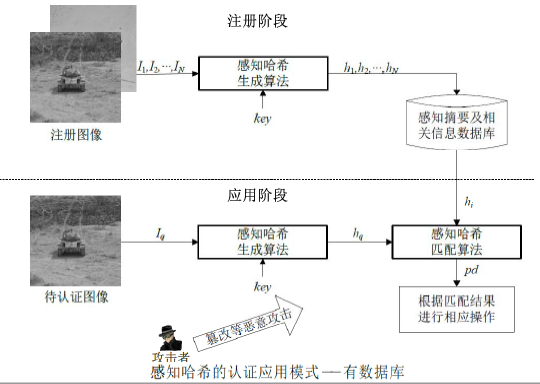
1. 认证











1. 信息隐藏与数字水印
2. 信息隐藏基本概念
3. 术语

Steganography 隐写(术)

Steganalysis 隐写分析

Cryptography 密码术

Payload 有效载荷

Capacity 容量

Transparency 透明性

Cover 载体

Distortion 失真

1. 技术背景

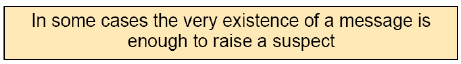
\*远古时代的隐写术

\*篡改检测和恢复

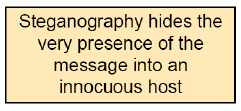
\*图像局部隐藏和恢复（特定目标消隐及图像修复技术）

1. 技术动机

\*Cryptography



\*Steganography



\*利用载体传递/携带某种信息：秘密信息、版权信息、认证信息、附加/辅助信息

\*不影响载体的正常使用（不被察觉）

1. 产生背景

\*问题：侵权、篡改

\*需求：既充分利用数字内容，又要有效地保护知识产权、内容安全

\*信息隐藏学：一门新兴的交叉学科

1. 相关概念
2. 信息隐藏定义：信息隐藏（Information Hiding），也叫数据隐藏（Data Hiding），指将秘密信息隐藏于另一非保密的载体之中。这里的载体可以是图像、音频、视频、文本、信道，或某编码体制或系统。
3. 术语解释

（1）原始载体：专指待嵌入秘密信息的原始载体数

据。

（2）嵌入：通常指通过修改载体数据的方式将秘密

信息隐藏到公开载体中的行为或过程。

（3）掩密载体：也称含密载体，专指嵌入秘密信息

后的载体数据。

（4）提取：指从掩密载体中提取事先所隐藏的秘密

信息的行为或过程。

1. 信息隐藏可行性

（1）多媒体信息自身存在很大的冗余性。

-将机密信息嵌入到多媒体数据中进行秘密传送是可行的，

并不会影响多媒体数据本身的传送和使用。

（2）人类视听觉系统的掩蔽效应。

-可充分利用这种掩蔽性将信息隐藏而不被察觉。

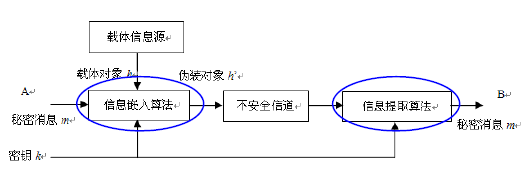
4、信息隐藏与传统密码学的区别

（1）密码学（加密通信）：研究如何将机密信息进行特殊的编码，以形成不可识别的密码形式（密文）进行传递。可能的监测者或非法拦截者可通过截取密文，并对其进行破译，或对密文进行破坏后再发送，从而影响机密信息的安全；

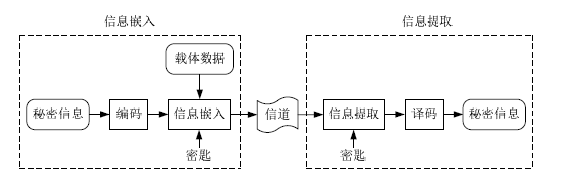
（2）信息隐藏：研究如何将某一机密信息秘密隐藏于另一公开的信息中，然后通过公开信息（载体）的传输来传递机密信息。监测者或非法拦截者则难以从公开信息中判断机密信息是否存在，难以截获机密信息，从而能保证机密信息的安全。

三、信息隐藏原理

1、原理框图



1. 基于通信的信息隐藏模型



原理：按秘密信息的传递过程一般可将信息隐藏系统分成两大模块：信息嵌入和信息提取。

（1）信息嵌入模块主要描述将秘密信息嵌入到载体数据中的过程。首先，为尽量减少待嵌入的数据，一般会预先对秘密信息进行信源编码；同时为提高秘密信息抵抗信道失真的干扰，可对秘密信息进行信道编码。然后，在密钥的控制下，依照所设计的信息嵌入算法将编码后的秘密信息嵌入到公开的载体数据中，得到掩密载体。掩密载体可通过公开的通信信道进行发布和传输，在传输过程中可能遭受到各种形式

的失真或干扰

（2）信息提取模块主要描述从接收到的掩密载体中提取秘密信息的过程。一般而言，信息

提取是信息嵌入的逆过程。

1. 信号处理角度理解信息隐藏

\*信息隐藏可视为在强背景信号（载体）中叠加一个弱信号（隐藏信息）。由于人的听觉系统和视觉系统的分辨能力收到一定的限制，叠加的弱信号只要低于某一个阈值，人就无法感觉到隐藏信息的存在。

1. 信息嵌入的各种公式表示
2. H’=H+f(H,W)

\*H：原始载体信号

\*H’：隐藏信息后的含密载体信号

\*W：待隐藏信息

1. hi’=hi+αwi
2. hi’=hi(1+αwi)
3. hi’=hi+α|hi|wi

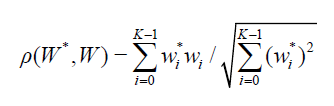
\*hi：原始载体信号

\*hi’：掩密载体信号

\*wi：待嵌入隐藏信号分量

\*α：嵌入强度

1. 信息提取的公式表示
2. w\* ( h\* h ) / α
3. w\* ( h\* h ) / α\*h’
4. 计算相似度的公式表示



=

7、水印检测的三个步骤

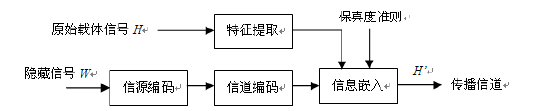
1. 计算检测的水印与原始水印信息的相关性
2. 门限化所得到的计算结果（阈值化判决）



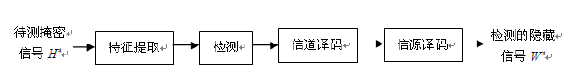
1. 判断水印是否存在
2. 信号处理角度理解信息隐藏——扩频通信模型

\*从数字通信的理论出发，可以理解为在一个宽带信道（原始载体信息）上采用扩频通信技术传输一个窄带信号（隐藏信息）。由于隐藏信号的能量较低，它分布在信道中任意特征上的能量是难以检测到的（隐藏信息的检测可理解为在一个含噪声信道中的弱信号检测问题）

1. 信息隐藏



1. 信息提取



1. 技术分类

1、根据应用目的

1. 隐写术

\*隐蔽通信技术

\*目的：将重要信息隐藏起来，以便不引起人注意的进行传输和存储

\*分类：语义隐写和技术隐写

\*技术要求：（**统计意义上的**）不可见性或隐蔽性，即不可检测性；掩盖“信息隐藏”行为或事实。

1. 数字水印

\*定义：通过在原始数据中嵌入秘密信息来证实数据所有权或鉴别数据真实性。被嵌入的水印可以是文字、标识、序列号等（容量），通常是不可见的（透明性），并可以经历一些不破坏原数据使用价值或商用价值的操作而能保存下来（鲁棒性）。

1. 隐蔽信道

\*定义：允许进程以危害系统安全策略的方式传输信息的通信信道

1. 阈下信道

\*定义：基于公钥密码技术的数字签名、认证等应用密码体制的输出密码数据中建立起来的一种隐蔽信道，除指定的接收者外，任何其他人均不知道密码数据中是否有阈下消息存在。

2、根据应用场合

（1）隐写术：实现信息的伪装的隐蔽性

（2）数字水印：水印信息的鲁棒性

1. 根据载体类型

文本信息隐藏、图像信息隐藏、音频信息隐藏、视频信息隐藏

1. 根据秘密信息隐藏位置

空域信息水印、频域信息水印

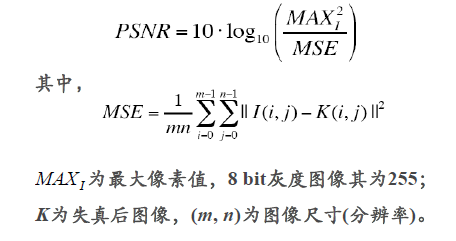
1. 信息隐藏技术的应用
2. 版权保护（鲁棒水印）
3. 内容认证（脆弱水印）
4. 隐秘通信（隐写）
5. 数字指纹
6. 技术要求
7. 隐写术：不可感知性、不可检测性、秘密性、较大水印容量、算法实现简单
8. 鲁棒水印：不可感知性、鲁棒性、抵抗恶意攻击能力、秘密性、算法实现简单
9. 完全脆弱水印：不可感知性、脆弱性（对任何处理都敏感）、秘密性、算法简单
10. 半脆弱水印：不可感知性、对内容改变型操作敏感、对内容保持型操作鲁棒、秘密性、算法简单

\*鲁棒性、容量、不可见性

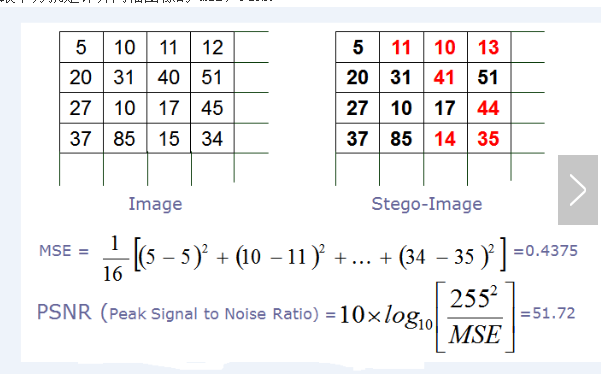
1. 评价指标
2. 透明性：信息隐藏行为不可感知且不影响被保护数据的正常使用

\*\*峰值信噪比：PSNR

1. 公式



1. 计算举例



1. 鲁棒性（脆弱性）：在经历有意或无意信号处理操作后，仍能完整或部分提取所隐藏秘密信息的能力
2. 容量：载体中所隐藏秘密信息数量（bit/pixel）
3. 空域/变换域信息隐藏技术
4. 空域信息隐藏技术

\*基本概念：在载体（图像、音频、视频）的空间域上进行信息隐藏，通过改变宿主像素值或采样值嵌入数据

\*优点：计算简单、效率高

\*缺点：难以抵抗常见信号处理的攻击及噪声干扰的影响，鲁棒性较差

1. 典型算法

（1）基于替换LSB的空域信息隐藏技术（LSB信息隐藏算法）

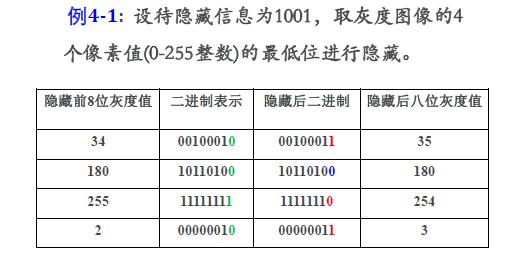
\*位平面：8级灰度图像（0~255）

①直接替换LSB方法

\*\*核心思想：用秘密信息取代LSB

\*\*实现方法：信息和载体lsb相同，不做修改；和载体lsb不同，原始lsb为奇数，减一，原始lsb为偶数，加一

\*\*举例：



\*\*嵌入位置的选取：连续嵌入（秘密信息+伪随机序列，可重复嵌入）

随机间隔（伪随机数发生器决定嵌入位置）

②基于奇偶校验位的LSB方法

\*\*核心思想：将载体分成不重叠区域，每个区域嵌入1比特信息。

计算奇偶校验位，如果奇偶校验位与秘密信息不同，则将区域I中LSB取值反转（区域内应含有奇数个像素）：



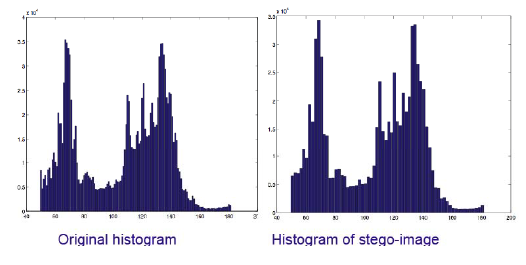
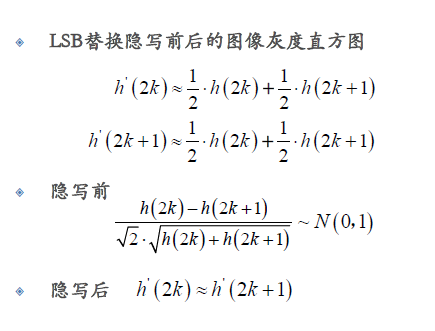
③基于替换LSB的空域信息隐藏

\*\*LSB：最不重要比特位

\*\*图像部分像素的最低一个或多个位平面的值被隐藏数据所代替

\*\*特点：具有较大的信息隐藏容量、计算简单、掩密图像失真小、隐藏数据的鲁棒性较差

\*\*隐写分析：



④MLSB（Multiple LSB）替换信息隐藏

\*\*方法一：随机选取最低多个位平面的比特位进行替换

\*\*方法二：随机选取像素，同时替换其多个最低有效位

⑤LSB匹配隐写（+-1隐写）

\*\*基本思想：带嵌入秘密信息比特与像素值得lsb不同时，随机加减一使像素值的LSB等于秘密信息比特

1. 基于patchwork的信息隐藏技术（空域）

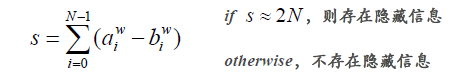
\*\*概念：拼凑算法只试图回答是否有水印存在，实际隐藏的只是1bit信息（单比特水印技术）

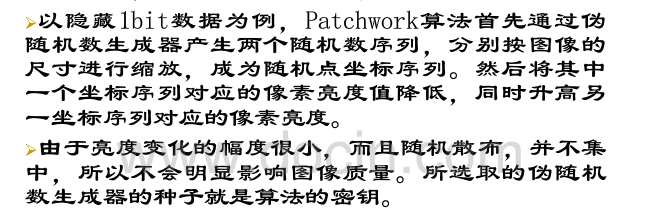
\*\*步骤：

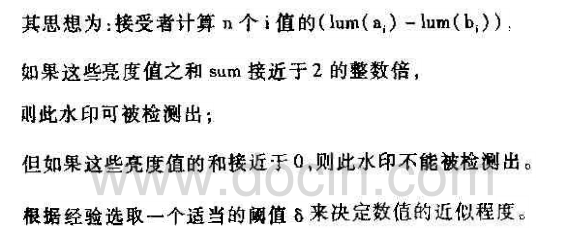
①用密钥初始化一个随机数发生器

②根据伪随机数发生器的输出，随机选择N个像素对（灰度值为(ai,bi)）

③令完成信息嵌入，整个图像的平均亮度保持不变。检测时：







\*\*特点：数据量小、透明性好、鲁棒性强

1. 变换域信息隐藏技术

\*基本概念：借助信号进行正交变换后重新分布的特点进行信息隐藏，可较好解决不可感知性和稳健性的矛盾。

\*常用变换：离散傅里叶变换（DFT）、离散余弦变换（DCT）、离散小波变换（DWT）

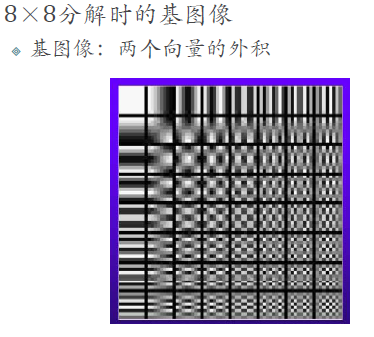
1. DCT

\*常用图像压缩标准，变换结果为实数

\*应用：JPEG、MPEG-2

\*过程：从载体中提取特征——>二维离散余弦变换——>选择适当系数嵌入水印——>二位离散余弦反变换

\*系数的选择：高频——不可见性更好、低频——鲁棒性更好、中频——平衡信噪比和鲁棒性



1. DWT

\*一种滤波运算，DWT转换后的域不仅有频域成分，还具有空域成分

\*特点：多分辨分析特点，能充分反映人类视觉特性

1. DFT

\*特点：变换结果为复数，有实部和虚部

\*幅值：

\*相位：

1. 变换域信息隐藏主要步骤

\*将宿主信号变换到频域空间

\*在变换域选择n个系数隐藏信息

\*根据规则修改选择的变换系数

\*反变换得到掩密载体

1. 优点

\*变换域中嵌入的信号能量可以比较均匀的分布到空域的所有像素上，有利于保证不可见性

\*变换域HVS（人眼视觉特性）和HAS（人类听觉系统）的某些特性能结合进去，有利于不可感知性和稳健性的提高

\*与国际数据压缩标准兼容，便于实现压缩域内信息隐藏算法

1. 缺点

\*计算量大、转换时可能造成信息丢失，不利于存储大量数据

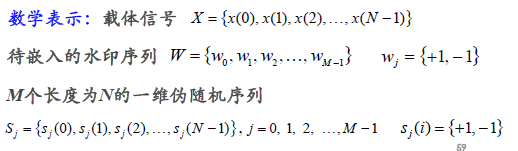
1. 基于扩频的信息隐藏技术

\*优点：具有很强的抗干扰性

\*基本概念：将水印分布在许多数据频域系数中，加入每个频域系数的信号能量很小，检测时将许多微弱的信号集中起来形成具有较高信噪比的输出值

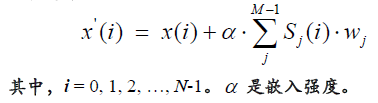
\*基本原理：基于扩频通信原理，扩频水印技术采用叠加伪随机序列的方式嵌入水印。具体地，在原始数据的空域或变换域上叠加经水印信息调制后的伪随机序列，检测时计算待检信号与伪随机序列之间的互相关系数，然后与阈值比较提取隐藏信息。

\*数学表式：

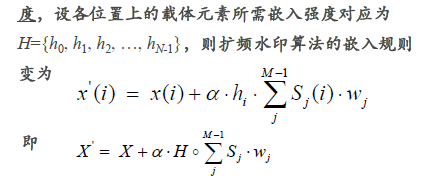




\*嵌入算法：在原始载体上以加性或乘性的方式叠加一个经水印信息调制后的扩频序列。因此，扩频水印方法的嵌入规则可统一地公式化描述为



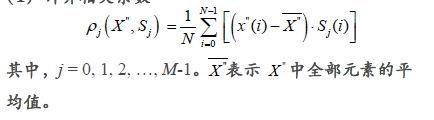
\*自适应嵌入算法：



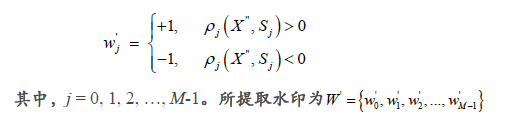
\*提取算法：基于相关性检测的水印判决方法，含水印载体在传输过程中可能受到干扰而失真，接收端收到的载体信号为：



1. 计算相关系数



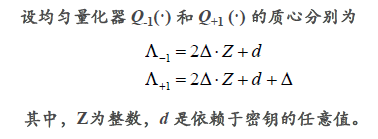
1. 利用阈值化方法判决水印信息



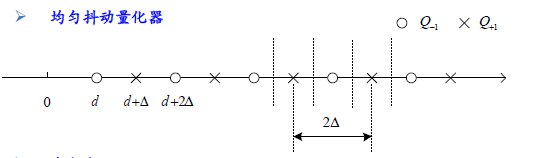
1. 统计比较原始水印和检出水印的对应元素，可得出水印检测算法的正检率和误检率（比特数所占比例）
2. QIM（二级量化索引调制）水印算法

\*基本原理：按照待嵌入的二进制水印比特 ，选择使用两个均匀量化器中的一个对载体信号x进行量化处理

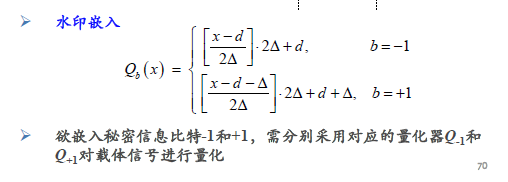
\*抖动（量化）调制：



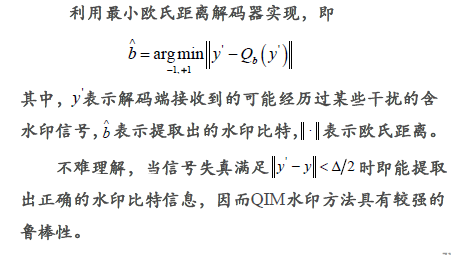
\*均匀抖动量化器



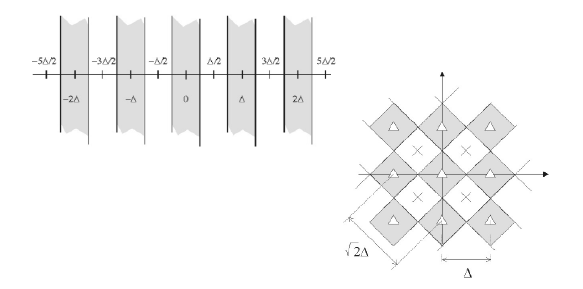
\*水印嵌入



\*水印提取



\*DM抖动调制（一维、二维...）



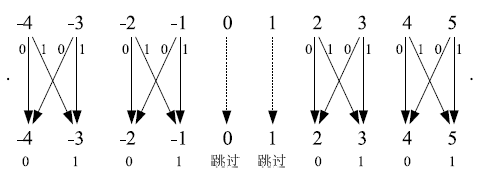
1. Jsteg、F3、F4、F5
2. Jsteg

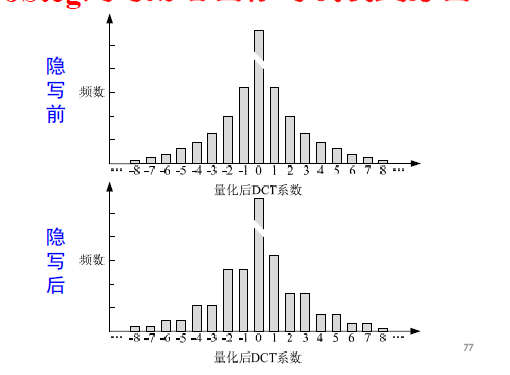
\*一种Jpeg图像隐写软件

\*方法：将LSB替换应用到JPEG图像中量化后**DCT系数**，绝对值为0或1的量化后DCT系数不嵌入任何信息（除了0和1以外，偶数加一，奇数减一）

\*缺点：不能抵抗卡方分析（和空域LSB替换隐写算法一样的安全缺陷 ）

\*JPEG图像量化后DCT系数直方图特性：绝对值越大的DCT系数出现的频数越低，对应直方图单元的值越小；随着DCT系数绝对值的增加，频数下降的幅度减小





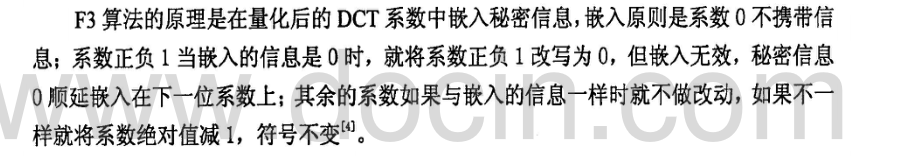
1. F3（改进JSteg算法）

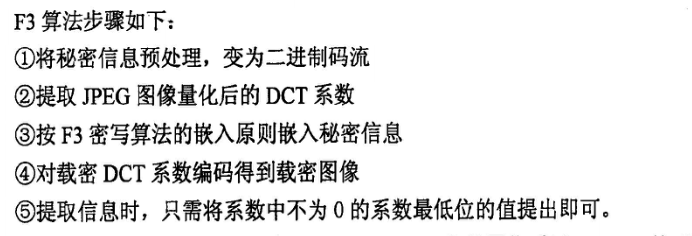
\*方法：信息嵌入时，若DCT系数的LSB与待嵌入秘密信息相同，不做改动；不同则将该**DCT系数绝对值**减1。值为0的量化DCT系数不嵌入任何信息

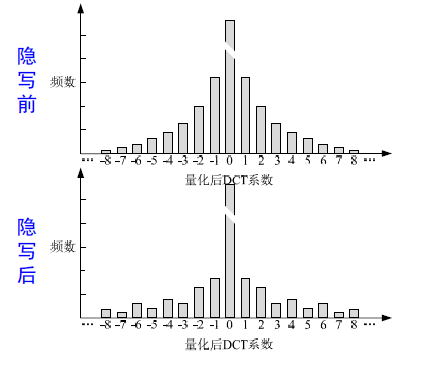
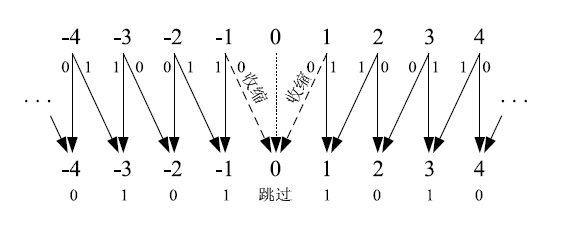
\*缺点：DCT系数直方图异常，偶数比奇数的bin高，因为F3密写由于嵌入无效导致隐藏了更多的信息0；0占比例大，嵌入量比较小；正负一都转换为0，导致密写后系数正负1大量减少（由于在值为+1、-1的量化后DCT系数上嵌入秘密信息比特0时，会形成无效的嵌入，继而将这些待嵌入的秘密信息比特0分摊到其它系数上，且最终由修改后为偶数的DCT系数来表征。）

\*优点：DCT系数直方图中不会出现值对趋于相等的现象，说明F3可以抵抗卡方分析

\*JPEG图像量化后DCT系数直方图特性：偶数值处单元高度



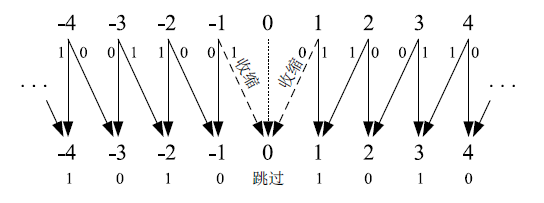


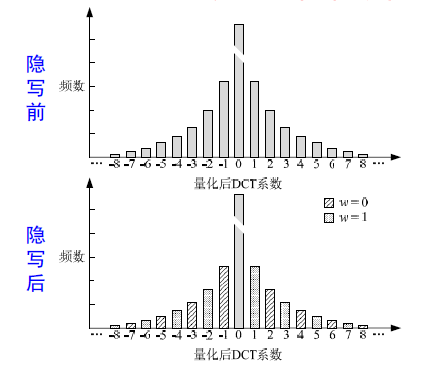


1. F4（改进F3算法）

\*方法：利用正奇系数和负偶系数代表1，正偶系数和负奇系数代表0；绝对值减一；值为0的量化DCT系数不嵌入任何信息

\*缺点：直方图特性得到保持（秘密信息0和1都重传，抵消单一的重传0造成的不足），但嵌入率较低

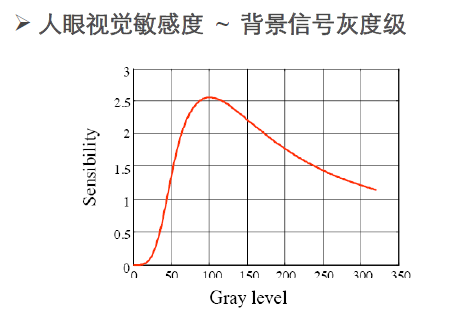




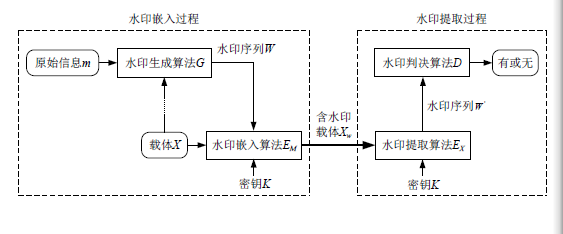
1. 基于HVS（人类视觉系统）的信息隐藏技术
2. 人的生理模型技术

\*包括：人类视觉系统HVS和人类听觉系统HAS

\*基本思想：利用从模型中导出的JND（Just Noticeable Difference）描述给定媒体的各个部分所能容忍的隐秘信号的最大强度，从而能避免破坏视觉（听觉）质量，这一方法同时具有好的透明性和稳健性。（自适应的控制水印嵌入强度）



1. 数字水印
2. 数字水印技术框架

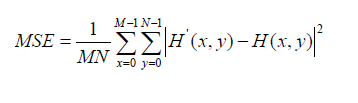


1. 分类
2. 按宿主信息：文本水印、图像水印、视频水印、矢量图水印
3. 按水印嵌入位置：空域数字水印和变换域数字水印
4. 按数字水印性质：鲁棒水印和脆弱水印

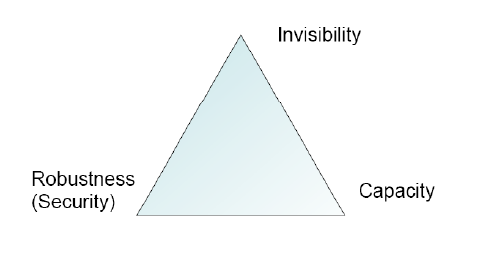
\*鲁棒水印：数字内容信息的版权保护和所有权认定，应能经受各种可能攻击；

\*脆弱水印可以进一步分为完全脆弱水印和半脆弱水印

1. 水印检测是否需要原始载体信息和水印信息：盲检测水印和非盲检测水印
2. 检测方法的角度：私有水印和公开水印
3. 水印载体能否无损灰度：可逆水印和不可逆水印
4. 评价指标
5. 安全性：水印信息应该是安全的，难以篡改或伪造
6. 不可见性：数字水印不可感知，应不影响被保护数据的正确使用。衡量隐蔽性的客观标准有均方误差MSE和信噪比SNR和峰值信噪比PSNR



1. 鲁棒性：指在经历过多种有意或无意的信号处理操作后，数字水印仍能保持部分完整性并能被准确鉴别。
2. 水印容量：嵌入的水印信息必须足以表示数字内容的创建者或所有者的标志信息，或购买者的序列号，有利于保护数字产权合法拥有者的权益



1. 攻击方法
2. 被动攻击：试图破解数字水印算法
3. 主动攻击：目的是篡改和破坏水印，使合法用户也不能读取水印信息

\*解释攻击及对策

1. 定义：在一些水印方案中，可能存在对检出的水印的多个解释，在解释攻击中，图像像素值或许被改变或许不改变，此类攻击要求对所攻击的特定水印算法进行深入彻底的分析
2. 对策：第一种方法是引入时戳机制，从而确定两个水印被嵌入的先后顺序;第二种方法是作者在注册水印序列的同时对原始作品加以注册，以便于增加对原始图像的检测;第三种方法是利用单向水印方案消除水印嵌入过程中的可逆性;第四种方法是利用双水印和盲检测技术，杜绝伪造原始图像的可能性。

\*信号处理攻击及对策

1. 定义：常见的信号处理攻击法包括无恶意的和常用的一些信号处理方法，我们对图像经常采取这些处理以适应不同的要求。信号处理攻击法也包括通过加上噪声而有意修改图像，以减弱图像水印的强度，我们用强度这一术语来衡量嵌入水印信号的幅度相对于嵌入的数据幅度，类似于通信技术中的调制系数这一概念。
2. 对策：在人类视觉特性决定的最大容许范围内，增加嵌入的力度;或者采用冗余嵌入技术。两种方法都会增加水印的强度，从而抵抗主动攻击。

\*分析攻击及对策

1. 定义：分析(计算)攻击法包括在水印的插入和检测阶段采用特殊方法来擦除或减弱图像中的水印。这类攻击往往是利用了特定的水印方案中的弱点，在许多例子中，它证明了分析研究已足够，不必在真实图像上测试这类攻击。共谋攻击(Collusionattack)或多重文档攻击(Multi-documentattack)就是这类攻击，共谋攻击用同一图像嵌入了不同水印后的不同版本组合而产生一个新的“嵌入水印”图像，从而减弱水印的强度。
2. 对策：采用了随机或伪随机的机制， 加强了水印对分析攻击的抵抗能力。

\*表达攻击及对策

1. 定义：不需要除去数字作品中嵌入的水印，它是通过操纵内容从而使水印检测器无法检测到水印的存在。实际上在表达攻击中并未改变任何图像像素值。
2. 对策： ①在嵌入水印的同时嵌入水印参照物。

②使用与图像相关的易损水印，当图像被分割时，易损水印能报告图像的失真情况。当易损水印不可被检测时，图像的质量也应降低到不可接受的程度。

③对嵌入水印的位置采用相对的位移地址，而不是采用绝对的存储位置。

1. 版权保护水印
2. 需满足的基本条件

\*隐藏于数字作品中且不可感知

\*可以被专用的数字电路识别

\*不必获取完整数据，仅从数据流中即可识别到数字水印

\*可以标记复制信息（“未曾复制”、“不能再复制”...）

\*漏检概率低

\*水印内容设计合理

\*必须使用成熟的技术嵌入或检测水印

1. 压缩域算法

\*基于Jpeg、Mpeg标准，节省了大量完全解码和重新编码过程

1. RST域算法

\*利用DFT、Fourier-Mellin变换，使经过旋转、缩放、平移后得到的图像在RST域保持一致

\*优点：具有很轻的抗几何变换能力

\*缺点：抵抗有损压缩、低通滤波等信号处理方法的稳健性不够

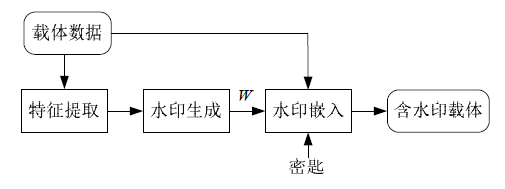
1. 内容认证水印
2. 基本原理

预先在原始载体中通过水印嵌入器隐藏某种认证信号，在需要验证时，通过水印检测器识别这些认证信号的变动，以鉴别待测待测载体数据的完整性和真实性。这里的水印信号可以是认为叠加的辅助信号或模板信号，也可以是依据载体内容或内容特征生成的校验信息

1. 数字水印认证系统：水印嵌入和水印检测

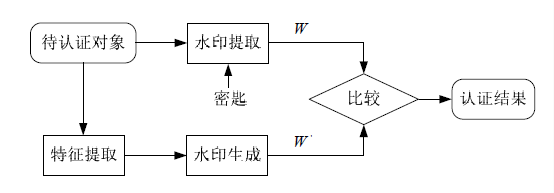
①认证水印嵌入

\*首先对原始载体进行特征提取，以此来构造水印信息，再将水印信息嵌入到原始载体中，得到嵌入水印后的受保护数字内容。



②认证水印检测

\*根据密钥提取出待检测水银细细，将提取出来的水印信息W和重新生成的水印信息W’相比较，若二者一致，则图像未被更改，不一致则认为图像被改动，给出改动详细信息。



1. 技术要求

\*敏感性：对改变语义的恶意操作敏感

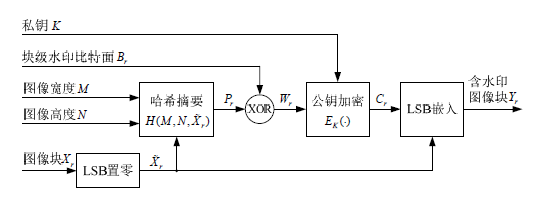
\*容忍性：能忍受普通的信息损失和非恶意操作

\*定位能力：系统能准确定位恶意篡改发生的具体位置

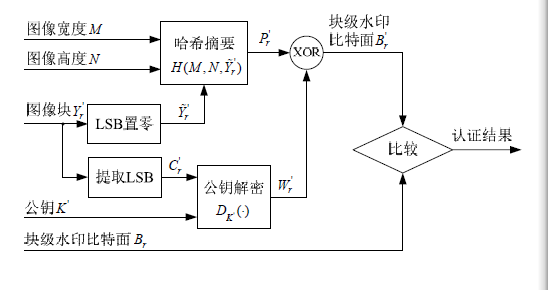
\*恢复能力：根据检测出的篡改区域进行恢复

1. Wong脆弱水印算法

\*水印嵌入流程



\*水印提取（运用了异或运算的特性）



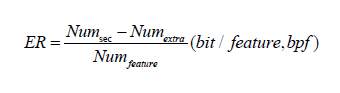
1. 可逆水印
2. 评价指标

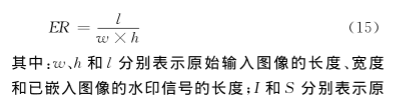
\*畸变程度：主观评价（人对嵌入秘密信息的载体的感觉）

客观评价（均方差和峰值信噪比）

\*嵌入率：嵌入量-嵌入到载体中的秘密信息比特数（实际嵌入量和有效嵌入量【实际可隐藏的嵌入量-附加信息的嵌入量】）

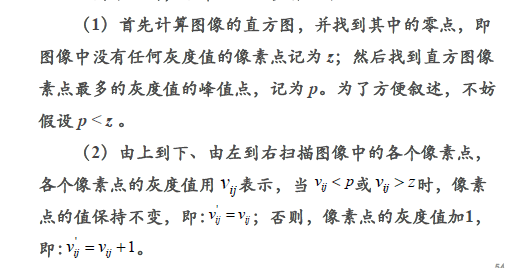
嵌入率（ER）-衡量有效嵌入量指标

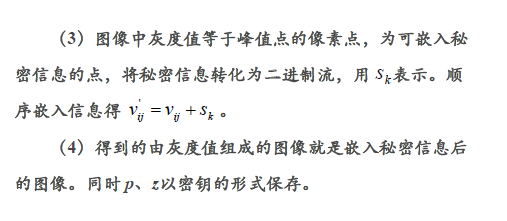




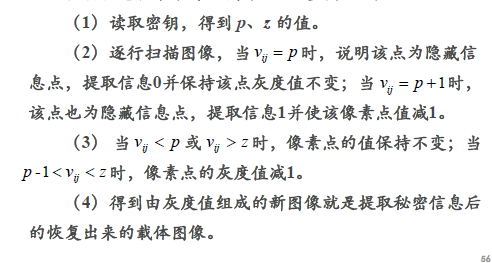
1. 基于直方图修改的可逆水印算法

①水印嵌入





②水印提取及原始载体恢复



③优点：产生较少的畸变，具有较高的峰值信噪比

直接在空域应用不会产生数据溢出问题

对于某些含大量相同背景的图像具有较高嵌入率

④缺点：嵌入率不稳定，一般图像嵌入率低

⑤改进：选择无穷远处为其差值直方图零值点

可选择两个或多个峰值进行可逆信息隐藏

进行多层隐藏

1. 信息隐藏的应用与发展
2. 数字知识产权保护（鲁棒水印）
3. 数据完整性鉴定、内容认证（脆弱、半脆弱）
4. 数据保密
5. 资料不可抵赖性的确认

五、思考题

1、信息隐藏与数字水印的区别与联系。

2、例举常见的信息隐藏技术。

3、简单描述数字水印的组成框架。

4、数字水印有哪些攻击，分别有何应对策略。

5、简述各典型数字水印算法的基本原理与、主要步骤、优缺点以及改进方法。

1. 数字取证技术
2. 基本概念

1、定义：数字取证是指为了揭示与数字产品相关的犯罪或过失行为，利用一切科学合法的方法和工具，对以二进制表示的数据进行识别、保存、收集、检查、分析和呈堂等活动过程。

2、特点：较高的精密性和脆弱性、较强的隐蔽性、多媒体性、收集迅速、易于保存、占用空间少、容量大

3、过程模型



二、数字取证分类

1、数字取证技术分类

①电子取证：恢复已被破坏的电子数据及提供相关的电子资料证据（究除计算机和网络以外的电子产品中）

②计算机取证：对文件的复制、被删除文件的恢复、缓冲区内容获取、系统日志分析

③网络取证：网络流的相关性、数据的完整性和包捕获的速率是网络取证分析内容。

2、证据取证分析技术分类

①基于取证过程模型的分析技术：：识别类、保存类、收集类、检查类、分析类以及出示类。

②基于数字设备运行历史模型的~：根据事件和状态的序列集合进行分析

③基于存储介质的取证分析方法：围绕存储介质中证据的获取、保护、传输以及分析等进行取证调查（基于永久性存储介质的取证分析和基于易失性内容取证分析方法）

三、数字内容篡改取证

1、数字图像篡改手段

\*图像合成、图像增强、图像润饰、图像修复、图像变形、计算机生成图形、JPEG重压缩、二次获取、图像拼接

\*数字照片图像的功能：客观记录真实场景及历史事件，传递可信信息；应用于司法取证、新闻纪实等

\*图像/音视频认证：鉴别图像数据的原始性、验证图像内容的真实性、完整性，图像来源认证

\*研究图像认证技术的意义：网络内容安全（可靠分享，保证图像信息的可信性和安全性）、司法与刑侦系统

\*主动认证技术：

1. 数字水印：隐藏认证信息（篡改检测与定位-（半）脆弱水印、恢复原始载体-可逆水印）
2. 数字签名：附加签名信息
3. 缺陷：实际图像未携带认证信息，需预处理，应用受阻

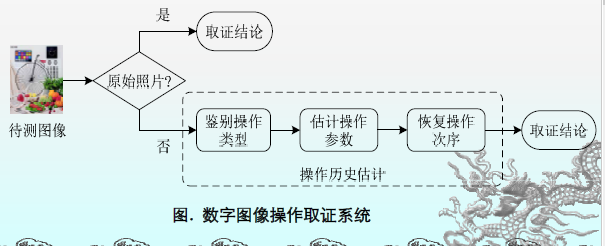


\*被动认证技术-数字取证

1. 图像篡改取证：操作检测、类型鉴别、参数估计、理事会副
2. 基本原理：原始图像内在特征存在严格的一致性和独特性，可作为图像(源)的固有“指纹”；任何操作都会在一定程度上破坏其原始性与完整性，不同类型操作会在图像上遗留不同的操作痕迹

\*数字图像取证（图像被动认证）

1. 目的：通过被动的盲分析手段识别图像来源和真伪，检测图像所经历的篡改操作，以及估计图像处理历史
2. 特点：仅以图像数据本身为分析对象，不需要对图像进行额外的预处理
3. 分类：数字图像操作取证、数字图像来源取证



\*图像操作分类

1. 内容篡改型：改变图像内容、结构、语义（图像拼接、图像合成、复制粘贴..）
2. 内容保持型：影响图像视觉质量（滤波、重采样、压缩...）

\*\*研究内容保持型操作取证的意义

• 鉴别数字照片图像的原始性

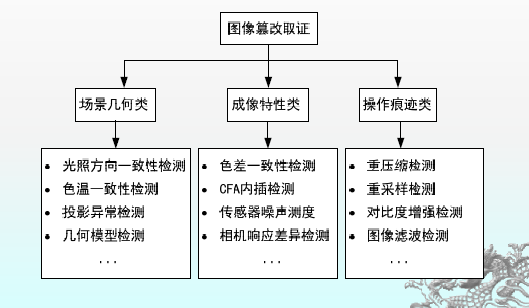
• 估计图像处理历史

• 检测涉及局部操作的拼接图像

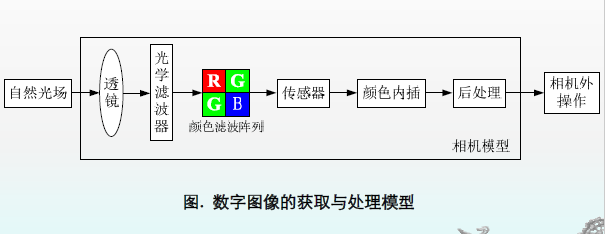
• 鉴别具体操作类型及参数，给出更精细的取证信息

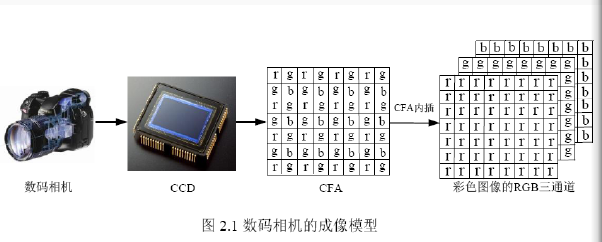
• 图像逆工程

\*图像篡改取证技术分类



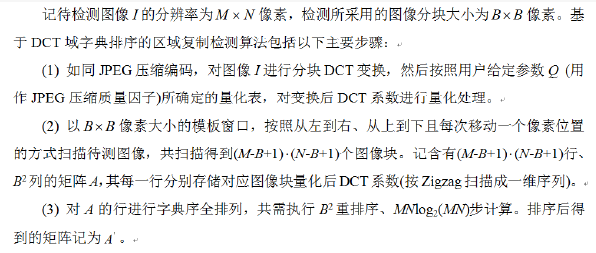
成像设备特性：

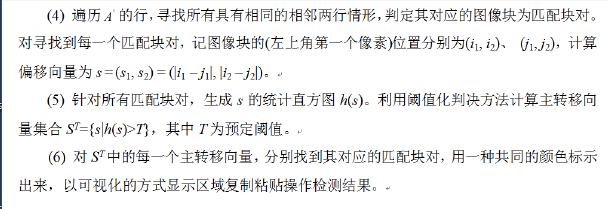




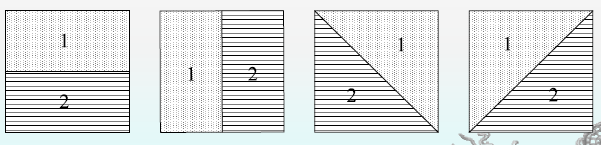
\*图像复制粘贴型篡改检测

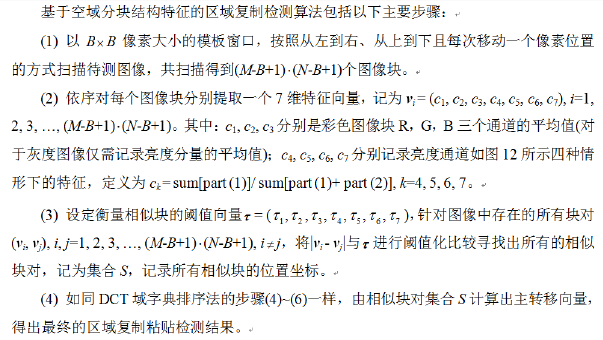
1. DCT域字典排序法





（2）空域分块结构特征法





\*数字内容取证评价标准

1. 准确度（P）



1. 完整度（R）



2、数字音频篡改手段

删除、剪接、插入、音频合成、修饰局部音频片段（滤波...）

3、数字视频篡改手段

① 帧复制或插入、删除操作，即视频合成操作

② 模糊润饰操作，消除局部因拼接造成的篡改痕迹

③ MPEG二次压缩操作

\*视频篡改取证方法

1. 单帧分析法
2. 基于帧间内在关联特性分析

四、数字内容来源取证

1、对数字内容生成设备/方式的盲鉴别，包括对设备类型、型号等具体参数的识别

2、数字图像来源：数码相机、计算机图形、扫描仪（扫描仪主要由光学成像部分、机械传动部分和转换电路部分组成，这几部分相互配合，将反映图像特征的光信号转换为计算机可接受的电信号。）

\*数字录音机：音频数字化通常需要经过三个阶段，即采样—量化—编码。数码录音笔通过对模拟信号的采样、编码将模拟信号通过数模转换器转换为数字信号，并进行一定的压缩进行存储。

3、设备来源：类型、品牌、型号、个体

4、来源取证评价标准

（1）检测率【TP】：数字内容所对应的来源被正确识别的比率

TP=真确识别的内容数目/所有数字内容样本

（2）漏检率：1-检出率

1. 虚警率【FP】：来源被错误识别的比率

FP=错误识别数/所有数字内容样本

1. 错误否定率：1-虚警率
2. ROC曲线：描述TP和FP之间的关系（ROC曲线的AUC可表征分类器的性能。AUC越接近1，表示分类效果越好；AUC越接近于0.5，说明分类性能越差。）
3. 数字图像来源取证
4. 基于图像统计特征
5. 基于成像通道特性：任何成像传感器都有其固有的模式噪声，一般不易消除，故可当做内部水印使用。由于装有单片CCD或CMOS的相机只能通过颜色插值才能获得彩色图像，而不同厂家甚至不同型号的相机使用不同的插值算法，只要能从测试图像中估计出插值周期，就可推算出所采用的插值算法，从而追溯出源相机。
6. 数字视频来源取证
7. 基于摄像设备内在特性
8. 利用视频码流特征
9. 思考题
10. 什么是数字取证
11. 数字取证分哪几类
12. 常用的数字图像篡改手段
13. 现有的数字图像篡改取证技术有哪几类？

5、数字内容来源取证的含义是什么？

6、简述数字图像来源取证的原理与方法。

\*\*期末复习

1. 基本概念
2. 信息隐藏
3. 隐写术
4. 阈下信道
5. （空域/频域）数字水印
6. （半）脆弱水印
7. 载体图像
8. 鲁棒性
9. 水印容量
10. 不可感知性（透明性、隐蔽性）
11. 安全性
12. PSNR
13. 可逆水印
14. 软件水印
15. 数字取证
16. 图像合成
17. 图像增强
18. 图像润饰
19. 计算机生成
20. JPEG重压缩（或称JPEG二次压缩）
21. MPEG重压缩（或称MPEG二次压缩）
22. 二次获取
23. 数字图像（内容）来源
24. 数字图像（内容）来源取证

二、信息隐藏

1、技术分类与评价指标（要求计算容量、PSNR等）

2、基本原理与模型

3、应用

4、空域信息隐藏算法：LSB系列，Patchwork

5、变换域信息隐藏算法：JSteg系列（含F3、F4），(DCT域)扩频水印，QIM

（重点考查对算法原理/步骤、算法优缺点及改进措施等方面的理解与思考）

三、数字水印

1、分类与评价指标、攻击方法、应用

2、内容认证数字水印（脆弱、半脆弱水印方法）：基本原理、流程图

3、版权保护数字水印（鲁棒水印）：概念、基本原理与方法

4、可逆水印：基于直方图修改的图像可逆水印算法

四、数字内容篡改取证

1、图像/音频/视频的篡改手段

2、典型篡改取证方法的分类及原理

3、篡改取证方法的评价指标

五、数字内容来源取证

1、图像/音频/视频来源：数码相机/摄像机/扫描仪/录音机/CG绘制等

(数字媒体生成原理)

2、典型数字内容来源取证方法的分类及原理

3、源取证方法的评价指标

六、隐写分析

1、了解“隐写分析”概念及系统模型（P124，5.5.1节）

2、理解隐写分析与隐写之间关系