《数字内容安全》

课程讲义

第4章 信息隐藏与数字水印

主要内容

1. 信息隐藏基本概念
2. 空域/变换域信息隐藏技术
3. 数字水印
4. 应用与发展

学习目标

- 理解信息隐藏与数字水印相关的基本概念
- 掌握空域和变换域的信息隐藏技术
- 掌握版权保护和内容认证数字水印技术

术语表（中英文）

- Information Hiding， 信息隐藏
- Digital Watermarking，数字水印
- Steganography，隐写(术)
- Steganalysis，隐写分析
- Robust(ness) 鲁棒(性)
- (Semi-)Fragile (半)脆弱
- Authentication 认证
- Cryptography 密码术
- Payload 有效载荷 Capacity 容量
- Transparency 透明性

术语表（中英文）

- Cover 载体
- Distortion 失真

主要内容

1. 信息隐藏基本概念
2. 空域/变换域信息隐藏技术
3. 数字水印
4. 应用与发展

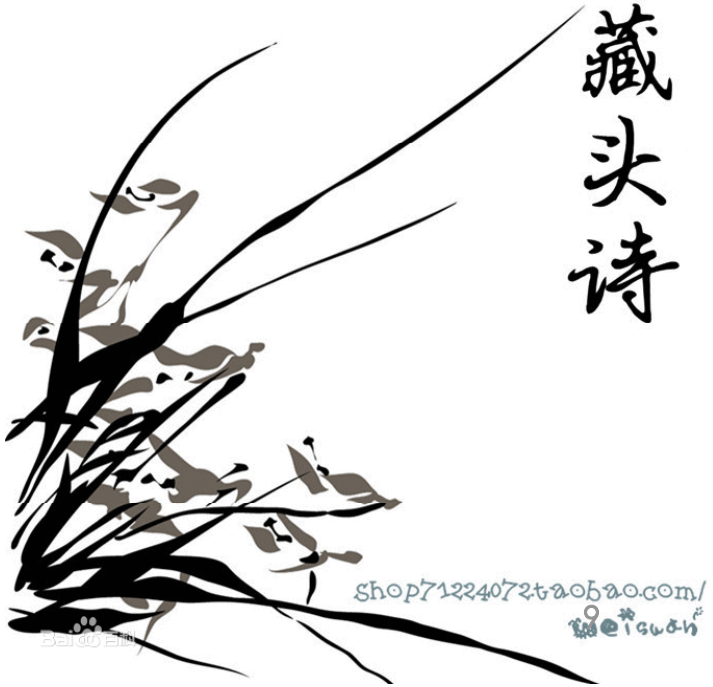
1 信息隐藏基本概念

- 1.1 技术背景（示例、动机）
- 1.2 相关概念
- 1.3 信息隐藏原理
- 1.4 技术分类
- 1.5 技术要求 / 评价指标

§1.1 技术背景

- 远古时代的隐写术
  - (1) 用头发掩盖信息
  - (2) 使用记书板隐藏信息
  - (3) 使用音乐谱隐藏信息
  - (4) 使用离合诗隐藏信息
  - (5) 使用微小图隐藏信息

芦花丛中一扁舟，
俊杰俄从此地游。
义士若能知此理，
反躬难逃可无忧。



Example 1： Text Steganography

"My friend Bob: Until yesterday I was using binoculars for stargazing. Today I decided to try my new telescope. The galaxies in Leo and Ursa Major were unbelievable! Next, I plan to check out some nebulas and then prepare to take a few snapshots of the new comet. Although I am satisfied with the telescope, I think I need to purchase light pollution filters to block the xenon lights from a nearby highway to improve the quality of my pictures. Cheers, Alice."

Take initial letters:
mfbuyiwubfstidttmnttgilaumwuniptcosnatpttafsotncaiaswttitintplpftbtxlfanhtitqompca

Filter with π = 3.141592653689793…-> buubdlupnpsspx

Take the preceeding letter in the alphabet: ATTACK TOMORROW

Example 2： Robust Image Watermarking

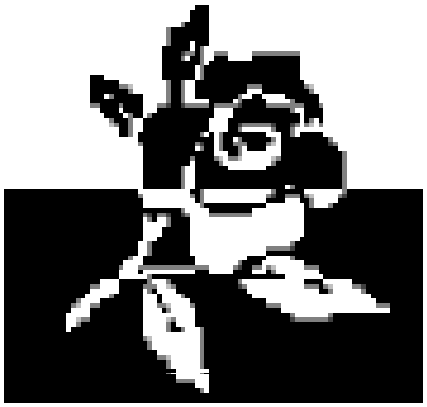
(a)
Original Lena

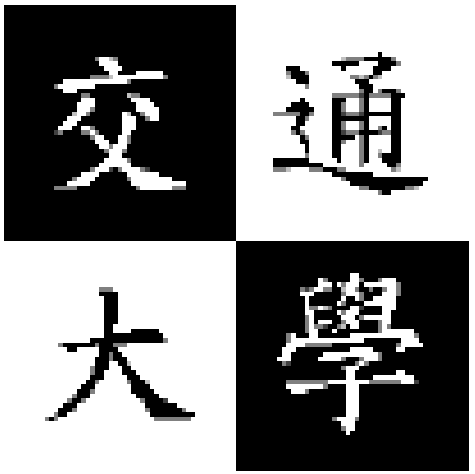
(b)
VQ compressed Lena, 31.53 dB

Fig. 2. The test image and VQ compressed one.

Cited from ‘VQ-Based Watermarking Techniques’

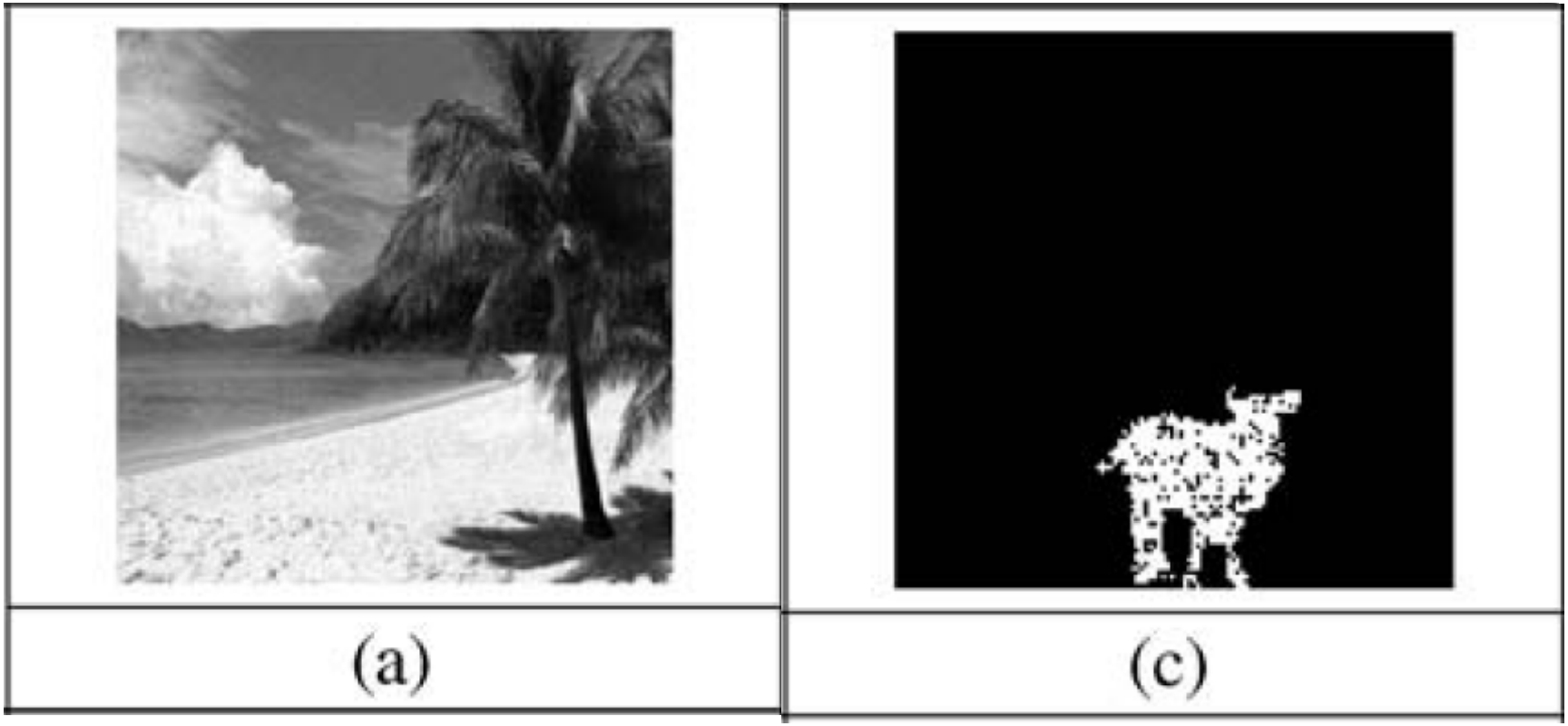
Example 2： Robust Image Watermarking (Cont)





Cited from ‘VQ-Based Watermarking Techniques’

Example 3： Fragile Watermarking for Image Authentication



Cited from ‘A hierarchical digital watermarking method for image tamper detection and recovery’, PR 2005

Example 4: 图像局部隐藏

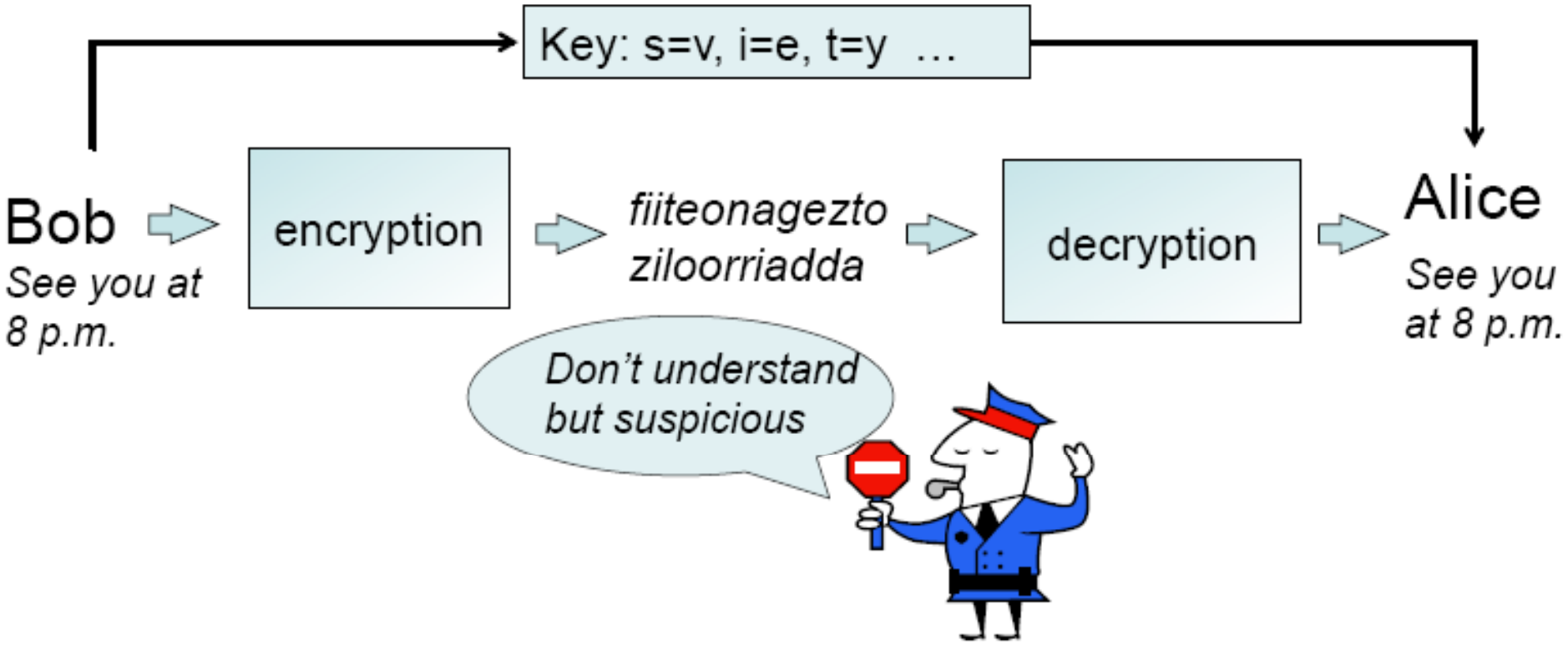
（特定目标消隐及图像修复技术）

局部图像恢复

局部图像隐藏

➢ 技术动机

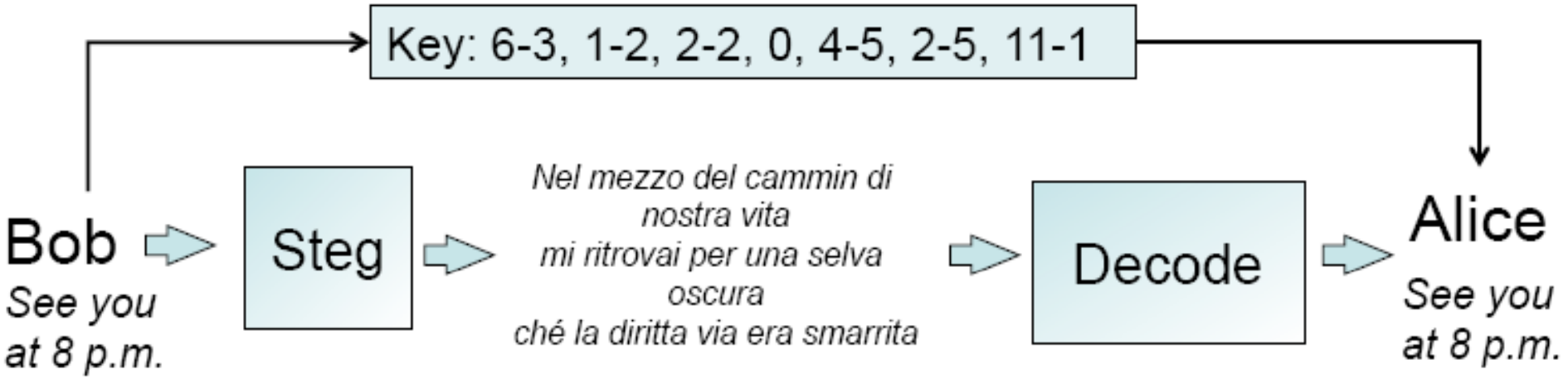
Cryptography



In some cases the very existence of a message is enough to raise a suspect

➢ 技术动机

Steganography



Steganography hides the very presence of the message into an innocuous host

➢ 技术动机

- 利用载体传递/携带某种信息
  - * 秘密信息
  - * 版权信息
  - * 认证信息
  - * 其它信息，如附加/辅助信息等
- 不影响载体的正常使用（不被察觉）

1.1 信息隐藏技术产生背景

- 问题：多媒体作品侵权、篡改日益严重；
- 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 信息隐藏基本概念

- 1.1 技术背景（示例、动机）
- 1.2 相关概念
- 1.3 信息隐藏原理
- 1.4 技术分类
- 1.5 技术要求 / 评价指标

1.2 相关概念

- 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。

信息隐藏相关术语

- **原始载体**：专指待嵌入秘密信息的原始载体数据。
- **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。
- **掩密载体**：也称含密载体，专指嵌入秘密信息后的载体数据。
- **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。

1.2 相关概念

- 信息隐藏的可行性

（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。

信息隐藏与传统密码学的区别

- 密码学：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。

- 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。

信息隐藏与传统密码学的区别

- 加密通信：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；

- 信息隐藏：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。

1　信息隐藏基本概念

- 1.1　技术背景（示例、动机）
- 1.2　相关概念
- 1.3　信息隐藏原理
- 1.4　技术分类
- 1.5　技术要求 / 评价指标

1.3 信息隐藏原理

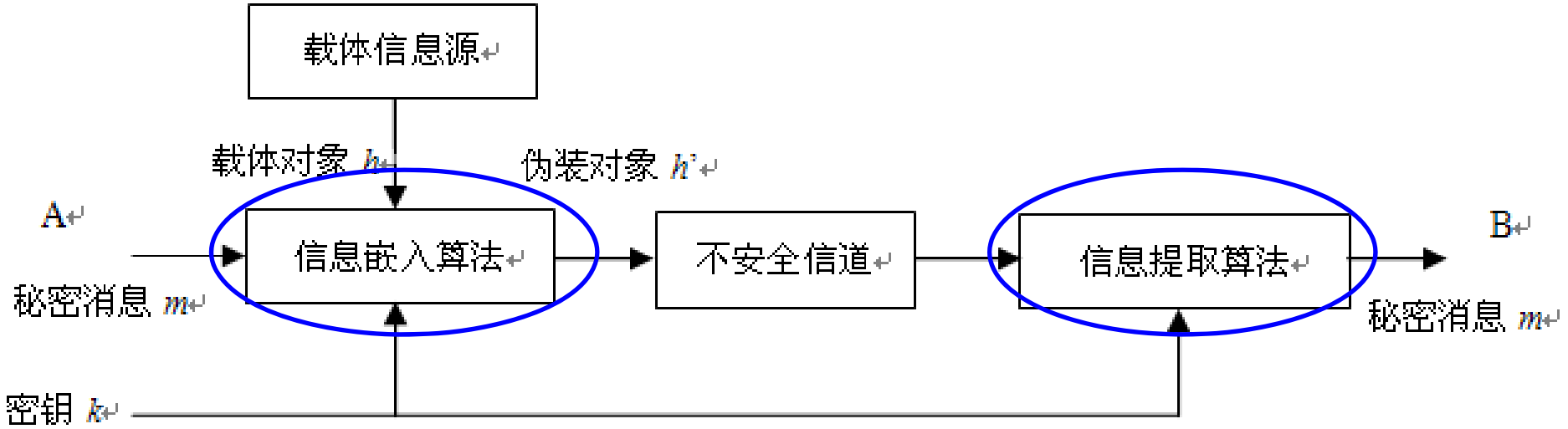
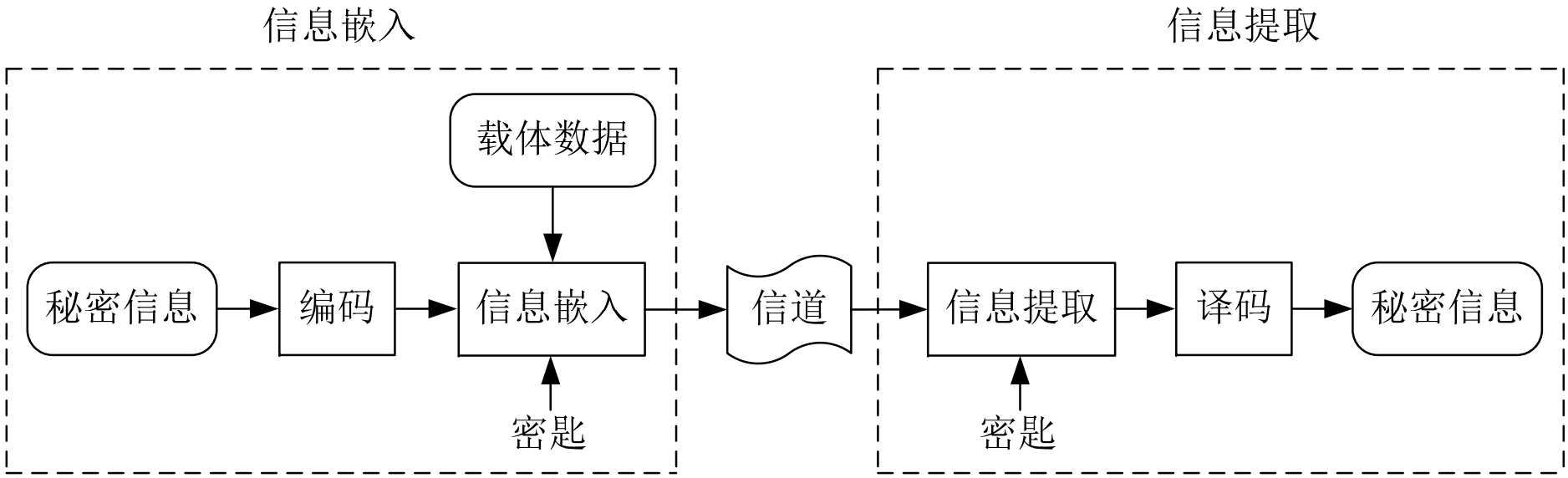


图 4-1 信息隐藏原理框图

基于通信的信息隐藏模型



- 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。
- **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
- **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**。

1.3 信息隐藏原理

- 从信号处理的角度来理解，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受到一定的限制，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。

1.3 信息隐藏原理

- 设 H 和 H' 分别表示原始载体信号和隐藏信息后的含秘载体信号，W 为待隐藏信息，信息隐藏的过程可表示为：

$$H' = H + f(H, W) \qquad (4\text{-}1)$$

1.3 信息隐藏原理

- **I. J. Cox** 提出了三种常用的信息嵌入公式，分别为：

$$h_i' = h_i + \alpha w_i \qquad (4-2)$$

$$h_i' = h_i(1 + \alpha w_i) \qquad (4-3)$$

$$h_i' = h_i + \alpha |h_i| w_i \qquad (4-4)$$

其中 h_i 和 h_i' 分别表示原始载体信号和隐藏信息后的掩密载体信号（或从中提取的特征值），w_i 为待嵌入隐藏信号分量，α 为嵌入强度。

1.3 信息隐藏原理

假设用 H^* 表示待测的掩密信号，从中提取的水印序列用 W^* 表示，$W^*=\{w_i^*\}$ 在相对于 H' 没有误差的情况下，隐藏信息可由式（4-2）和式（4-3）提取：

$$w_i^*=(h_i^*-h_i)/\alpha \qquad w_i^*=(h_i^*-h_i)/\alpha\cdot h_i$$

水印检测通常需要三个步骤：

（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）；

（3）判断水印是否存在。

1.3 信息隐藏原理

为了确定是否含有水印，可以通过下式计算相似度：

$$\rho(W^*,W)=\sum_{i=0}^{K-1}w_i^*w_i \Big/ \sqrt{\sum_{i=0}^{K-1}(w_i^*)^2} \qquad (4\text{-}5)$$

水印存在与否的判定标准为：若 $\rho(W^*,W)>T$,可以判定被测掩密信号中有水印存在；否则没有。T 为阈值。

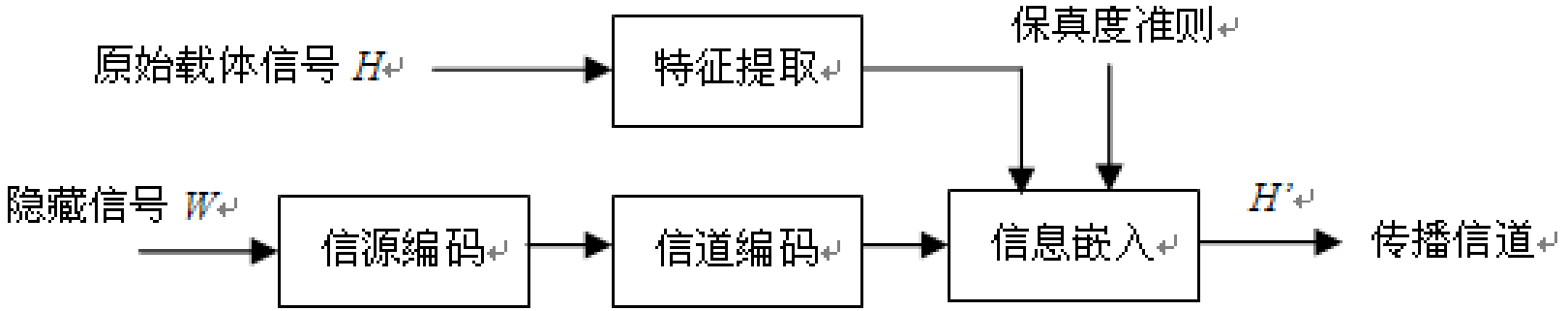
1.3 信息隐藏原理

- 信息隐藏技术模型：扩频通信模型

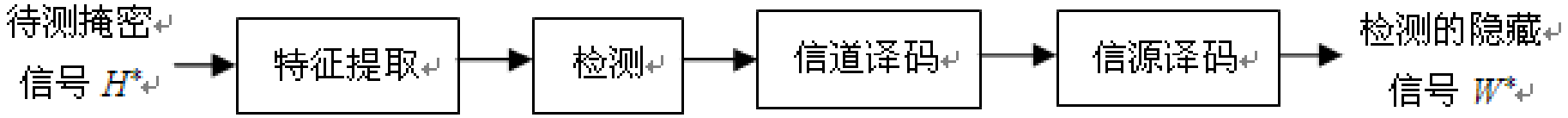
从数字通信的理论出发，信息隐藏可理解为在一个宽带信道（原始载体信息）上采用扩频通信技术传输一个窄带信号（隐藏信息）。由于隐藏信号的能量较低，它分布到信道中任意特征上的能量是难以检测到的；隐藏信息的检测则可理解为在一个含噪声信道中的弱信号检测问题。

1.3 信息隐藏原理

- 信息隐藏技术模型：扩频通信模型



（a）信息隐藏



（b）信息提取

1 信息隐藏基本概念

- 1.1 技术背景（示例、动机）
- 1.2 相关概念
- 1.3 信息隐藏原理
- 1.4 技术分类
- 1.5 技术要求 / 评价指标

1.4 信息隐藏技术分类

- 根据信息隐藏技术的应用目的和应用场合不同，信息隐藏可分为许多分支。

  （1）隐写术

  （2）数字水印

  （3）隐蔽信道

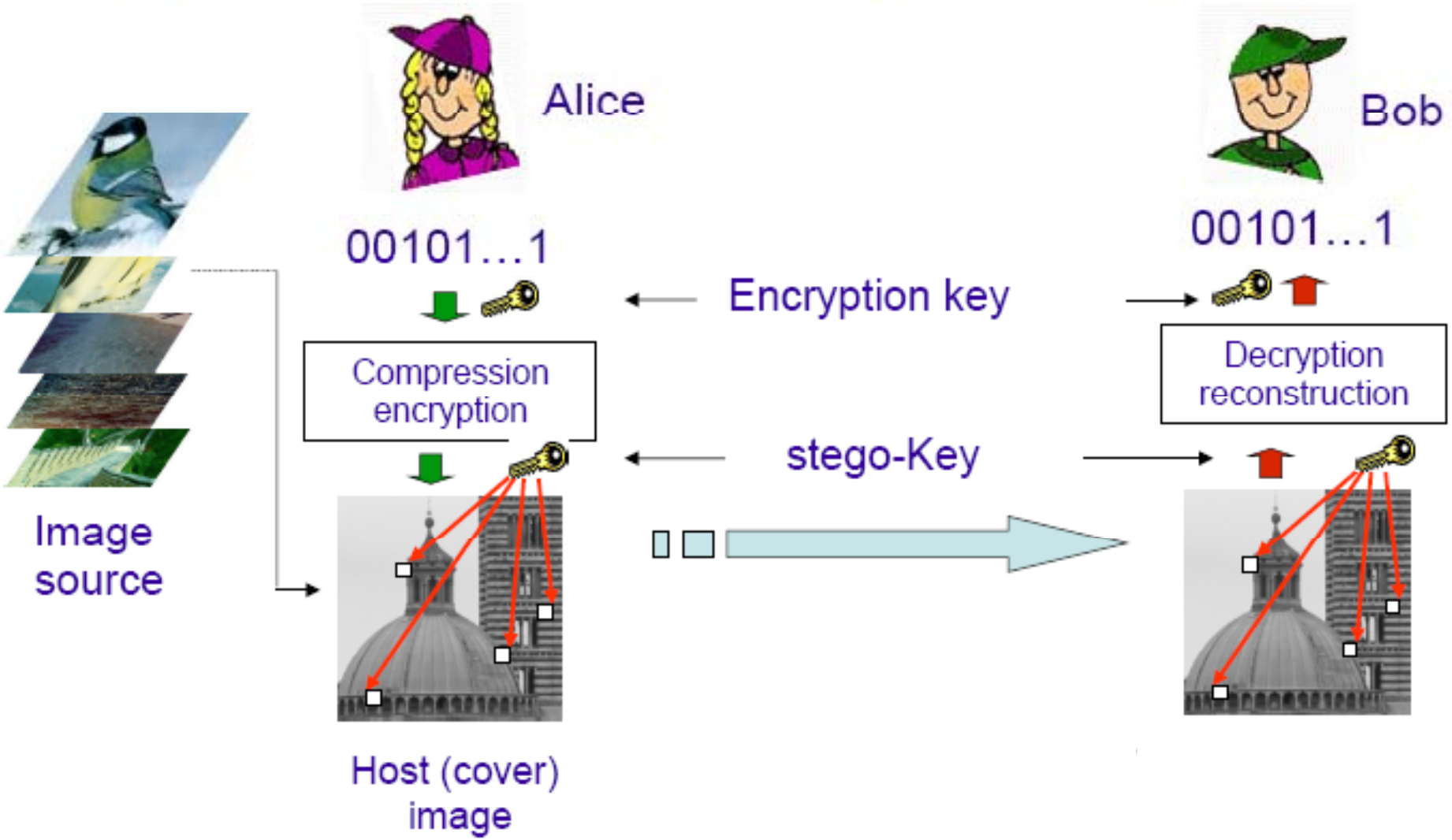
  （4）阈下信道

隐写术

- 隐写术是一种隐蔽通信技术，其主要目的是将重要的信息隐藏起来，以便不引起人注意地进行传输和存储。隐写术包括语义隐写和技术隐写。

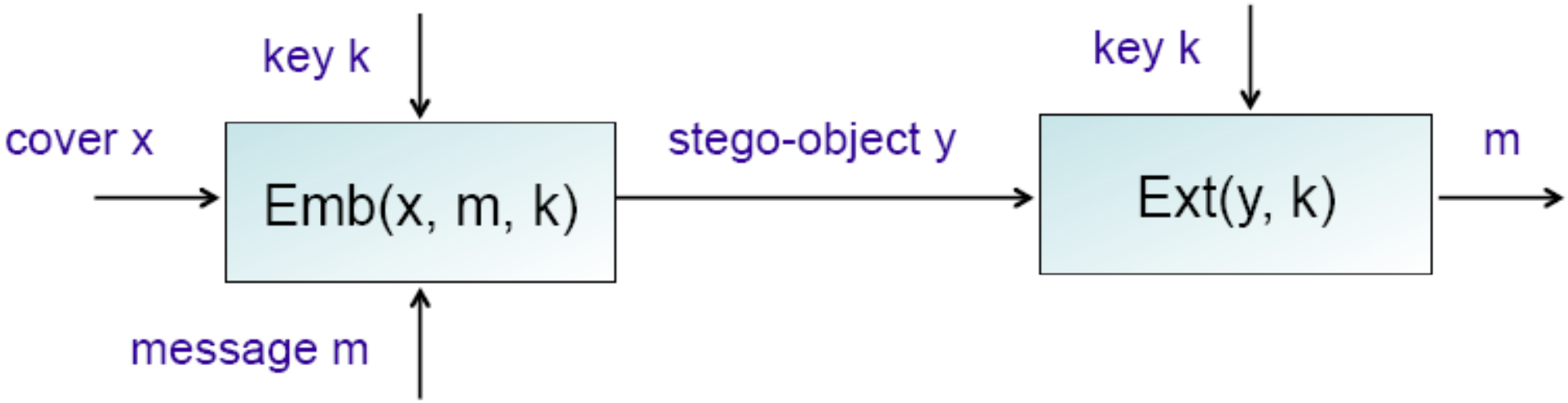
- 核心的技术要求：（统计意义上的）不可见性/隐蔽性，即不可检 测性；掩盖“信息隐藏”行为或事实。

A rigorous framework: the prisoner problem



Steganography by cover modification

- By far the most common approach
- It allows large payloads, however security must be studied carefully



- Payload = $\log_2(|m|)$ / sizeof(x); Distortion = d(x,y) = $\sum_{i=1}^{n}\left(x(i) - y(i)\right)^2$

数字水印

透明性

容量

鲁棒性

数字水印技术是信息隐藏技术的另一重要分支，通过在原始数据中嵌入秘密信息——水印来证实数据所有权或鉴别数据的真实性。被嵌入的水印可以是一段文字、标识、序列号等，通常是不可见或不可察的，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。

隐蔽通信

- 隐蔽信道是指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。
- 隐蔽信道分析工作包括：
  - ✓ 信道识别是对系统的静态分析，强调对设计和代码进行分析发现所有潜在的隐蔽信道。
  - ✓ 信道度量是对信道传输能力和威胁程度的评价。
  - ✓ 信道处置措施包括信道消除、限制和审计。

阈下信道

阈下信道是指在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。

1.4 信息隐藏技术分类

- 根据应用场合的不同要求，信息隐藏技术可以分为隐写术和数字水印两个主要分支。前者重点研究如何实现信息的伪装的隐蔽性；后者重点考虑水印信息的稳健性（即鲁棒性），如对各种可能攻击的敏感性等。

- 根据隐藏协议，信息隐藏还可分为无密钥信息隐藏、私钥信息隐藏、公钥信息隐藏。

1.4 信息隐藏技术分类

- 根据载体类型的不同，信息隐藏可分为：

文本信息隐藏、图像信息隐藏、音频信息隐藏、视频信息隐藏、用于二维矢量图的图形信息隐藏、用于三维网格模型的网格信息隐藏、软件信息隐藏，以及数据库信息隐藏等。

- 根据秘密信息隐藏位置的不同，信息隐藏可以分为空域信息隐藏和频域信息隐藏。

信息隐藏技术的应用

- 版权保护 （via 鲁棒水印）
- 内容认证 （via 脆弱水印）
- 隐密通信 （via 隐写）
- 数字指纹：也称叛逆者跟踪、操作跟踪或事务追踪。
- 广播监控：通过识别预先嵌入的水印来监控作品实际播放的时间、时长和地点等相关广播信息。
- 设备控制：也称拷贝控制。通过水印信号控制作品读取设备或播放设备的运行和某些功能。
- 标注：在载体作品中嵌入其它诸如标注、解释或辅助类信息，以提高作品在流通和应用环节的附加值。

1 信息隐藏基本概念

- 1.1 技术背景（示例、动机）
- 1.2 相关概念
- 1.3 信息隐藏原理
- 1.4 技术分类
- 1.5 技术要求 / 评价指标

1.5 信息隐藏技术要求

1）隐写术：隐写术的要求包括不可感知性和不可检测性、秘密性、较大的水印容量以及算法实现简单。

2）鲁棒水印：鲁棒水印最重要的要求包括不可感知性、鲁棒性、抵抗恶意攻击能力（安全性）、秘密性以及算法实现简单等。

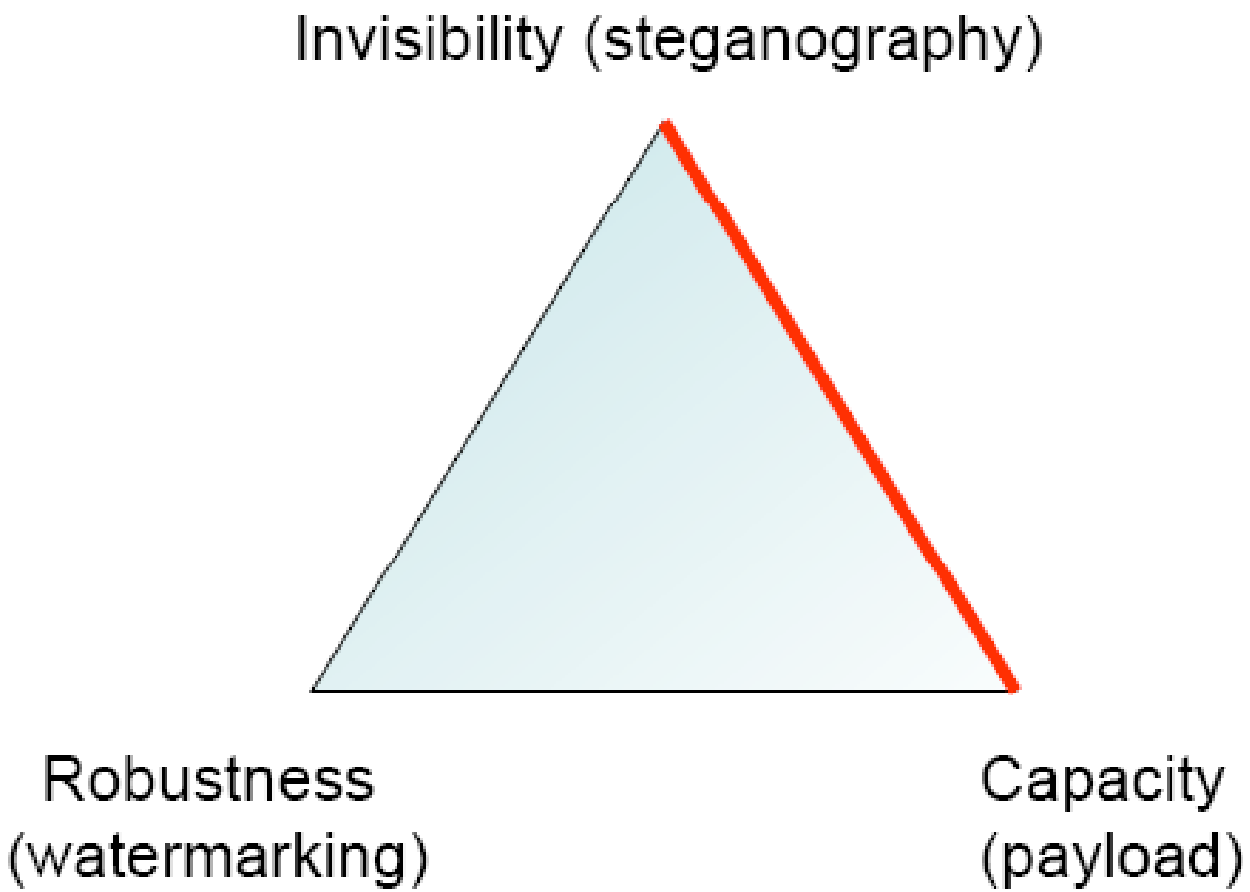
1.5 信息隐藏技术要求

3）完全脆弱水印：最重要的要求包括不可感性、对任何处理的敏感性、秘密性以及算法实现简单等。

4）半脆弱水印：最重要的要求包括不可感性、对恶意攻击（内容改变型操作）的敏感性、对合法处理（内容保持型操作）的鲁棒性、秘密性以及算法实现简单等。

Opposite requirements

In all data hiding applications (not only steganography) designers must face with 3 opposite requirements



➢ 信息隐藏技术（评价）指标

（1）**透明性**：信息隐藏行为应是不可感知的，且应不影响被保护数据的正常使用 。

（2）**鲁棒性（脆弱性）**：指在经历多种有意或无意的信号处理操作后，仍能完整或部分提取所隐藏秘密信息的能力。

（3）**容量**： 载体中所隐藏秘密信息的数量。如：bit/pixel， bit/non-zero coefficient

透明性：视觉质量失真度量

- **Peak Signal-to-Noise Ratio (PSNR), 峰值信噪比**，定义为：

$$PSNR = 10 \cdot \log_{10}\left(\frac{MAX_I^2}{MSE}\right)$$

其中，

$$MSE = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1} \| I(i,j) - K(i,j) \|^2$$

MAX_I为最大像素值，**8 bit**灰度图像其为**255**；

K为失真后图像，**(*m*, *n*)**为图像尺寸(分辨率)。

透明性 → 统计不可检测（隐写）

Cover image

LSB of the green channel (original)

LSB of the green channel (stego-image)

下一讲

1. 信息隐藏基本概念
2. 空域/变换域信息隐藏技术
3. 数字水印
4. 应用与发展