第三章 数字隐写技术

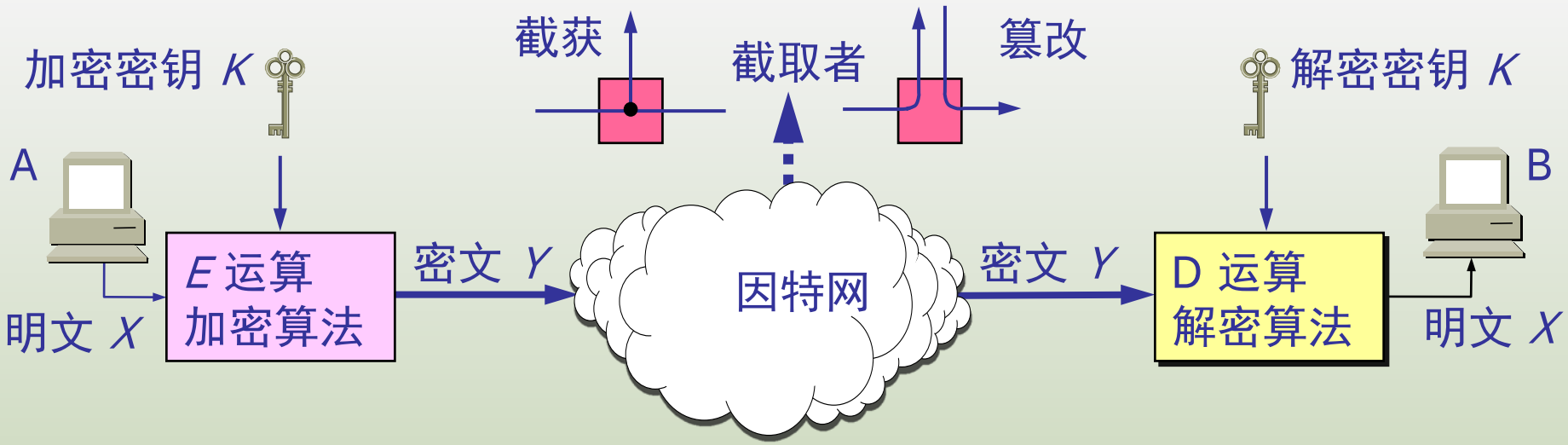
周满
15271802577
zhouman@hust.edu.cn
华中科技大学网络空间安全学院

数字隐写概述

- 一、信息隐藏及其历史
- 二、现代信息隐藏
- 三、信息隐藏技术原理
- 四、数字水印

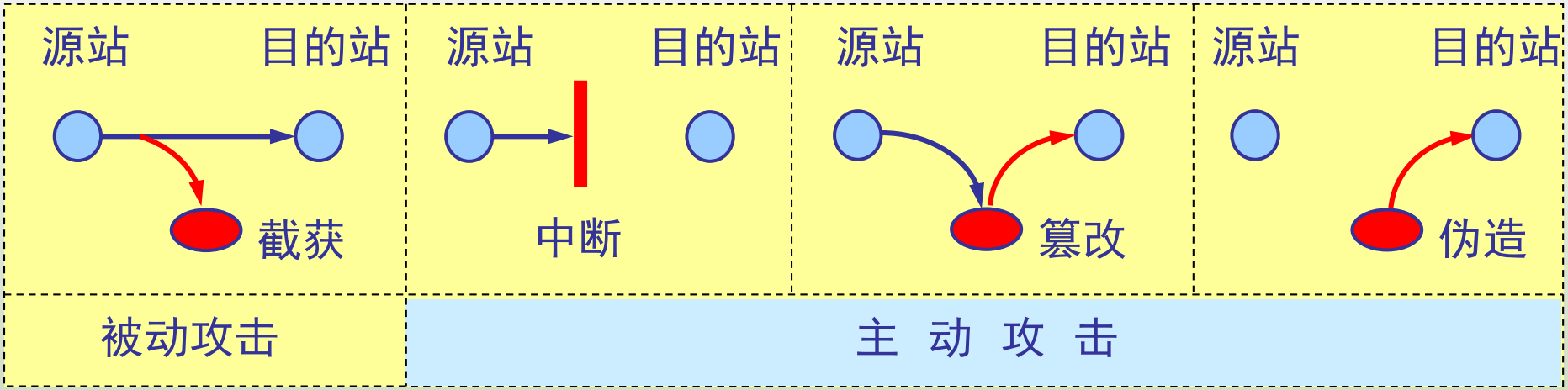
保密通信的问题

- 现代保密通信技术：
  - 采用数据加密的方式，形成不可识别的密文进行传递，保证传输安全



保密通信的问题

- 传递的数据是密文，容易引起敌方的注意
- 通信系统传输的各类信息时刻处于敌方监视、侦收、窃听的威胁之中，如若防护措施不力，各种通信设施将会变成敌方的情报源



是否存在另外的保密通信方式?

隐蔽通信

- 加密：通过加密算法和密钥对信息本身进行保护，但是信息的传递过程是暴露的
- 隐蔽：将秘密信息隐藏于可公开的媒体信息中，掩盖信息存在的事实
- 将密码学与隐蔽通信相结合，就可以同时保证信息本身的安全和信息传递过程的安全

思考

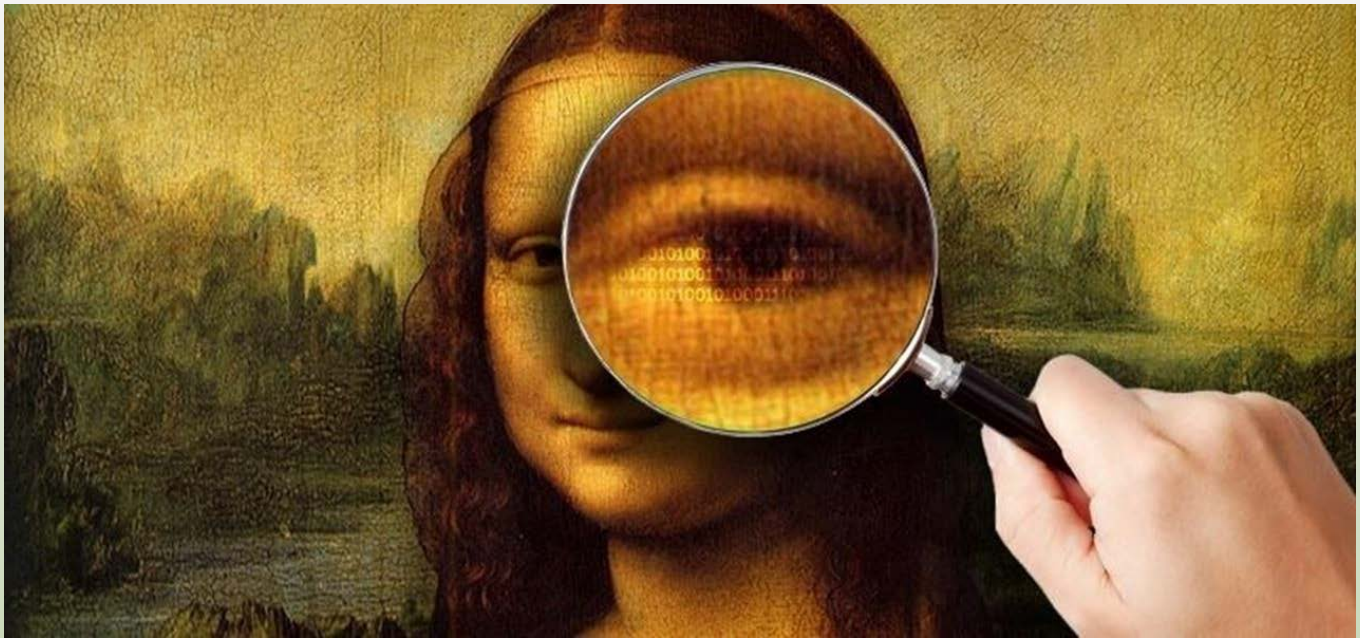
- 电影里存在隐蔽通信场景吗?

思考

- 电影里存在隐蔽通信场景吗?

什么是信息隐藏

- 隐写术（信息隐藏）类似于生物学上的保护色，它将主体（某一机密信息）秘密隐藏于外界环境（某公开载体）中，然后通过公开媒体来传输隐藏的机密信息



历史悠久

信息隐藏，是一门体现人类高度智慧的信息安全斗争技术和艺术。从古至今，几乎所有新的信息隐藏手段和技术一旦出现，就会立即用于情报作战中，不仅演绎出许多惊心动魄、惊险绝伦的故事，而且在一定程度上决定着战争的胜负乃至国家命运

信息隐藏的历史

- 早在公元前440年，隐写术就已经被应用
- 历史上关于隐写术的最早记载可以在古希腊历史学家希罗多德的著作中找到
  - 古希腊奴隶的头皮上写字

信息隐藏的历史

- 早在公元前440年，隐写术就已经被应用
- 历史上关于隐写术的最早记载可以在古希腊历史学家希罗多德的著作中找到
  - 反抗波斯国王入侵-涂蜡板上写字

信息隐藏的历史

- 我国古代也有利用隐写术进行秘密信息传递或军事命令传达的记载
  - 姜子牙告诉周武王，使用长短不同的竹板来表示前方战况，从而避免泄露军情

武王问太公曰：‘引兵深入诸侯之地，三军卒有缓急，或利或害。吾将以近通远，从中应外，以给三军之用，为之奈何？’.....——太公曰：‘主与将有阴符，凡八等：有大胜克敌之符，长一尺；破军擒将之符，长九寸；降城得邑之符，长八寸；却敌报远之符，长七寸；警众坚守之符，长六寸；请粮益兵之符，长五寸；败军亡将之符。长四寸；失利亡士之符。长三寸。诸奉使行符，稽留者，若符事泄，闻者告者皆诛之。八符者，主将秘闻，所以阴通言语，不泄中外相知之术。敌虽圣智，莫之能识。’——武王曰：‘善哉！’

——战国兵书《六韬·龙韬》

信息隐藏的历史

- 我国古代也有利用隐写术进行秘密信息传递或军事命令传达的记载
  - 北宋曾公亮在《武经总要》中将常用军事情报编写为40条短语

1请弓、2请箭、3请刀、4请甲、5请枪旗
6请锅幕、7请马、8 请衣赐、9请粮料、10请草料
11请车牛、12请船、13请攻城守具、14请添兵
15请移营、16请进军、17请退军、18请固守
19未见贼、20 见贼讫、21贼多、22贼少、23贼相敌
24贼添兵、25贼移营26贼进兵、27贼退兵、28贼固守
29围得贼城、30解围城、31被贼围、32贼围解
33战不胜、34战大胜、35战大捷、36将士投降
37将士叛、38士卒病、39都将病、40战小胜

信息隐藏的历史

- 基本过程
  - 选择一首五言律诗作为密钥，每一字都对应一条短语构成码本

    - 国破山河在，城春草木深
    - 感时花溅泪，恨别鸟惊心
    - 烽火连三月，家书抵万金
    - 白头搔更短，浑欲不胜簪

——杜甫《春望》

古代隐写术

- 技术性的隐写术
- 语言学中的隐写术
- 用于版权保护的隐写术

技术性的隐写术

- 用头发掩盖信息
  - 将消息写在头皮上，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（公元前440年）
- 使用涂蜡板隐藏信息
  - 首先去掉书记板上的腊，然后将消息写在木板上，再用腊覆盖，这样处理后的书记板看起来是一个完全空白的
- 将信函隐藏在信使的鞋底、衣服的皱褶中，妇女的头饰和首饰中等

技术性的隐写术

- 在一篇信函中，通过改变其中某些字母笔划的高度，或者在某些字母上面或下面挖出非常小的孔，以标识某些特殊的字母，组成秘密信息
- 采用隐形的墨水在特定字母上制作非常小的斑点（17世纪）
- 微缩胶片（1860年）
  - 使用军用信鸽传递微缩胶片中的情报
  - 将胶片粘贴在无关紧要的杂志等文字材料中的句号或逗号上

技术性的隐写术

- 使用化学方法的隐写术
  - 用笔蘸淀粉水在白纸上写字，纸晾干后什么也看不到；喷上碘水后，淀粉和碘水会起化学反应显出棕色文字
  - 但随着“万用显影剂”的发明，此方法就无效了。其原理是，根据纸张纤维的变化情况，来确定纸张哪些部位被水打湿过，这样所有采用墨水的隐写方法都无效了
- 在艺术作品中的隐写术
  - 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

语言学的隐写术

- 藏头诗

我画蓝江水悠悠，
爱晚亭上枫叶愁。
秋月溶溶照佛寺，
香烟袅袅绕经楼。

化工何意把春催？
缘到名园花自开。
道是东风原有主，
人人不敢上花台。

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。

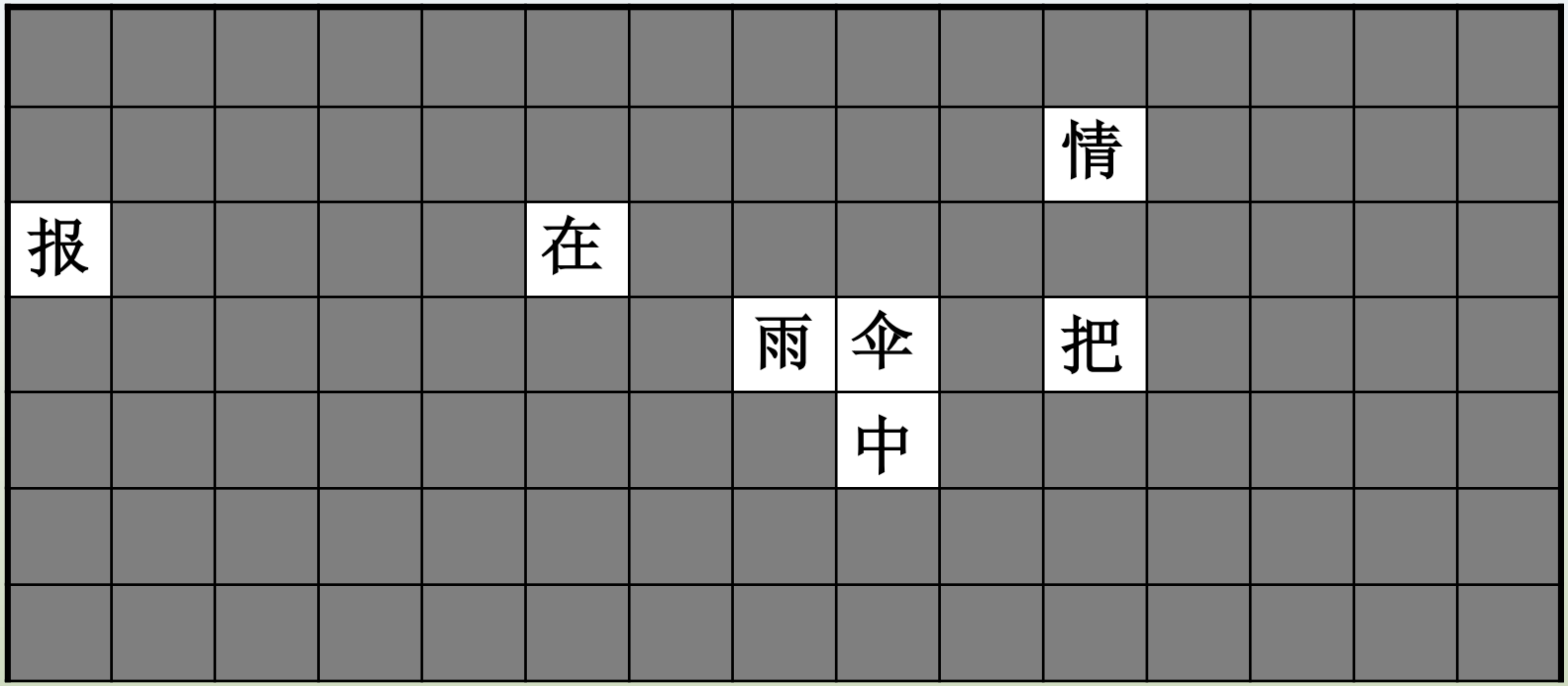
精神炯炯，
老貌堂堂。
乌巾白鬓，
龟鹤呈祥。

语言学的隐写术

- 乐谱
  - 二战传奇间谍加西亚：收集情报全靠“编”，而且还猜得八九不离十

语言学的隐写术

- 漏格法
  - 中国古代设计的信息隐藏方法，意大利数学家卡尔达诺（1501-1576）也发明了这种方法



语言学的隐写术

- 漏格法
  - 中国古代设计的信息隐藏方法，意大利数学家卡尔达诺（1501-1576）也发明了这种方法

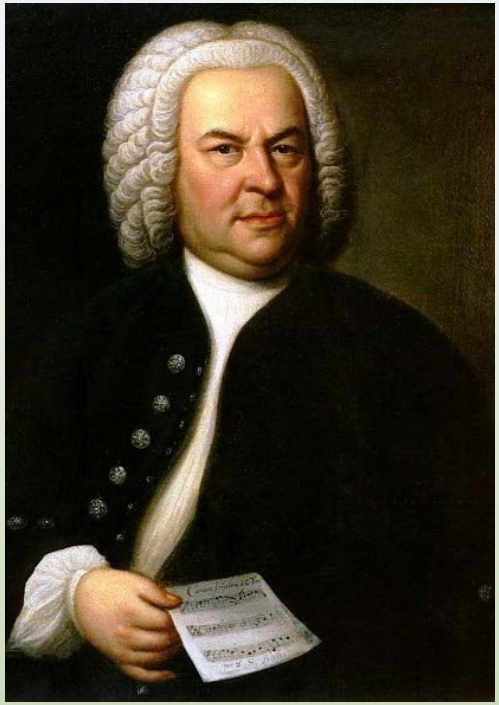
王	先	生	：										
		来	信	收	到	，	你	的	盛	情	真	是	难	以
报	答	。	我	已	在	昨	天	抵	答	广	州	。	秋	雨
连	绵	，	每	天	需	备	雨	伞	一	把	方	能	上	街
，	苦	矣	！	大	约	本	月	中	旬	我	才	能	返	回
，	届	时	再	见	。									
									弟		李	明		

用于版权保护的隐写术

- 核对校验图 （作品摘要）：
  - 克洛德.洛兰，17世纪一个很有名的风景画家，创作了一本素描集
  - 在素描和油画作品之间进行比较就会发现，素描是专门设计用来作为油画作品的“核对校验图”
  - 任何一个细心的观察者根据这本书仔细对照后就能判定一幅给定的油画是不是赝品

用于版权保护的隐写术

- 核对乐谱音符：
  - 德国作曲家巴赫，被称为“西方音乐之父”
  - 刻意将下图四个音符相连使用，翻译成音名正好就是巴赫自己的名字，这可能是巴赫首次为自己树立版权意识

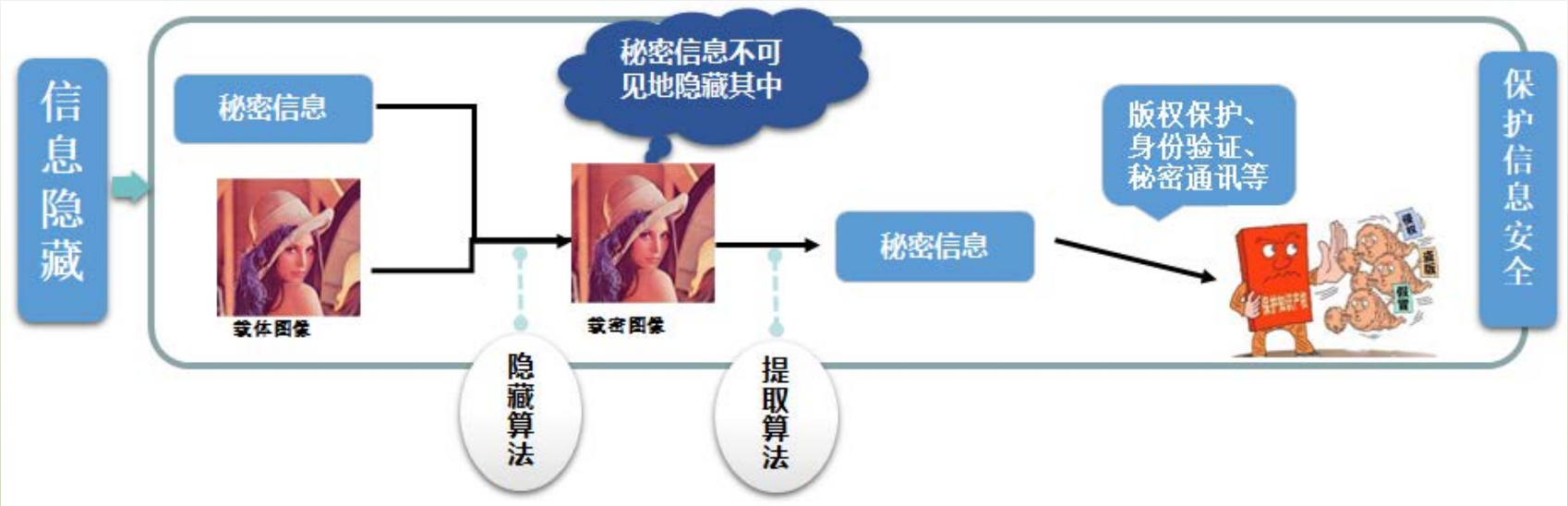


数字隐写概述

- 一、信息隐藏及其历史
- 二、现代信息隐藏
- 三、信息隐藏技术原理
- 四、数字水印

现代信息隐藏

- 古老的信息伪装手段和应用条件是十分有限的，在很长一段时间里，信息隐藏技术无论在研究领域还是在实际应用中都没有受到太大的注意
- 现代信息隐藏可以看做古典信息隐藏方法与现代多媒体信号处理技术的结合



现代信息隐藏

- 利用以数字信号处理理论（图像信号处理、音频信号处理、视频信号处理等）、人类感知理论（视觉感知、听觉感知）、现代通信技术、密码技术等为代表的伪装式信息隐藏方法来研究信息的保密和安全问题

基地组织用图像隐写发布行动计划

2001,09
911事件

俄罗斯间谍采用图像隐写传递情报

2010,06
美俄间谍战

基地组织在色情视频中隐藏情报

2012,05
反恐战

欧洲刑事侦缉机构破解犯罪分子使用的隐写术

2020,03
刑事侦查

现代信息隐藏

- 计算机取证专家Gary C. Kessler做的图片隐写示例
- 利用网上即可下载的图片隐写软件，将伯灵顿国际机场的图片藏进了鱼的图片中
- 接收者拿到图片后使用相似的软件就可提取出飞机场地图

现代信息隐藏

- 2010年美国发生过一起轰动一时的“俄罗斯间谍案”
- FBI在新泽西州抓获了10名俄罗斯特工，并引起了两国外交震荡

现代信息隐藏

- 可能吗?
  - 利用人类感知系统的冗余
    - 人类感知系统的分辨能力是有限的，对某些频段具有一定的掩蔽效应，比如，人眼对灰度的分辨率只有几十个灰度级别，听觉系统也有类似的局限性
  - 利用计算机处理系统的冗余
    - 多媒体数据本身存在着很大的冗余. 从信息论的角度看，未压缩的多媒体信息的编码效率是很低的，所以将消息嵌入到媒体数据中进行秘密传送是可行的
  - 利用各种潜在的隐蔽信道
    - 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隐蔽信道，可以被一个不可信的程序用来向它的控制者泄露信息
  - 技术上是可行的

现代信息隐藏

- 需要吗?
  - 现代战争——信息战

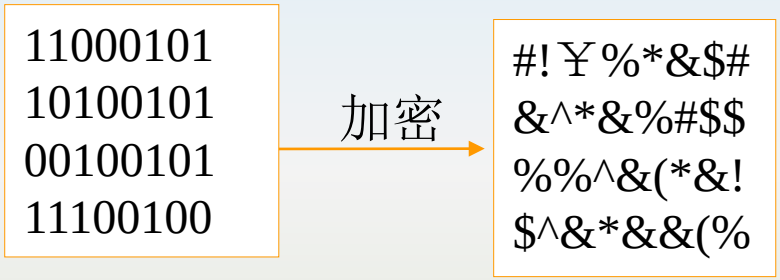
    尤其是国家安全部门需要研究伪装式信息安全的攻与防

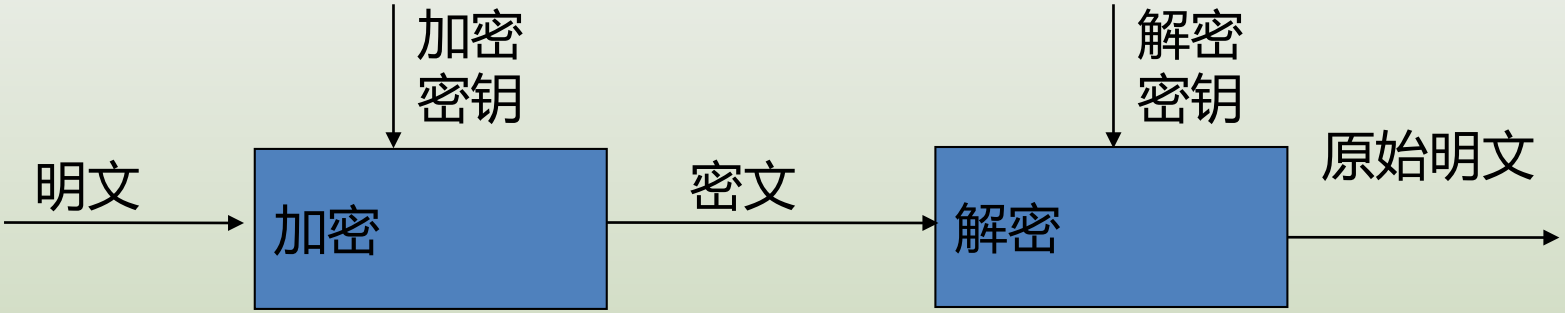
  - 数字水印

    数字产品无失真复制的特点，造成版权保护和管理方面的漏洞，数字水印为版权保护提供捷径

信息隐藏与密码

- 密码（Cryptography） - Hides contents of the communication



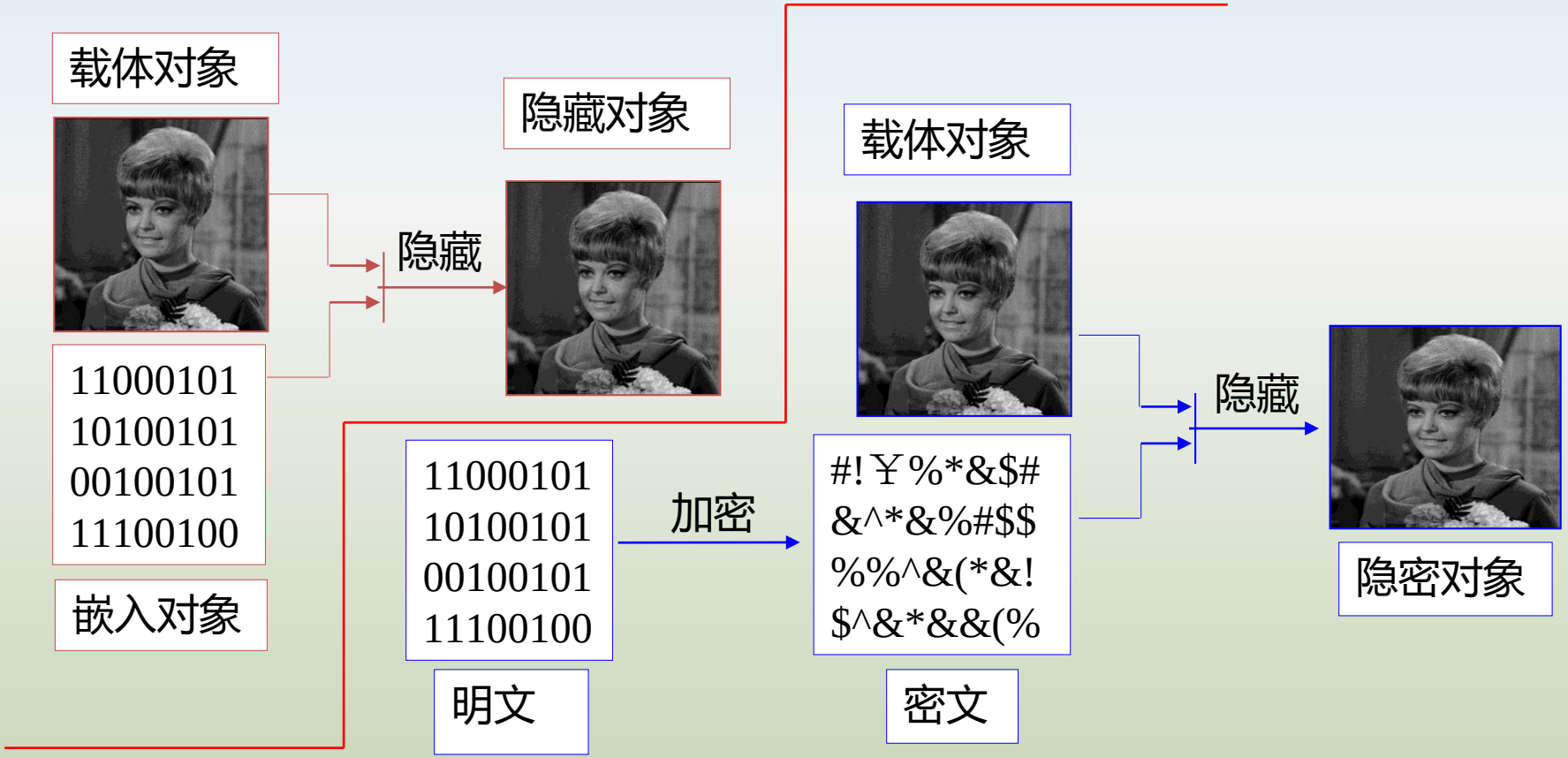


信息隐藏与密码

- 加密方法有一个致命的缺点，那就是它明确地提示攻击者哪些是重要信息，容易引起攻击者的好奇和注意
- 密文有被破解的可能性，一旦加密文件经过破解后其内容就完全透明了
- 攻击者也可以在破译失败的情况下将信息破坏，使得合法用户也无法阅读信息内容

信息隐藏与密码

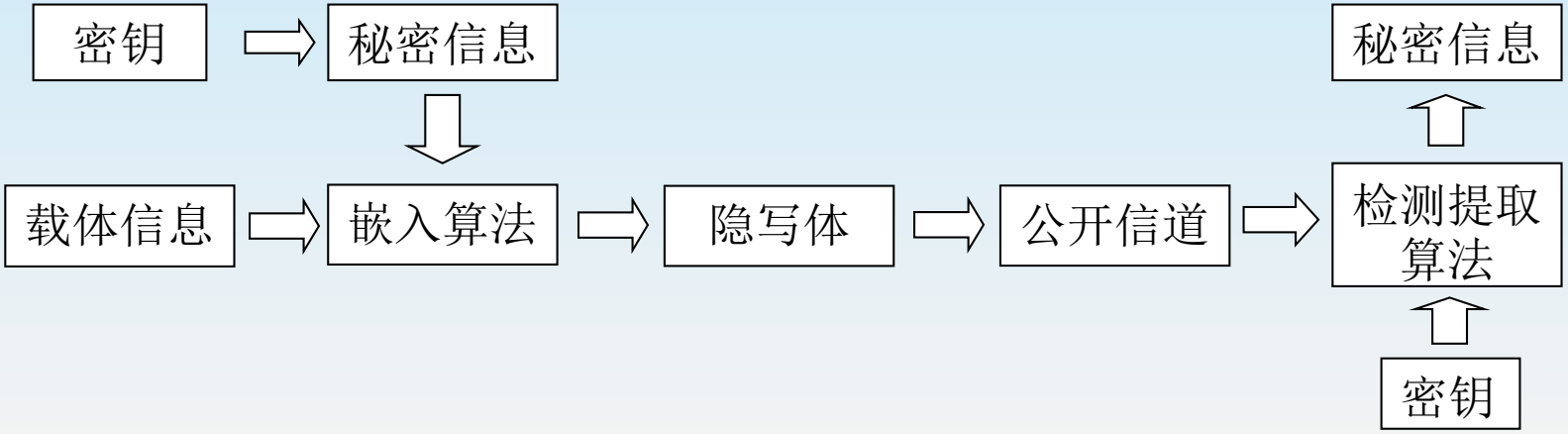
- 信息隐藏（information hiding） - Hides even the presence of the communication



数字隐写概述

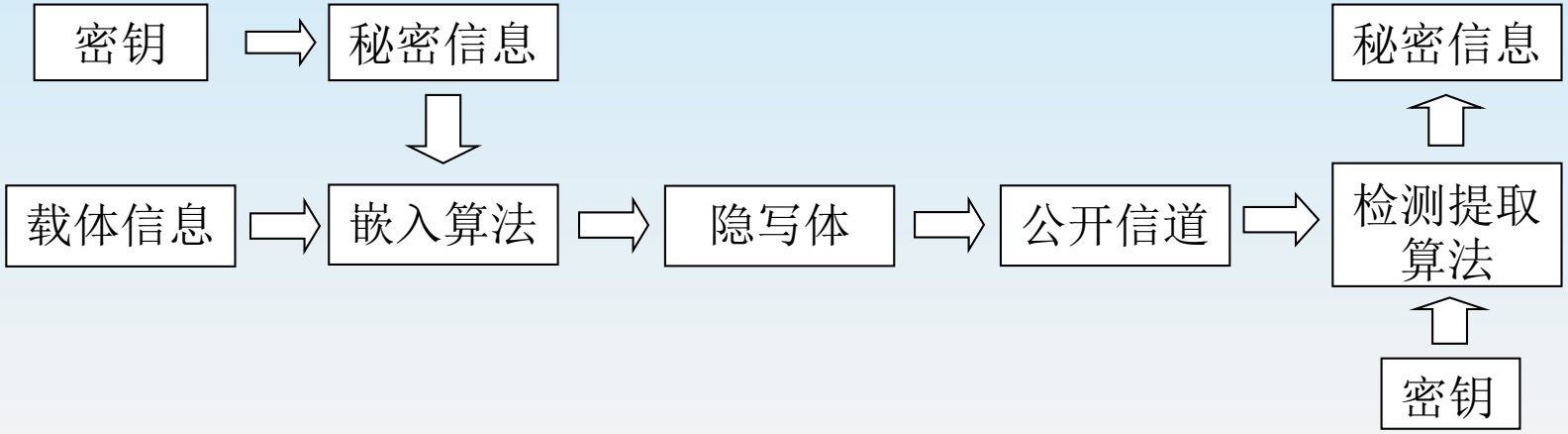
- 一、信息隐藏及其历史
- 二、现代信息隐藏
- 三、信息隐藏技术原理
- 四、数字水印

隐写系统-对象



- 宿主信息：载体信息（Cover-object）
- 嵌入的数据：秘密信息（Message）
- 嵌有数据的信息：隐写体（Setgo-object）

隐写系统-组成



(1) 秘密信息嵌入算法：利用密钥实现在公开的载体中隐藏秘密信息

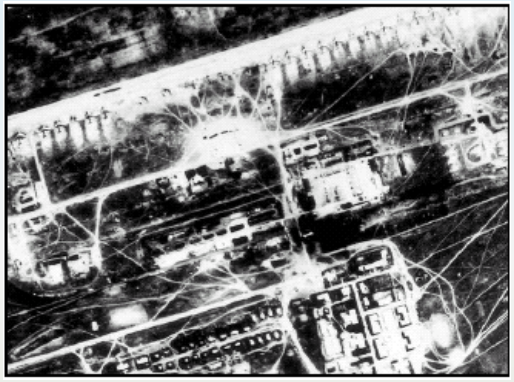
(2) 秘密信息检测/提取算法：利用密钥从载体中检测/恢复出秘密信息

(3) 密钥传递方式：采取保密信道传送，在密钥未知的前提下，未授权的第三者很难从隐密载体中得到信息或删除信息

信息隐藏的思想

- 守
  - 尽可能多地将信息隐藏在公开消息之中
  - 尽可能不让对手发现任何破绽
- 攻
  - 尽可能地发现和破坏对手利用信息隐藏技术隐藏在公开消息中的机密信息

信息隐藏——守



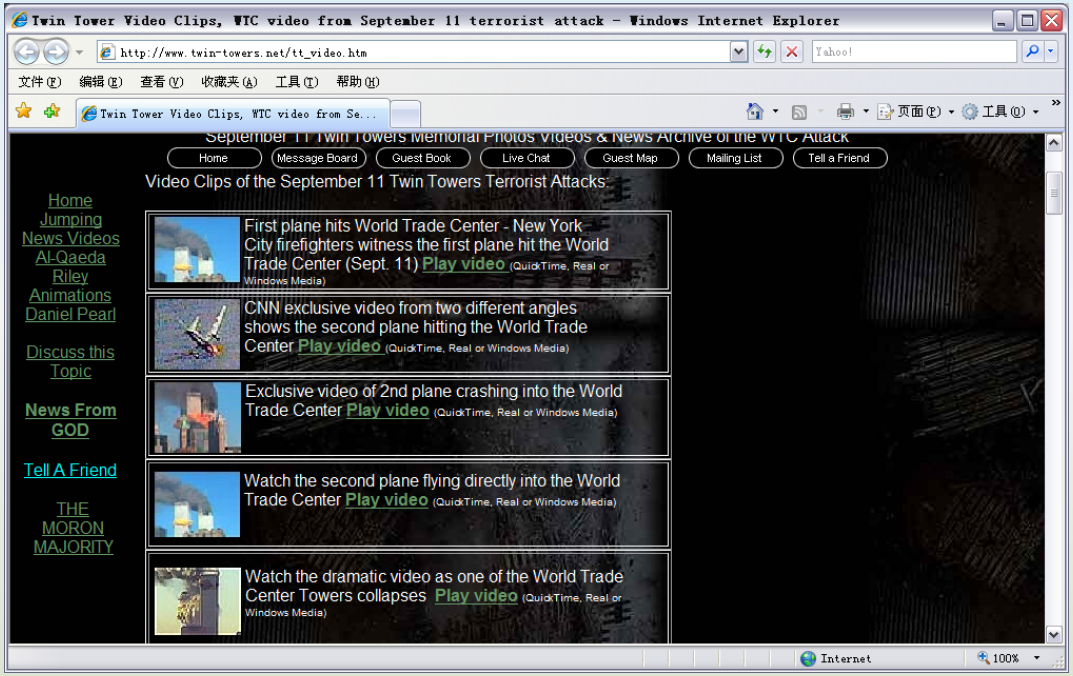
被卫星收集到的苏联战略轰炸机（卫星数据）

用S-Tools工具隐藏机场图片（载体为名画）

隐藏后的图像（感知无差别）

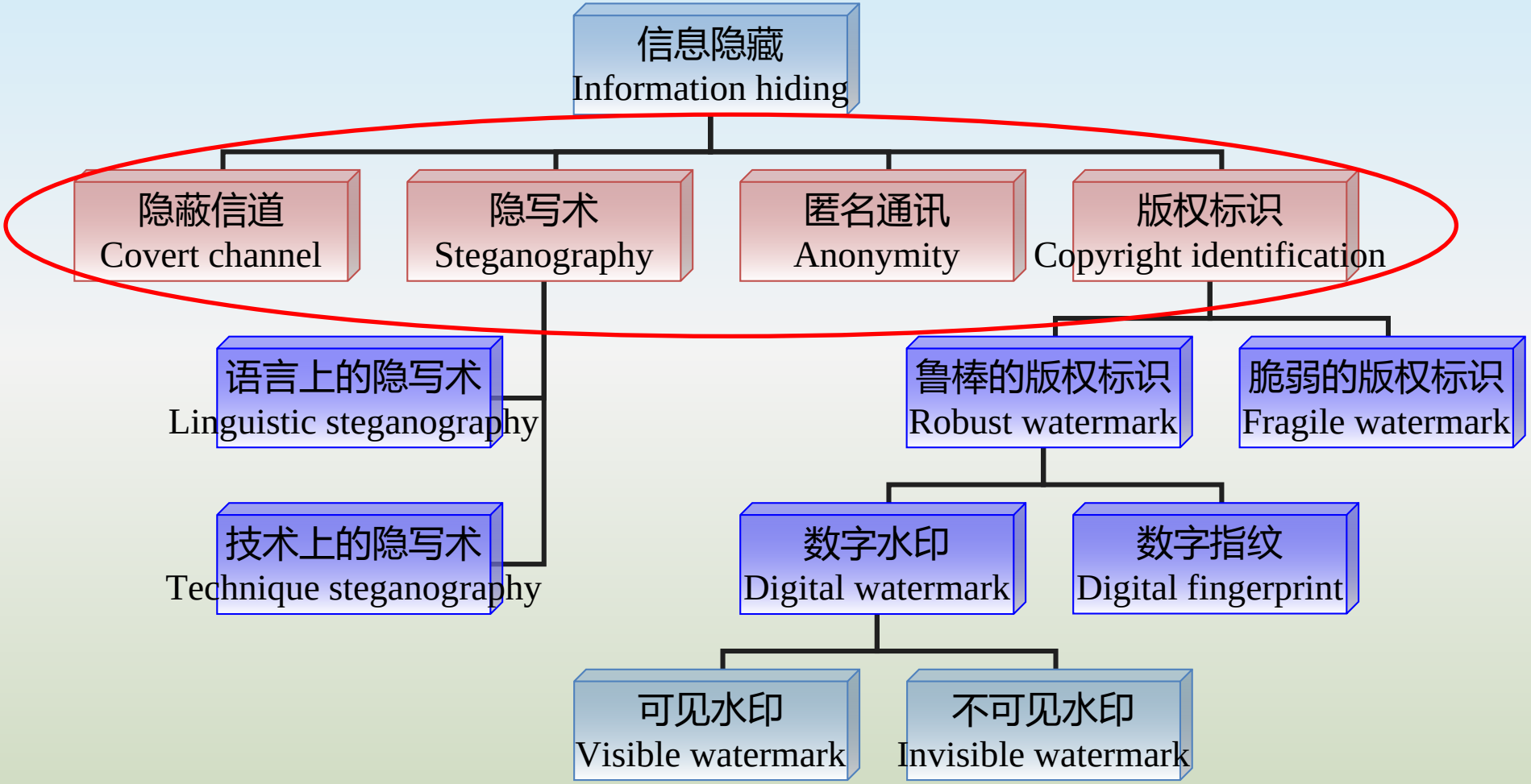
机密信息的隐蔽分发

信息隐藏——攻



发现对手隐藏在公开消息中的机密信息

信息隐藏分类


信息隐藏
Information hiding
隐蔽信道
Covert channel
隐写术
Steganography
匿名通讯
Anonymity
版权标识
Copyright identification
语言上的隐写术
Linguistic steganography
技术上的隐写术
Technique steganography
鲁棒的版权标识
Robust watermark
脆弱的版权标识
Fragile watermark
数字水印
Digital watermark
数字指纹
Digital fingerprint
可见水印
Visible watermark
不可见水印
Invisible watermark

信息隐藏分类

- 按载体分类
- 按密钥分类
- 按嵌入域分类
- 按提取要求分类
- 按保护对象分类

按载体分类

- 图像
- 视频
- 音频
- 文本
- 软件
- 通信协议

所有具备冗余的位置都可以隐藏信息

按密钥分类

按照隐藏信息的嵌入和提取是否采用相同密钥，分为：

- 对称隐藏算法（相同）
- 公钥隐藏算法（不同）

按嵌入域分类

- 空域隐写
  - LSB方法
  - 方法简单，鲁棒性差
- 变换域隐写
  - DCT变换，小波变换，傅立叶变换等
  - 信号能量分散，感知掩蔽特征方便结合，与数据压缩标准兼容，鲁棒性强

按提取要求分类

根据在提取隐藏信息时是否需要利用原始载体C，分为：

- 盲隐藏（不需要）
- 非盲隐藏（需要）

按保护对象分类

- 隐写术
  - 在不引起任何怀疑的情况下秘密传送消息
  - 要求：嵌入大容量信息，不容易被检测

- 数字水印
  - 嵌入载体相关信息，目的是进行版权保护、所有权证明、盗版源追踪、完整性保护
  - 要求：鲁棒性和不可感知性强

数字隐写概述

- 一、信息隐藏及其历史
- 二、现代信息隐藏
- 三、信息隐藏技术原理
- 四、数字水印

数字水印的提出

- 数字时代的福音:
  - 创建、处理、分发、存储和体验数字内容更加方便
  - 保证用户更加方便而且完美地体验丰富的数字内容
  - 成本的降低、质量保持不变，使得媒体应用范围迅速扩大
- 困境
  - 内容和介质逐渐无关：DVD－>闪盘、U盘
  - （有线、无线）电视－> 网络视频

数字水印的提出

- 版权管理 = 介质管理
  - 报纸/图书
  - 磁带/录像带
  - CD, VCD, DVD
  - 电视频道
- 模拟内容复制和分发费时费力，并且产生的效果欠佳
- 版权拥有者和用户的价值关系靠纸、塑料和电缆维系

数字水印的提出

- 全球盗版量每增加10%，全球相关的经济损失则增加1.2%。

——联合国教科文组织

- 在美国，盗版每年造成的经济损失已经达到580亿美元，损失的工作岗位为37.3万个，美国工人每年损失163亿美元的收入，美国政府每年的税金收入至少损失26亿美元。

——美国政策创新协会（IPI）2007

- 在中国，2006年仅盗版软件一项一年对国家经济带来的损失高达656亿元。

——国家知识产权局 2006

随着盗版工具普及化，盗版传播高速化，盗版危害加速化的趋势日益严重，极大地危害了数字作品的创造者、发行商的利益，阻碍了经济发展与社会进步，对全球经济产生巨大的影响。

数字水印的提出

- 传统的密码学方法不足以保护多媒体数据安全
  - 数据一旦解密则不再有任何保护措施
  - 加密难以适应多媒体文件的格式转换
- 数字水印
  - 对数字产品标识真伪，版权保护
    - 利用人类听觉、视觉系统的特点，在图像、音频、视频中加入一定的信息，使人们很难分辨出加水印后的资料与原始资料的区别，而通过专门的检验步骤又能提取出所加信息，以此证明原创者对数字媒体的版权

数字水印的提出

- 定义
  - 在数字化数据内容中嵌入不明显的记号。被嵌入的记号通常是不可见或不可察觉的，但是通过一些计算操作可以被检测或被提取
- 应用领域
  - 原始数据的真伪鉴别、数据侦测与跟踪、数字产品版权保护等。数字水印不仅要实现有效的版权保护，而且加入水印后的图像必须与原始图像具有同样的应用价值

数字水印的应用

- 数字版权保护
  - 其动机是在数字作品中嵌入作品来源以及所有权等信息，在所有权起争执时，版权所有者能从被恶意攻击后的数字作品中正确提取出水印信息

数字水印的应用

- 多媒体认证和篡改检测
  - 在多媒体数据中事先嵌入完整性信息，然后在检测时提取这个信息，用来确定宿主数据是否被修改过

数字水印的应用

- 数字指纹与盗版追踪
  - 在发行的每个拷贝中嵌入不同的水印，通常称之为“数字指纹”，其目的是传输合法接收者（不是数据来源者）的信息，主要用于识别数据的单个发行拷贝，类似软件产品的序列号，对监控和跟踪流通数据的非法拷贝非常有用

数字水印的应用

- 拷贝控制和访问控制
  - 嵌入的水印包括特定的拷贝控制和访问控制策略。
  - 水印检测器通常被集成在录制/播放设备中，通过特定的硬件或软件检测是否符合控制策略，以启动或关闭录制和播放模块，相关拷贝控制权限包括：
    - 不允许复制
    - 仅允许复制一次
    - 允许复制多次

数字水印的应用

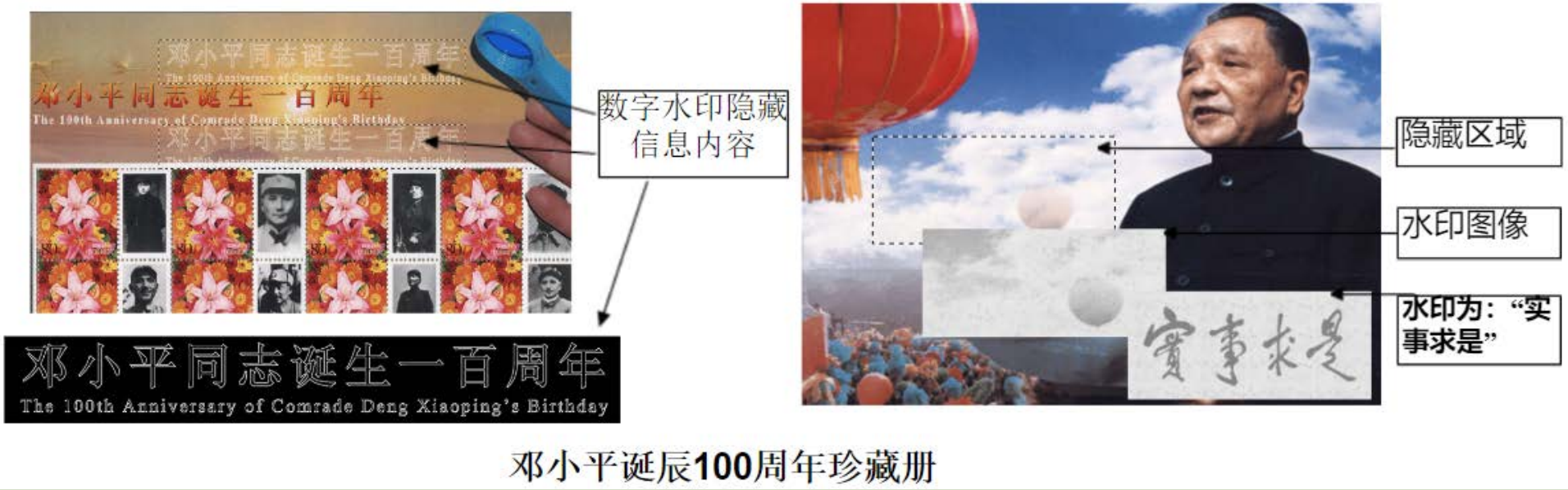
- 广播监视
  - 电视网络的商业广告播放费用极其昂贵，都是按秒计算费用
  - 在商业广告中嵌入水印后，可以使用自动检测系统来检测商业广告是否按照预定要求播放
  - 广播监视系统不仅可以保护商业广告，而且可以保护有价值的电视节目

数字水印的应用

- 商务交易中的票据防伪、电子印章
  - 随着高质量图像输入输出设备的发展，货币、支票以及其他票据的伪造变得更加容易
  - 2005年《电子签名法》的确立说明用于票据防伪的数字水印技术受到我国政府的高度重视

数字水印的应用

- 全球第一个采用数字水印的邮票：纪念邓小平100诞辰周年邮票



数字水印的概念与原理

水印嵌入系统

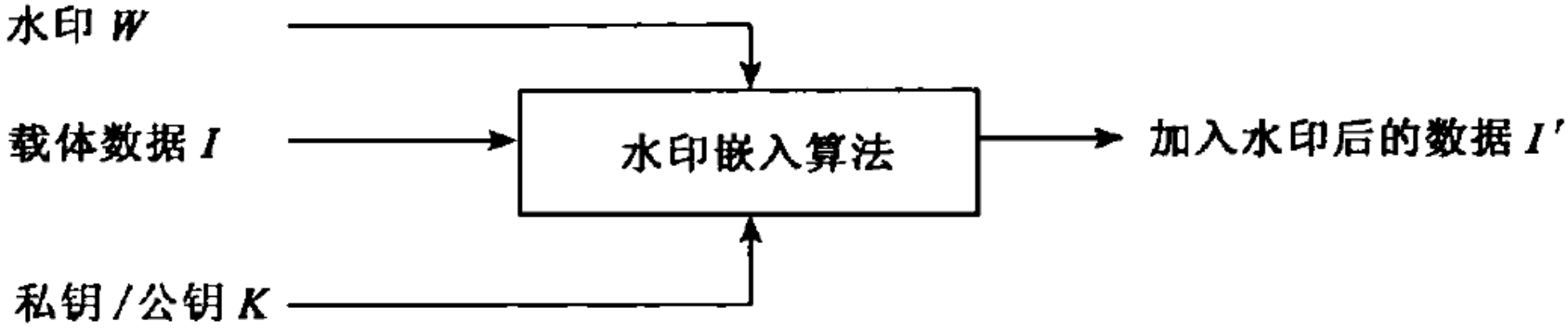


图 3.1　数字水印嵌入方案

数字水印的概念与原理

水印恢复系统

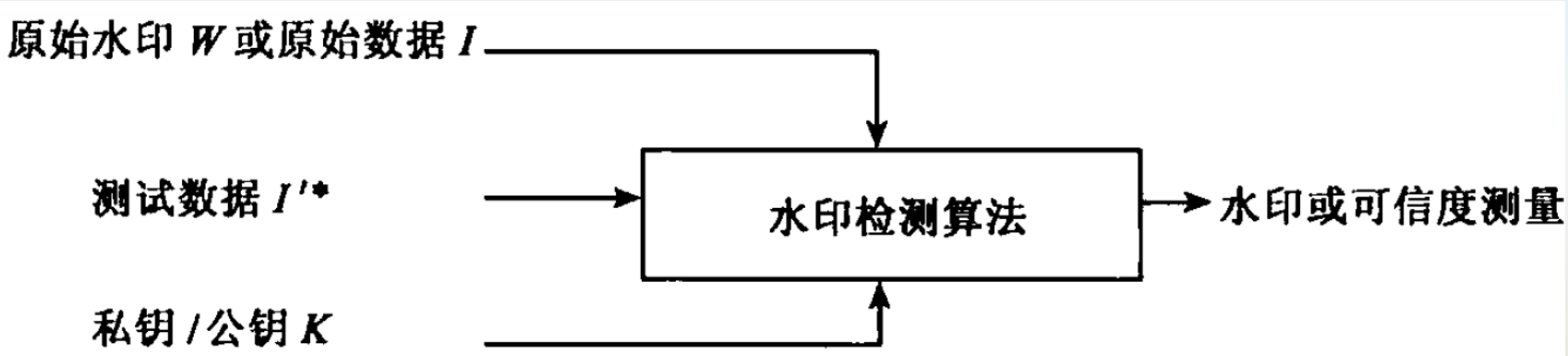


图 3.2　数字水印恢复方案

数字水印的概念与原理

信息隐藏与数字水印的区别

	信息隐藏	数字水印
用途	用于保密通信	用于版权标识
前提	一般不知有隐藏信息（如果已怀疑有隐藏信息，则已经不安全）	可以公布保护对象有水印存在
主要攻击	隐写分析（分析是否为正常载体）	水印擦除
主要考核	透明性	鲁棒性

水印检测模型

- 水印检测过程中，设水印提取函数为D，具体步骤如下：
  - 提取原始水印：例如文字、徽标

$$W^* = D(I'^*, I, K)$$

  - 0-1判决：判定水印存在与否

$$C(W, W^*, K, \delta) = \begin{cases} 1, & W\text{存在} \\ 0, & W\text{不存在} \end{cases}$$

水印提取模型

- 在完整性确认和篡改提示应用中，必须能够精确提取出嵌入的水印信息，从而通过水印的完整性来确认多媒体数据的完整性

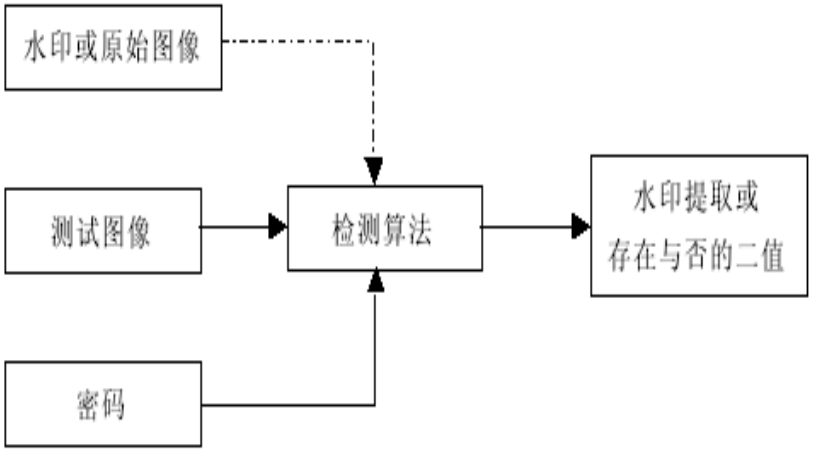


图2-3 水印图像检测算法

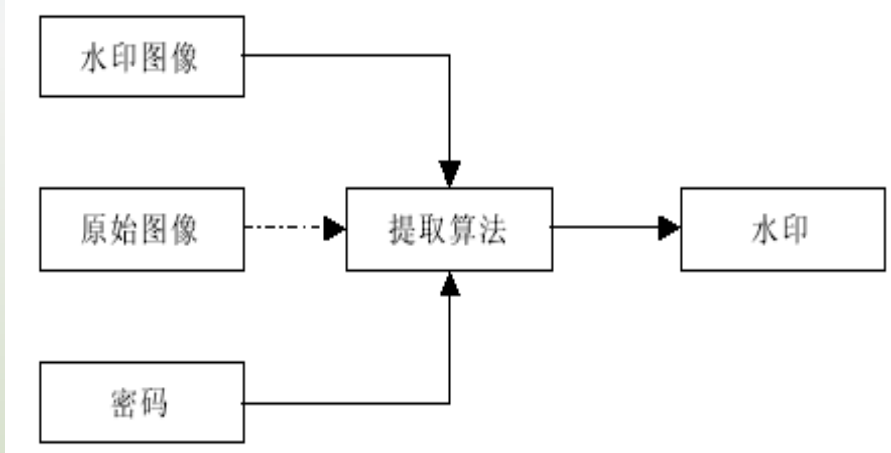


图2-2 水印提取算法

数字水印的性能评价

- 鲁棒性
  - 水印信息能够经受住各种常用信号处理运算的能力
- 抗攻击性
  - 水印系统抵抗恶意攻击的性能
- 保真性
  - 即不可感知性，要求嵌入水印后媒体视音频质量的变化不易被观察者所觉察
- 水印容量
  - 指可以在载体中嵌入的信息量

鲁棒性、保真性、水印容量三者之间达到平衡

数字水印-攻击

- 去除攻击
  - 试图削弱载体中的水印强度，或破坏载体中的水印存在
- 共谋攻击
  - 恶意用户群通过共享信息，产生非法内容
- 表达攻击
  - 试图使水印检测失效
- 解释攻击
  - 通过伪造水印来达到目的
- 法律攻击
  - 利用法律上的漏洞

去除攻击

- 对整个嵌入数字水印后的载体数据进行操作来干扰嵌入的数字水印幅度，从而导致数字水印的提取发生错误，或者根本无法提取出数字水印信号

- 常见的操作有滤波，加噪，图像锐化、有损压缩、像素域量化、修改直方图、颜色量化

共谋攻击

- 共谋攻击类型I：相同的水印嵌入到大量的不同数据中。共谋者们只需要叠加手中大量的不同数据，就能估计出嵌入的水印信息

- 共谋攻击类型II：不同的水印嵌入到相同数据的不同拷贝中。共谋者们只须叠加手中大量的拷贝，就能统计平均出不含水印的数据对象

表达攻击

- 不以完全去除水印为目的，而是试图使得水印信息无法被检测
- 试图破坏载体数据和数字水印的同步性，使数字水印的相关检测失效或使嵌入的数字水印提取不出来
- 通常采几何变换方法，如缩放、空间方向的平移、时间方向的平移(视频数字作品)、旋转剪切、像素置换、二次抽样化、像素的插入或抽取等

解释攻击

- 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种解释
- 混淆攻击：试图生成一个伪源数据、伪数字水印化数据来混淆含有真正数字水印的数字作品的版权
- 虽然载体数据是真实的，数字水印信号也存在，但是由于嵌入了一个或多个伪造的数字水印，混淆了第一个含有主权信息的数字水印，失去了唯一性

法律攻击

- 不同国家和地区有不同的法律规定
- 法律攻击利用版权及数字信息所有权在法律上的漏洞和不健全，破坏数字水印的价值
- 据此应健全相关法律条例和公证制度，将数字水印信息作为电子证据应用于版权的仲裁