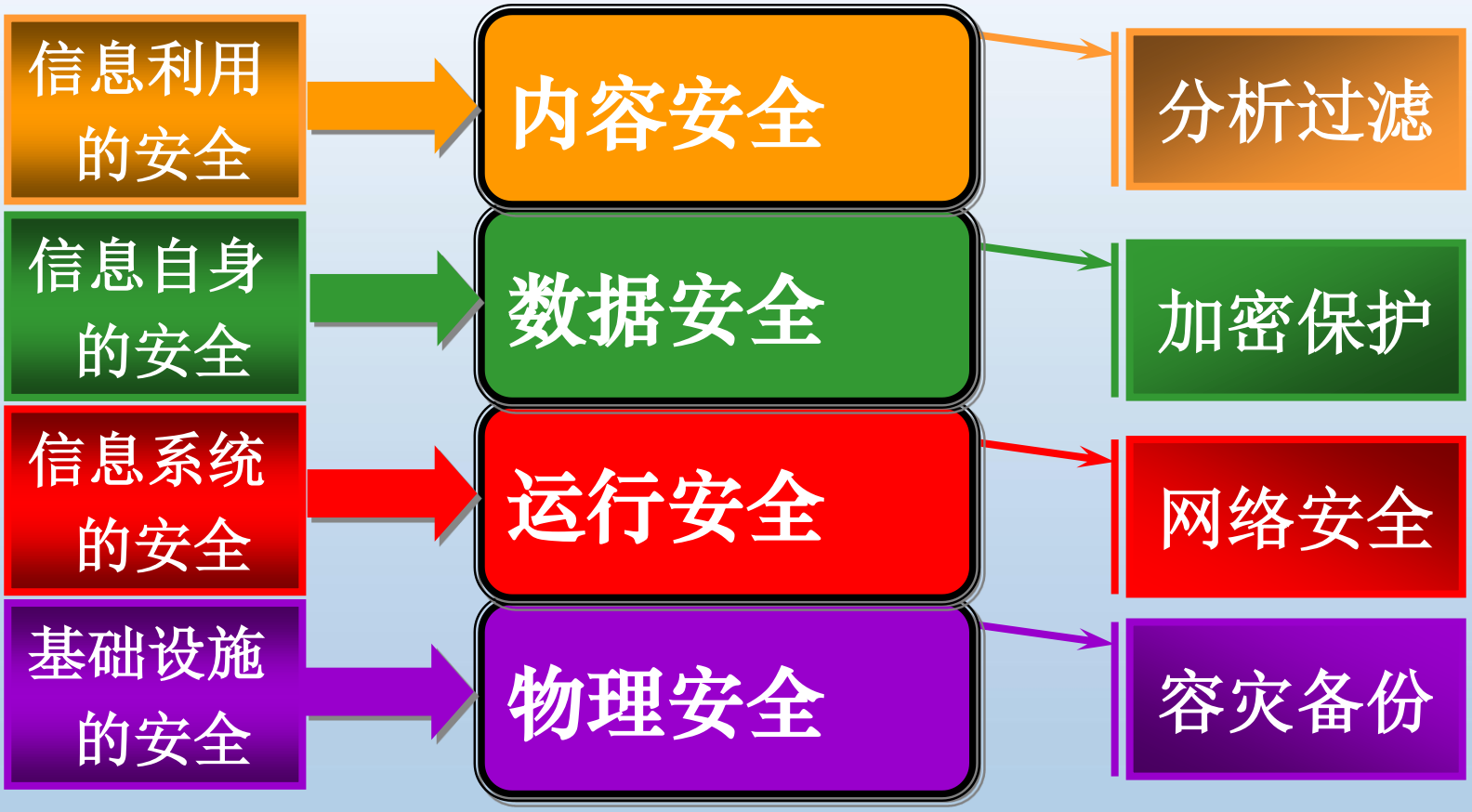
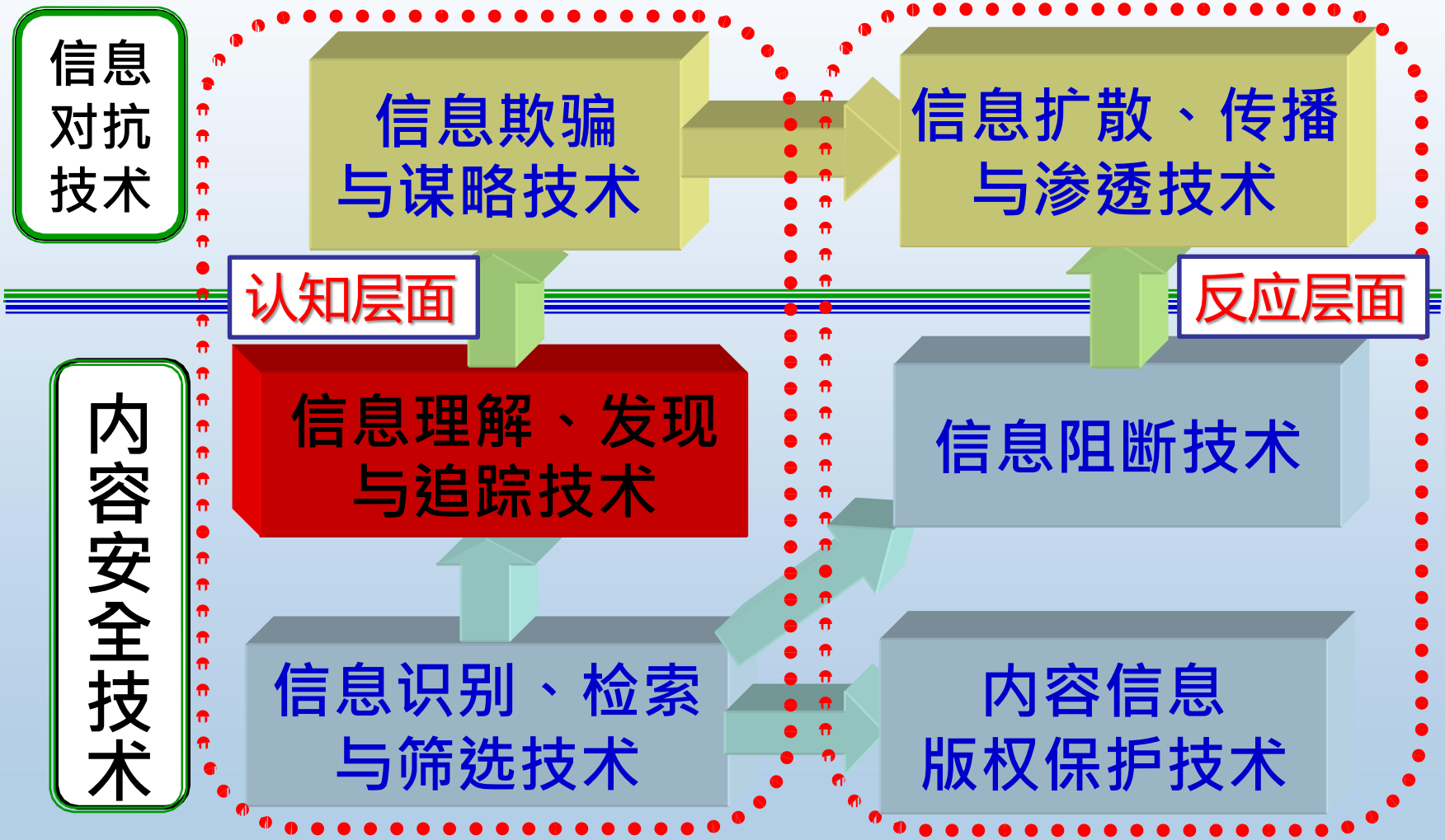
第一部分 数字内容安全概述

信息安全整体概念

- 基本概念：信息安全概述
- 宏观：网络安全模型
- 基石：法律法规与标准
- 技术：
  - 密码基础
    - 保密技术
    - 密码应用
  - 网络安全
  - 内容安全
  - 灾备技术
- 保障：
  - 信息安全管理


信息利用的安全
信息自身的安全
信息系统的安全
基础设施的安全
内容安全
数据安全
运行安全
物理安全
分析过滤
加密保护
网络安全
容灾备份
保护目标
信息安全层次模型
主要作用

数字内容安全概念


信息对抗技术
信息欺骗与谋略技术
信息扩散、传播与渗透技术
认知层面
反应层面
内容安全技术
信息理解、发现与追踪技术
信息阻断技术
信息识别、检索与筛选技术
内容信息版权保护技术

数字内容安全分类

- 图像、音频、视频、文本等的
  - 安全传输（加密、隐藏）
  - 安全利用（内容理解、检索、分类、识别、过滤、消息源追踪、版权管理、等）
- 应用
  - 舆情（网络文化，网络热点事件）
  - 信息过滤、分析
  - 信息隐藏
  - 数字版权管理

数字内容安全核心技术

1. 信息获取技术

分为主动获取技术和被动获取技术。

主动获取技术通过向网络注入数据包后的反馈来获取信息，特点是接入方式简单，能够获取更广泛的信息内容，但会对网络造成额外的负担。

被动获取技术则在网络出入口上通过镜像或旁路侦听方式获取网络信息，特点是接入需要网络管理者的协作，获取的内容仅限于进出本地网络的数据流，但不会对网络造成额外流量。

数字内容安全核心技术

2．信息内容识别技术

信息内容识别是指对获取的网络信息内容进行识别、判断、分类，确定其是否为所需要的目标内容，识别的准确度和速度是其中的重要指标。主要分为文字、音频、图像、图形识别。

目前文字识别技术已得到广泛应用，音频识别也在一定范围内使用，但图像识别的准确性还有待进一步提高离实际应用尚有一定的距离。

数字内容安全核心技术

3．控制/阻断技术

对于识别出的非法信息内容，阻止或中断用户对其访问，成功率和实时性是两个重要指标。

从阻断依据上分为基于IP地址阻断、基于内容的阻断；从实现方式上分为软件阻断和硬件阻断；

从阻断方法上分为数据包重定向和数据包丢弃。

具体地，在垃圾邮件剔除、涉密内容过滤、著作权盗用的取证、有害及色情内容的阻断和警告等方面已经投入使用。

数字内容安全核心技术

4．信息内容分级

网络“无时差、零距离”的特点使得不良内容以前所未有的速度在全球扩散，网络不良内容甚至还会造成青少年生理上的伤害。应该建立自己的网上内容分级标准，让父母保护他们的孩子远离互联网上有潜在危害的内容。

数字内容安全核心技术

5. 图像过滤

一些不良网络信息的提供者采取了回避某些敏感词汇，将文本嵌入到图像文件中，或直接以图像文件的形式出现等方法，从而可以轻易地通过网络过滤和监测系统。为此，需要对网页中的图像进行分析和理解实现网络过滤。目前这一技术还没有达到实用系统的要求。

数字内容安全核心技术

6．信息内容审计

信息内容审计的目标就是真实全面地将发生在网络上的所有事件记录下来，为事后的追查提供完整准确的资料。通过对网络信息进行审计，政府部门可以实时监控本区域内Internet的使用情况，为信息安全的执法提供依据。虽然审计措施相对网上的攻击和窃密行为是有些被动，它对追查网上发生的犯罪行为起到十分重要的作用，也对内部人员犯罪起到了威慑作用。

采用的主要技术是以旁路方式捕获受控网段内的数据流，通过协议分析、模式匹配等技术手段对网络数据流进行审计，并对非法流量进行监控和取证。

数字内容安全核心技术

审计技术的发展趋势可归纳为以下几个主要方面：

1）包捕获技术。通过采用零拷贝技术，尽可能减少内存拷贝开销。

2）模式匹配技术，提高多关键字条件下的模式匹配效率以及中文信息模糊匹配精度和效率。

3）协议分析与还原技术。解决对数据包分片的分析与还原技术、抵御DDoS攻击对探测引擎的影响，拓展对网络应用协议分析的范围。

4）对各种复杂条件下的信息源精确定位技术。

5）数据检索与智能化统计分析技术。

数字内容安全技术与产品

- 信息内容分级标准的制定及相应的过滤产品与技术
- 信息资产的安全等级评定技术及产品
- 大流量网络信息的实时监控技术与产品
- 移动终端的防病毒与防泄漏技术与产品
- IPv6的信息内容安全技术与产品
- 骨干网内容过滤技术与产品
- 基于图像内容监管技术与产品
- 基于音频的内容监管技术与产品
- 国家级分布式网络内容监管体系
- 信息内容的渗透与反渗透技术与产品
- 网关型网络蠕虫及病毒的查杀技术与产品

数字内容安全所面临的挑战

- 体系框架与基础理论的缺失
  - 关于信息内容安全模型、框架体系的研究尚属空白，信息内容安全也缺少相应基础理论的研究与支持
- 信息流规模的飞速增长
  - 庞大的网络流量对信息内容的海量信息获取、存储及实时处理能力提出了严峻的挑战
- 信息的异构性和多源化
  - 信息流的结构已经日趋多样化。文本、语音、图像、视频等多媒体信息在网上通过各种手段进行传播

数字内容安全所面临的挑战

- 信息的广泛性和海量性
  - 由于信息量的飞速增长以及信息的快速分布、扩散、演变，互联网与人类社会的深度交融使得对信息的理解判断更为复杂
- 测试验证平台与相关标准的缺失
  - 缺乏面向信息内容安全技术研发的测试验证平台，难以为信息内容安全技术和系统的研发提供有效的配套环境支持
  - 缺少相关的信息内容安全技术标准，导致信息内容安全系统的研发始终处于被动境地，事倍功半

研究内容

应用技术研究

以实用化为主要目的，设计并实现适合各种环境的信息隐藏和数字水印系统

应用基础研究

针对图像、声音、视频等载体，研究相应的信息隐藏和数字水印算法

基础理论研究

信息隐藏模型、理论框架、容量、安全性理论等

方向之一：

信息隐藏（隐写术）

信息隐藏

- 信息隐藏在计算机科学中所处的位置
  - 基础理论（理论计算机，量子计算）
  - 计算机软件（可信软件）
  - 计算机体系结构（多核技术）
  - 计算机硬件
  - 计算机应用技术（多媒体，人工智能）
  - 自然语言理解与机器翻译
  - 信息安全（密码学，信息隐藏）
  - 计算机网络（无线传感器网络，自组网）

相关概念

信息安全

- 提到信息安全，人们自然会想到密码
- 密码术的起源可以追溯到四千多年前的古埃及、古罗马和古希腊
- 古代：
  - 密码术：以信息无法被看懂为目的
  - 隐写术：以隐蔽机密信息的存在为目的
- 现代：
  - 现代密码学
  - 伪装式信息安全：信息隐藏、数字水印

信息隐藏基本概念

囚犯问题

- 两个囚犯A和B被关押在监狱的不同牢房，他们想通过一种隐蔽的方式交换信息，但是交换信息必须要通过看守的检查。因此，他们要想办法在不引起看守者怀疑的情况下，在看似正常的信息中，传递他们之间的秘密信息
- 被动看守者：只是检查传递的信息有没有可疑的地方
- 主动看守者：故意去修改一些可能隐藏有信息的地方，或者假装自己是其中的一个囚犯，隐藏进伪造的消息，传递给另一个囚犯

针对的问题

- 依靠密码学不能完全解决问题
  - 加密方法有一个缺点，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，并有被破解的可能性，而且一旦加密文件经过破解后其内容就完全透明了。
  - 攻击者可以在破译失败的情况下将信息破坏，使得即使是合法的接收者也无法阅读信息内容。

数字媒体的知识产权保护问题

- 互联网上的数字媒体应用正在呈爆炸式的增长，越来越多的知识产品以电子版的方式在网上传播。
- 数字信号处理和网络传输技术可以对数字媒体(数字音频，图象和视频)的原版进行无限制的任意编辑，修改，拷贝和散布，造成数字媒体的知识产权保护和信息安全的问题日益突出。

信息隐藏的历史

- 古代的隐写术
  - 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

古代的隐写术——技术性的

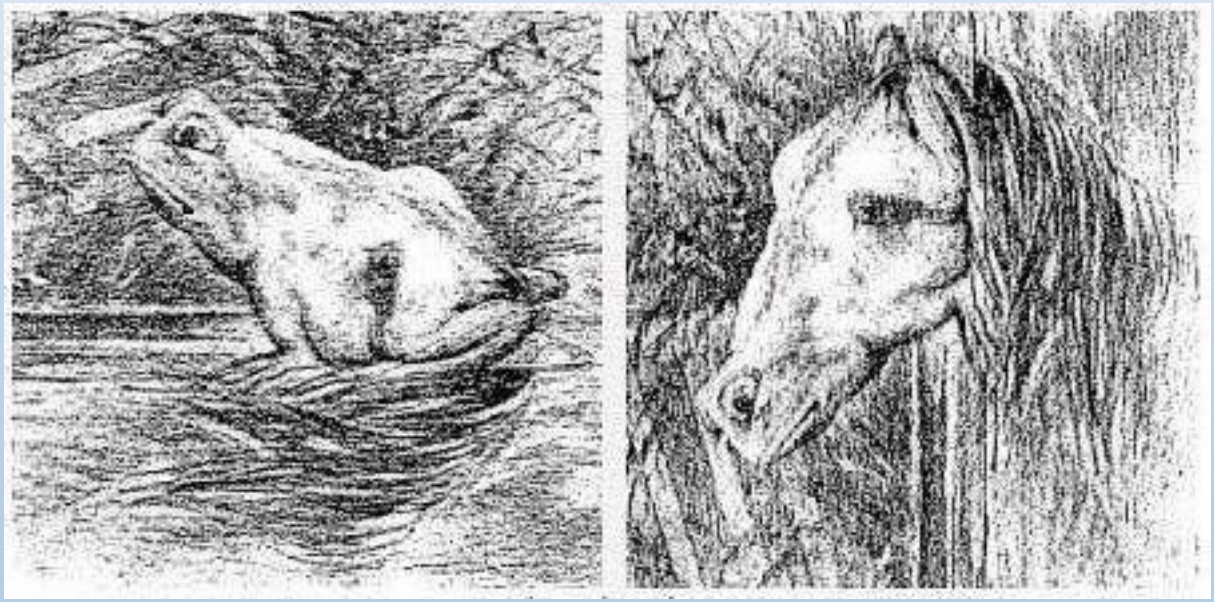
- 用头发掩盖信息
  - 将消息写在头皮上，等到头发长出来后，消息被遮盖，这样消息可以在各个部落中传递（公元前440年）
- 使用记事板隐藏信息
  - 首先去掉记事板上的腊，然后将消息写在木板上，再用腊覆盖，这样处理后的记事板看起来是一个完全空白的
- 将信函隐藏在信使的鞋底、衣服的皱褶中，妇女的头饰和首饰中等

- 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，这些特殊的字母组成秘密信息
  - 采用无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）
- 信鸽传递
  - 粘贴在无关紧要的杂志等文字材料中的句号或逗号上

- 使用化学方法的隐写术
  - 用笔蘸淀粉水在白纸上写字，然后喷上碘水，则淀粉和碘起化学反应后显出棕色字体
- 化学的进步促使人们开发更加先进的墨水和显影剂
  - 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，来确定纸张的哪些部位被水打湿过，这样，所有采用墨水的隐写方法，在“万用显影剂”下都无效了。

■ 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



古代的隐写术——语言学的

- 藏头诗

施耐庵《水浒传》第61回
吴用诱使卢俊义将离合诗

卢花潭上有扁舟，
俊杰黄昏独自游。
义到尽头原有命，
反弓逃难必无忧。

题于墙上，使卢俊义遭官府
迫害逼上梁山

乐谱

- 第二次世界大战期间，一位热情的女钢琴家，常为联军作慰问演出，并通过电台播放自己谱写的钢琴曲。由于联军在战场上接连遭到失败，反间谍机关开始怀疑到这位女钢琴家，可一时又因找不到钢琴家传递情报的手段和途径而迟迟不能决断。原来，这位德国忠实的女间谍，从联军军官那里获得军事情报后，就按照事先规定的密码巧妙地将其编成乐谱，并在电台演奏时一次次公开将重要情报通过悠扬的琴声传递出去。

卡登格子

- 中国古代设计的信息隐藏方法中，发送者和接收者各持一张完全相同的、带有许多小孔的纸，这些孔的位置是被随机选定的。发送者将这张带有孔的纸覆盖在一张纸上，将秘密信息写在小孔的位置上，然后移去上面的纸，根据下面的纸上留下的字和空余位置，编写一段普通的文章。接收者只要把带孔的纸覆盖在这段普通文字上，就可以读出留在小孔中的秘密信息

在16世纪早期，意大利数学家Cardan(1501-1576)也发明了这种方法，这种方法现在被称作卡登格子法

古代的隐写术——用于版权保护

- 纸张中的水印
- 高级酒店的信笺纸中的水印
- 纸币中的水印

现阶段研究背景

- 随着通信技术和网络的快速发展，各种层次 重要信息的安全问题日益受到重视
  - 信息的安全传递成为信息安全的重要方面
  - 虽然现有的密码技术可以保证信息本身的机密性，但秘 密信息正在传递的事实是暴露的
- 数字作品的合法使用变得越来越迫切
  - 盗版与反盗版的斗争愈演愈烈
- 以信息隐藏为代表的“非加密安全技术”已经成为 解决上述问题的主要手段之一

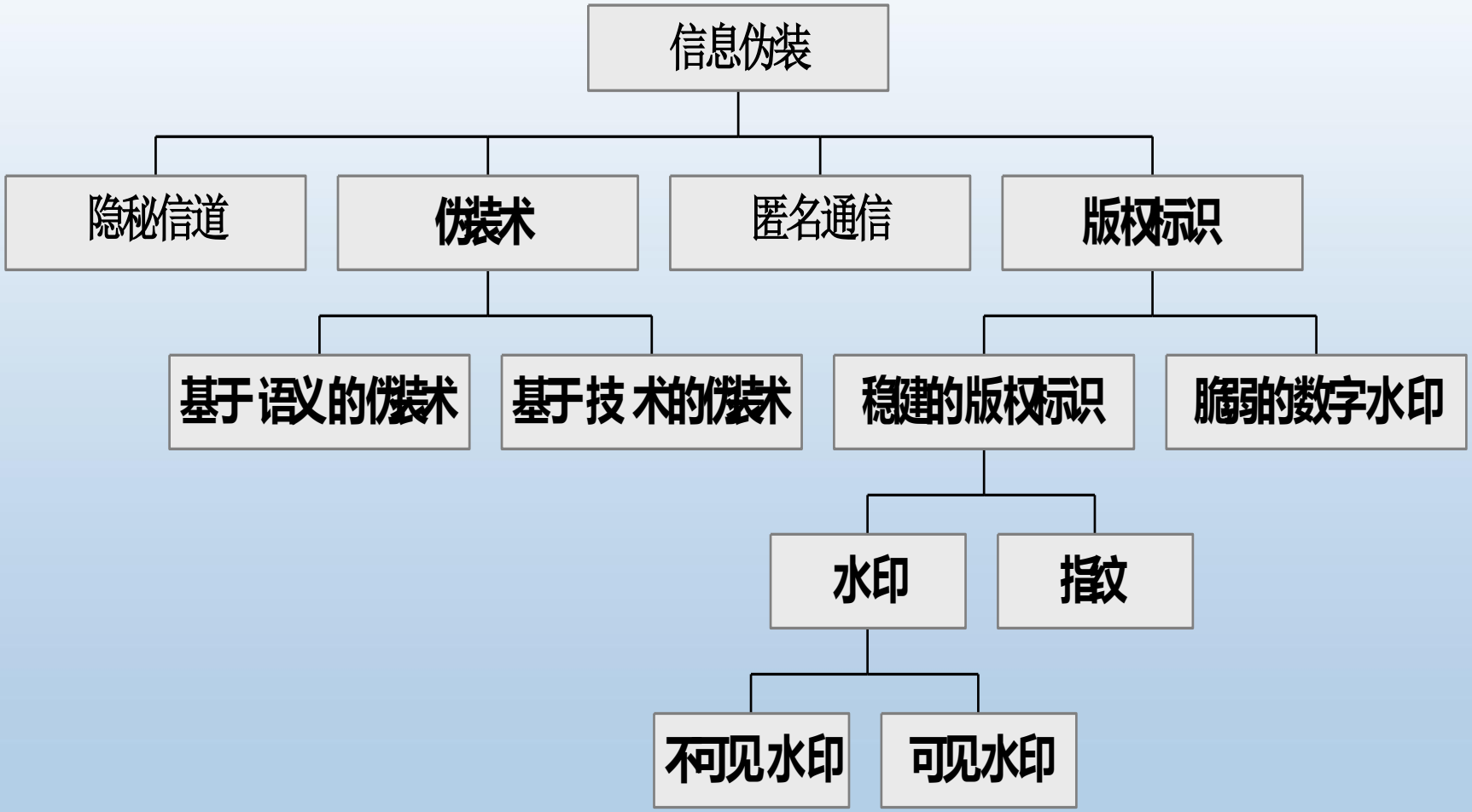
信息隐藏的思想

- 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（视觉理论、听觉理论）
  - 现代通信技术
  - 密码技术

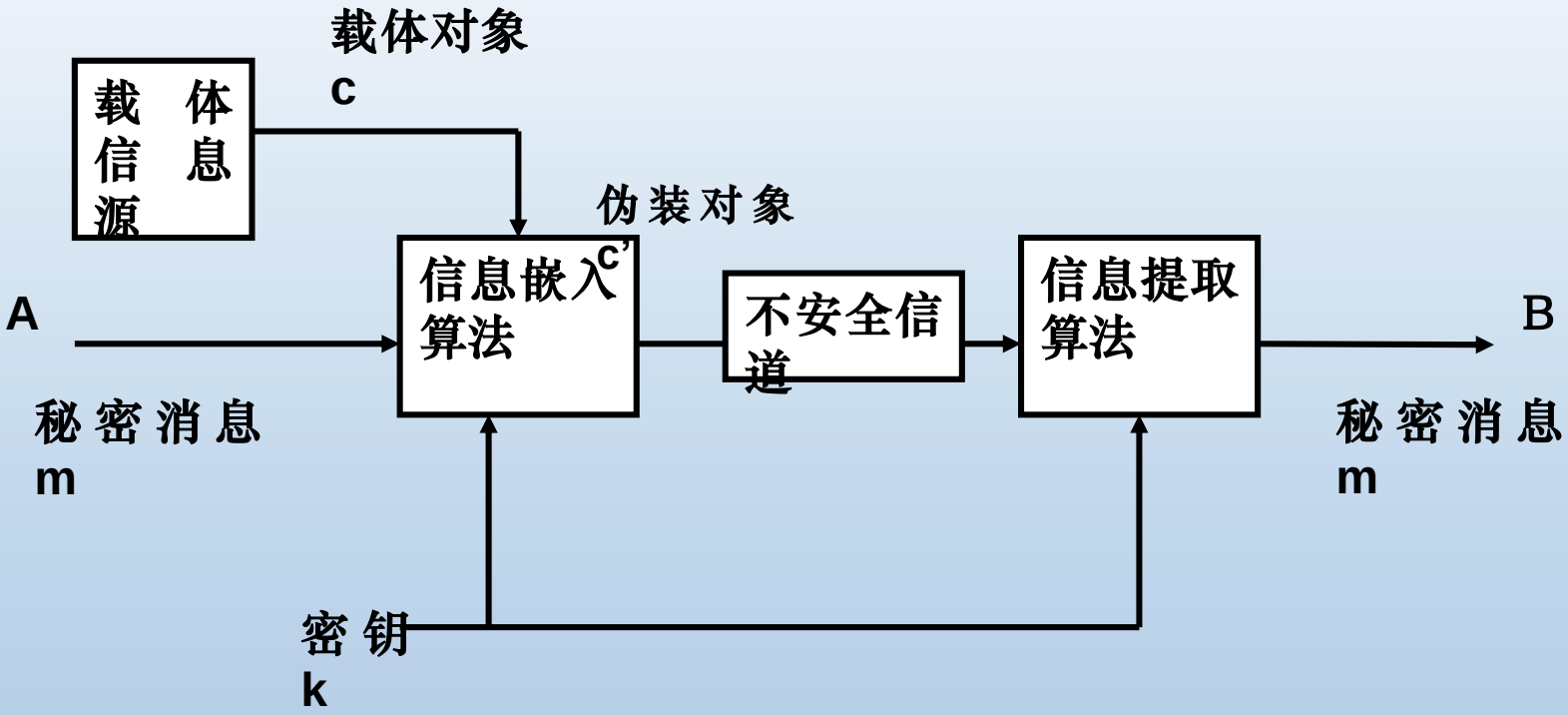
  等为代表的伪装式信息隐藏方法来研究信息的保密和安全问题

- **隐藏者**
  - 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
- **攻击者**
  - 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

信息伪装技术的分类


信息伪装
隐秘信道
伪装术
匿名通信
版权标识
基于语义的伪装术
基于技术的伪装术
稳健的版权标识
脆弱的数字水印
水印
指纹
不可见水印
可见水印

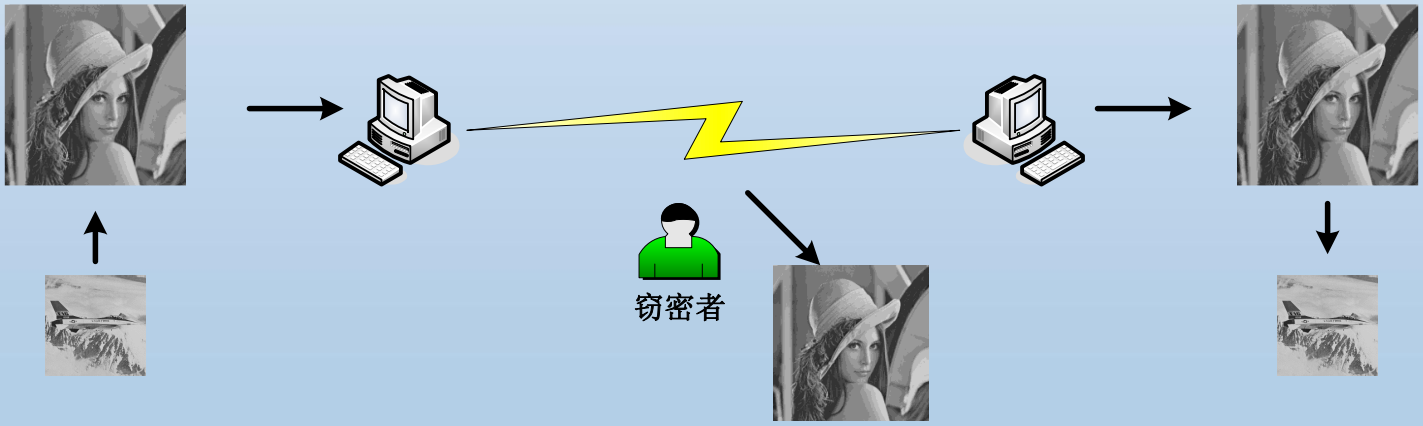
信息隐藏原理框图



信息隐藏的原理框图

实现信息隐藏的基本要求

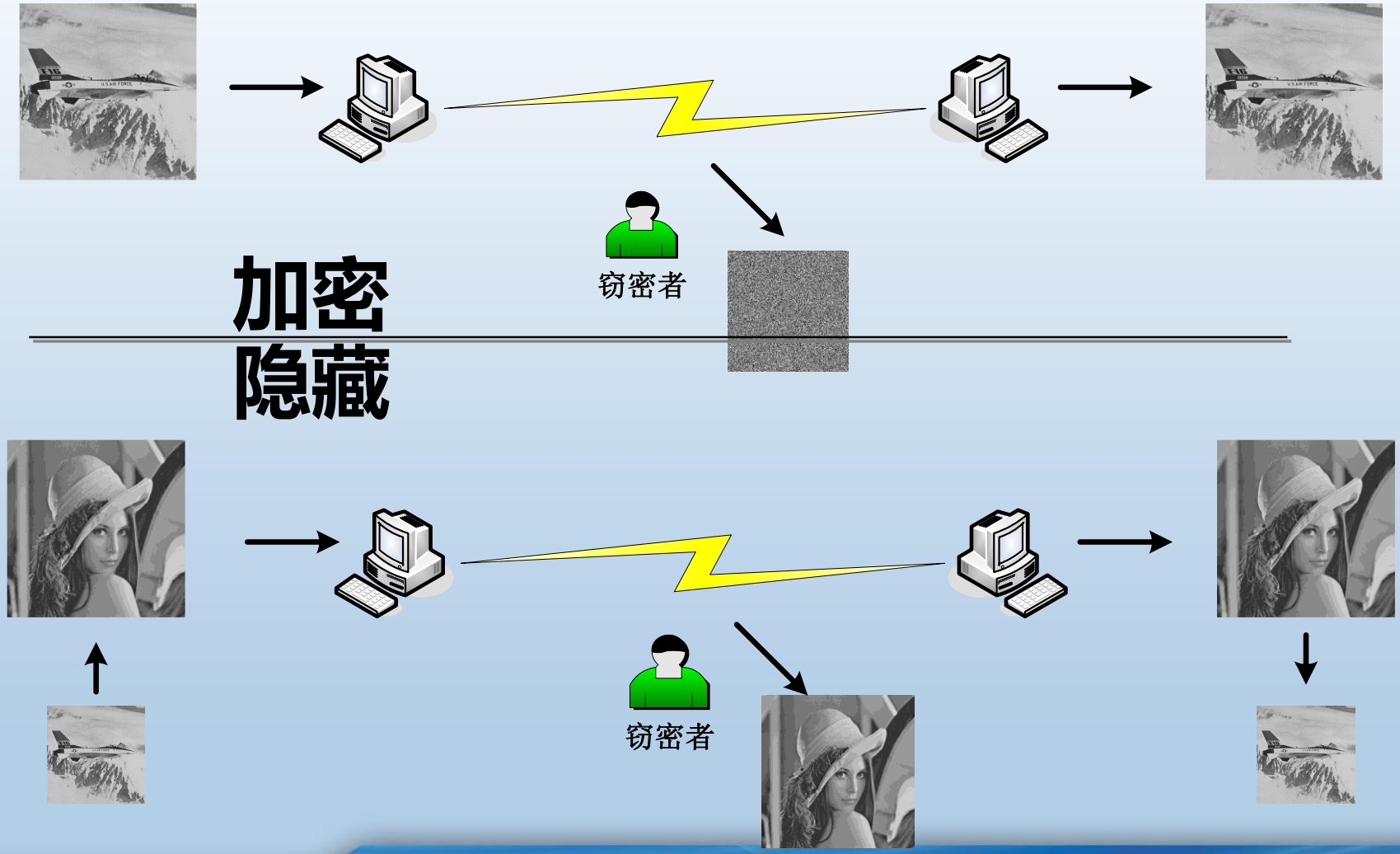
- 载体对象是正常的，不会引起怀疑
- 不可视通信的**安全性**取决于第三方**有没有能力**将载体对象和伪装对象区别开来
- 对伪装对象的正常处理，不应破坏隐藏的信息



隐写术 - 伪装式保密通信

- 利用人类感知系统以及计算机处理系统的冗余
- 载体可以是任何一种多媒体数据，如音频、视频、图像、甚至文本、数据等
- 被隐藏的信息也可以是任何形式（全部作为比特流）
- 主要用于军队和安全部门

隐蔽通信的例子



信息隐藏的主要分支

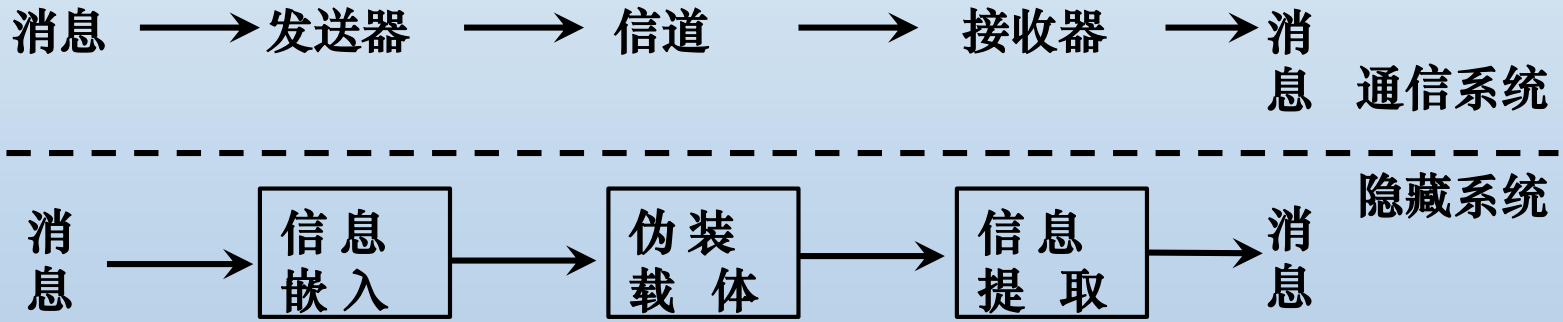
- 隐写术－伪装式保密通信
- 数字水印－数字产品版权保护

信息隐藏的通信模型

- 目前对信息隐藏的理论研究还不充分
  - 缺乏像Shannon通信理论这样的理论基础
  - 缺乏对人类感知模型的充分理解
  - 缺乏对信息隐藏方案的有效度量方法等
- 目前一种研究方法是：将信息隐藏过程类比 于隐蔽信息的通信过程

隐藏系统与通信系统的比较

- 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



隐藏系统与通信系统的比较

- 目标相同：都是向某种媒介（称为信道）中 引入一些信息，然后尽可能可靠地将该信息 提取出来
- 约束条件：
  - 通信系统：最大的平均功率或峰值功率约束
  - 隐藏系统：感官约束

隐藏系统与通信系统的比较

- 信道干扰
  - 通信系统：主要为传输媒介的干扰，如设备噪声、 大气环境干扰等
  - 隐藏系统：不只受到无意的干扰，还受到各种主 动攻击
  - 隐藏系统：已知更多的信道信息（载体信号是已 知的）

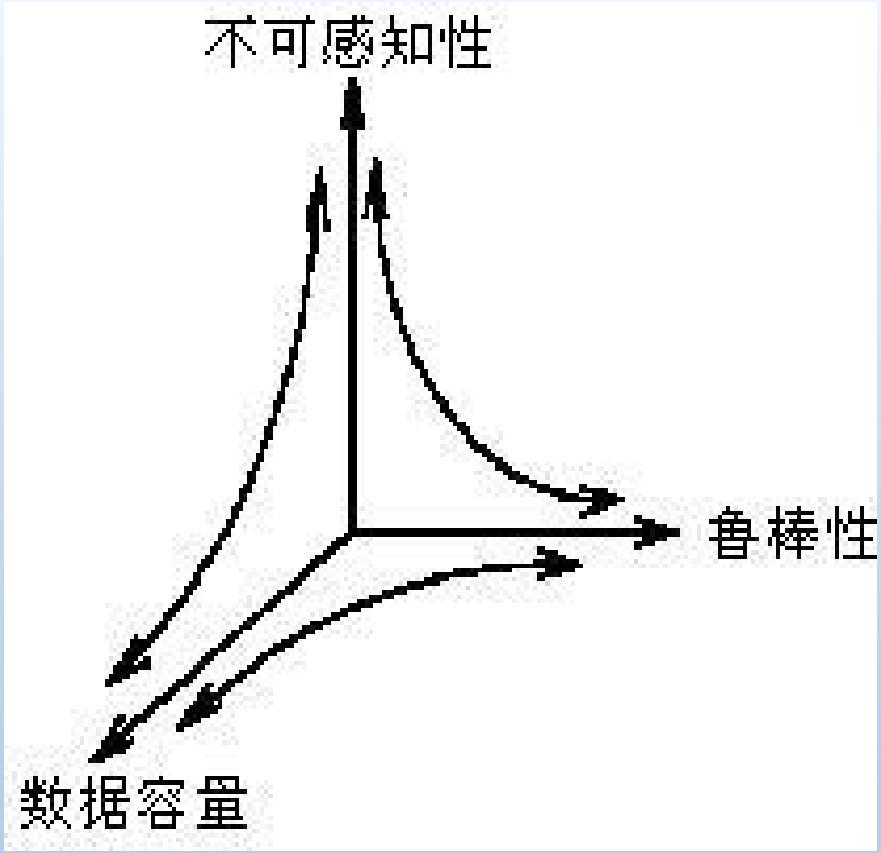
信息隐藏的安全性

- 信息隐藏系统的安全性
  - 系统自身算法的安全性
  - 各种攻击情况下的安全性
- 攻击一个信息隐藏系统
  - 证明隐藏信息的存在
  - 破坏隐藏信息
  - 提取隐藏信息
- 理论安全的：如果能够证明其安全性
- 现实安全的：如果攻击者经过各种方法仍然不能判断 是否有信息隐藏

信息隐藏的攻击

- 被动攻击
  - 监视和破译隐藏的秘密信息
- 主动攻击
  - 破坏隐藏的秘密信息
  - 篡改秘密信息
- 非恶意修改
  - 压缩编码，信号处理技术，格式转换，等

安全性、鲁棒性和容量之间的关系



信息隐藏的应用

- 军事和情报部门
  - 现代化战争的胜负，越来越取决于对信息的掌握 和控制权
  - 军事通信中通常使用诸如扩展频谱调制或流星散 射传输的技术使得信号很难被敌方检测到或破坏 掉
  - 信息隐藏正是可以达到不被敌方检测和破坏的目 的

信息隐藏的应用

- 需要匿名的场合
  - 包括很多合法的行为，如公平的在线选举、个人 隐私的安全传递、保护在线自由发言、使用电子 现金等
  - 非法的行为，如诽谤、敲诈勒索以及假冒的商业 购买行为
  - 在信息隐藏技术的应用中，使用者的伦理道德水 平并不是很清楚，所以提供信息隐藏技术时需要 仔细考虑并尽量避免可能的滥用

- 美国9.11恐怖袭击事件发生前不久，“USA Today”有报道称在1998年两座东非美国大使馆的炸弹攻击事件中，拉登等人曾利用聊天室、色情BBS等网站隐藏恐怖攻击目标的地图和照片，并下达恐怖活动的指示。在9.11事件发生之后，“Wired News”上也有文章指出恐怖分子在eBay和Amazon等拍卖网站上利用数字图像作为载体进行隐密通信。

方向之二：

数字水印

数字水印

- 信息隐藏在民用领域的应用：数字水印
- 数字作品的特点：无失真复制、传播，易修改，易发表
- 数字作品的版权保护需要：
  - 确定、鉴别作者的版权声明
  - 追踪盗版
  - 拷贝保护

信息隐藏与数字水印的关系

- 数字水印是广义信息隐藏的一个分支
- 实现数字版权管理（DRM）

数字水印的定义

- 水印
  - 存在于纸张、纸币中，用于标识真伪
- 数字水印
  - 对数字产品标识真伪
  - 数字图书馆、网络音频和视频、数字地图等
- 数字水印的定义
  - 数字水印是永久镶嵌在其他数据（宿主数据）中具有可鉴别性的数字信号或模式，并且不影响宿主数据的可用性

数字水印的特点

- 数字水印的特点
  - 安全性
    - 数字水印难以被发现、擦除、篡改或伪造，同 时，要有较低的虚警率
  - 可证明性
    - 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
- 不可感知性
  - 从感官上和统计上都不可感知

数字水印的特点

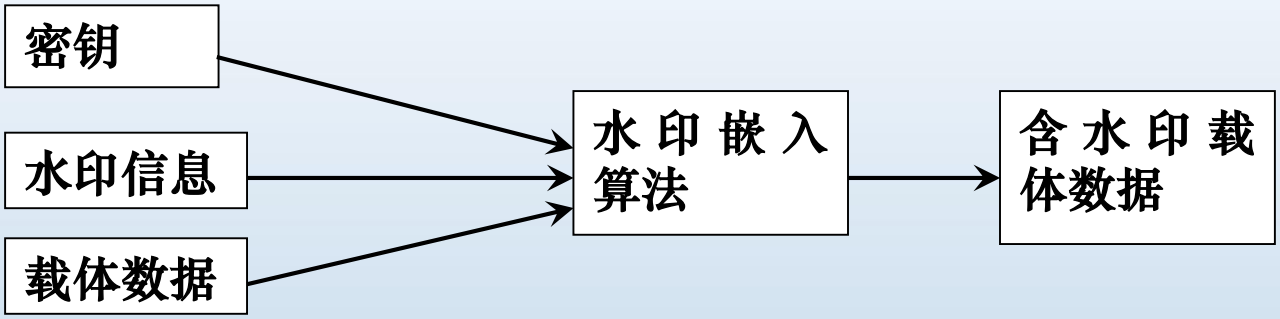
- 稳健性
  - 数字水印应该难以被擦除，任何试图完全破坏水印的努力将对载体的质量产生严重破坏
  - 好的水印算法应该对信号处理、几何变形、恶意攻击等具有稳健性
- 脆弱性（完全脆弱性，半脆弱性）

数字水印三要素

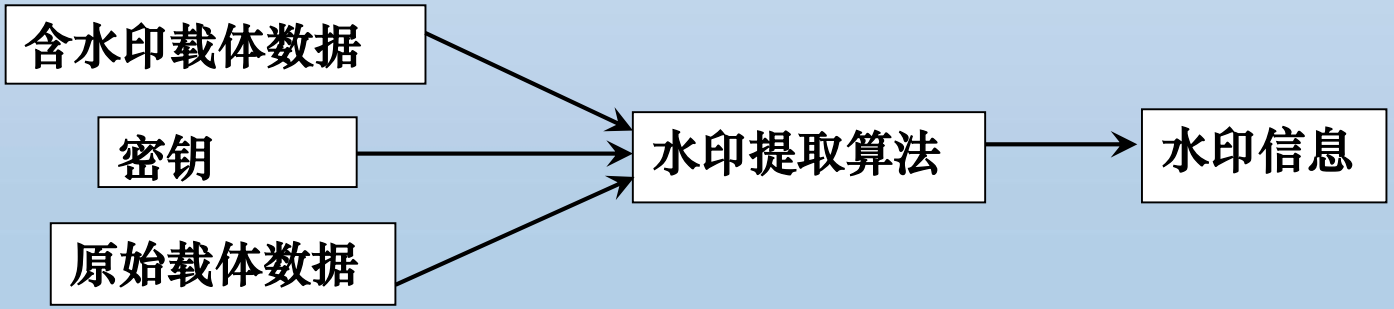
- 水印本身的结构
  - 版权所有者、合法使用者等具体信息
  - 伪随机序列
  - 图标
- 水印嵌入算法
- 水印检测算法

数字水印嵌入和提取模型

水印嵌入模型



水印提取模型



数字水印的分类

- 从载体上分类
- 从外观上分类
- 从加载方式上分类
- 从检测方法上分类
- 从水印特性上分类
- 从使用目的上分类

从载体上分类

- 图像水印
  - 图像是使用最多的一种多媒体数据，也是经常引起版权纠纷的一类载体
  - 彩色/灰度图像，卡通，设计图，二值图像（徽标、文字），等
- 视频水印
  - 保护视频产品和节目制作者的合法利益
- 音频水印
  - 保护MP3、CD、广播电台的节目内容等
- 文档水印
  - 确定文档数据的所有者

从外观上分类

- 可见水印（可察觉水印）
  - 如电视节目上的半透明标识，其目的在于明确标识版权，防止非法的使用，虽然降低了资料的商业价值，却无损于所有者的使用
- 不可见水印（不可察觉水印）
  - 水印在视觉上不可见，目的是为了将来起诉非法使用者。不可见水印往往用在商业用的高质量图像上，而且往往配合数据解密技术一同使用

从加载方式上分类

- 空间域水印
  - LSB方法
  - 拼凑方法
  - 文档结构微调方法
- 变换域水印
  - DCT变换，小波变换，傅立叶变换，Fourier-Mellin变换或其它变换

从检测方法上分类

- 私有水印和公开水印
  - 私有水印（非盲水印）：水印检测时需要原始载 体
  - 公开水印（盲水印）：水印检测时无需原始载体
- 私钥水印和公钥水印
  - 私钥水印：水印加载和检测使用同一密钥
  - 公钥水印：水印加载和检测使用不同的密钥（同 密码学中的公钥密码）

从水印特性上分类

- 健壮性数字水印
  - 要求水印能够经受各种常用的操作，包括无意的或恶意的处 理
  - 只要载体信号没有被破坏到不可使用的程度，都应该能够检 测出水印信息
- 脆弱性数字水印（完全脆弱性/半脆弱性）
  - 要求水印对载体的变化很敏感，根据水印的状态来判断数据 是否被篡改过
  - 特点：载体数据经过很微小的处理后，水印就会被改变或毁 掉
  - 主要用于完整性保护
  - 与稳健性水印的要求相反

脆弱性数字水印 示例

原始图像

含水印图像

脆弱性数字水印 示例——JPEG有损压缩

认为没有内容篡改

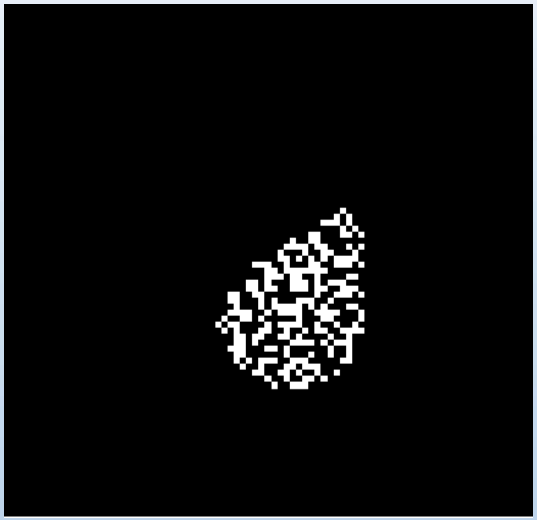
不同JPEG压缩比下篡改率

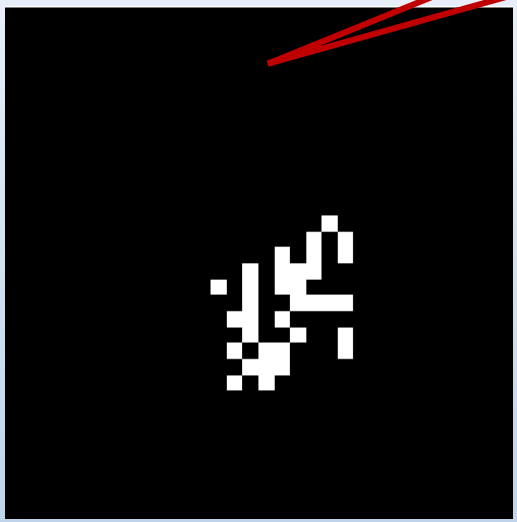
JPEG 压 缩 质量	第一级	第二级	第三级	第四级
90	0	0	0	0
80	0.0251	0	0	0
70	0.1409	0	0	0
60	0.2486	0.0125	0.0078	0

结论：当压缩质量为60时，图像的低频部分的篡改率仍为0，认为是可信的。即该算法能够抵抗JPEG压缩

脆弱性数字水印 示例——局部篡改

指出内容篡改区域

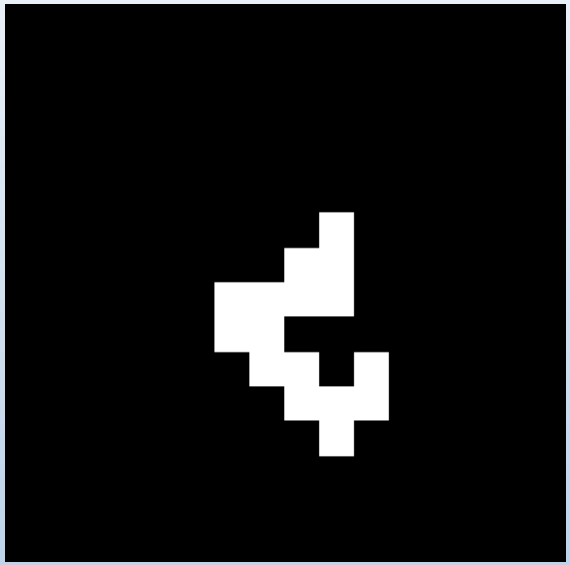




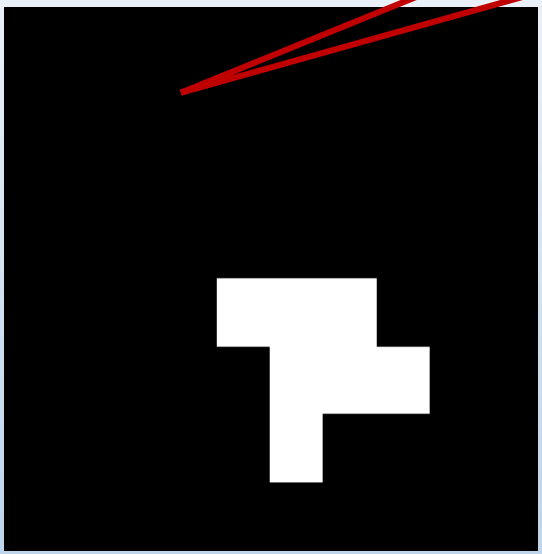
第一层　　第二层

不同小波层上进行失真检测的结果

指出内容篡改区域



第三层



第四层

结论：该算法能够区分常用的图像处理操作和恶意攻击，并且能很好地定位出图像的篡改位置

从使用目的上分类

- 版权标识水印
  - 基于数据源的水印
  - 水印信息标识作者、所有者、发行者等，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
- 数字指纹水印
  - 基于数据目的的水印
  - 包含关于本件产品的版权信息，以及购买者的个人信息，可以用于防止数字产品的非法拷贝和非法传播

数字水印的应用

- 版权保护：表明对数字产品的所有权
- 数字指纹：用于防止数字产品被非法复制和 散发
- 认证和完整性校验：验证数字内容未被修改 或假冒
- 内容标识和隐藏标识：多媒体内容检索
- 使用控制：控制复制次数
- 内容保护：保护内容不被滥用

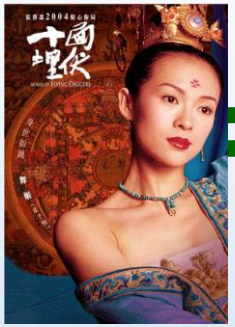
数字水印的应用

- 信息隐藏在民用领域的应用：数字水印
- 数字作品的特点：无失真复制、传播，易修改，易发表
- 数字作品的版权保护需要：
  - 确定、鉴别作者的版权声明
  - 追踪盗版
  - 拷贝保护

数字水印的应用

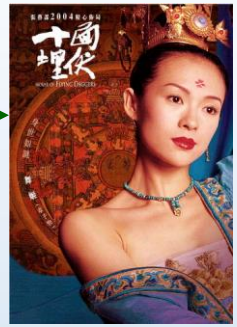
- 用于**版权保护**的数字水印：将版权所有者的信息，嵌入在要保护的数字多媒体作品中，从而防止其他团体对该作品宣称拥有版权
- 用于**盗版跟踪**的数字指纹：同一个作品被不同用户买去，售出时不仅嵌入了版权所有者信息，而且还嵌入了购买者信息，如果市场上发现盗版，可以识别盗版者
- 用于**拷贝保护**的数字水印：水印与作品的使用工具相结合（如软硬件播放器等），使得盗版的作品无法使用

版权管理的例子



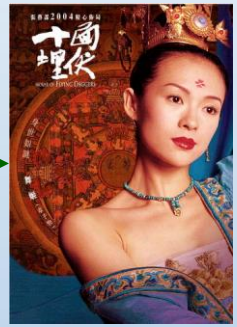
版权所有：

新画面影业公司



拷贝持有者：

新东安影院



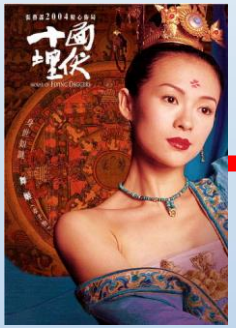
拷贝持有者：

东方新世纪影院

.....

拷贝持有者：

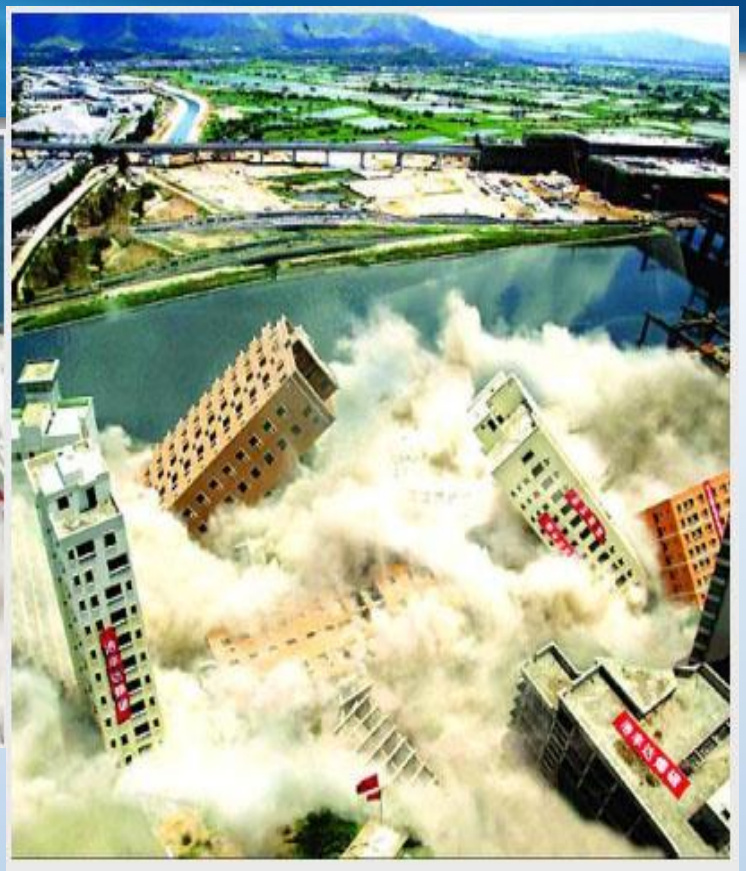
音像制作公司



盗版影碟

盗版来源是谁?

其他例子



爆炸当天发回图片（左）和“华赛”金奖作品（右）

2006年第二届中国国际新闻摄影比赛（简称“华赛”）爆出了最大新闻：获得经济与科技新闻类单幅金奖的作品《中国农村城市化改革第一爆》疑为合成作品，经组委会认定后最终被取消金奖获奖资格。

- 2007年底至2008年上半年，连续爆出的“华南虎”造假事件、“藏羚羊”照片事件和“广场鸽”照片造假更是打碎了不少人长期以来对影像真实性的信心

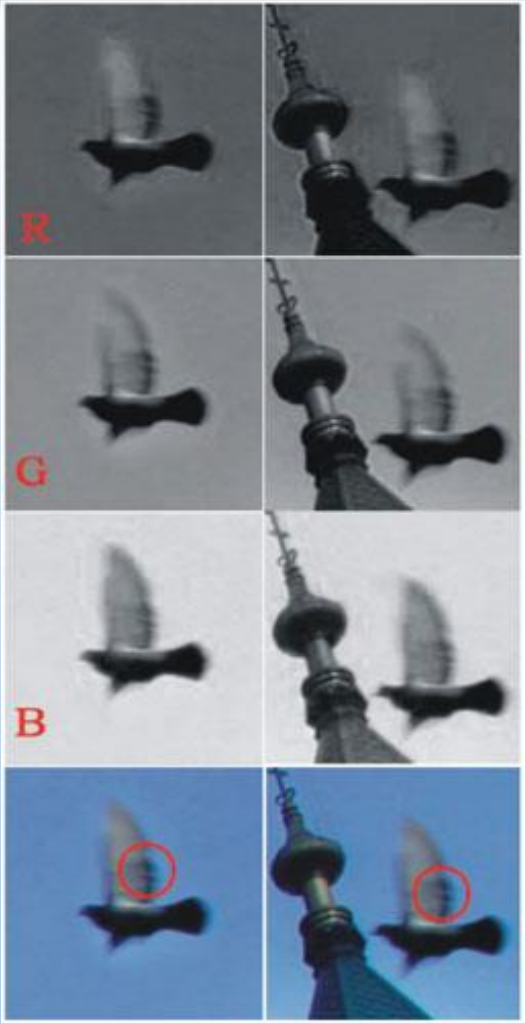
网友指出的三大疑点

①网友发现此处有红色拼接线

②火车经过时，藏羚羊依然呈直线前进，与其易受惊吓的习性不符

③两张拍摄于不同月份的照片中，两块石头的形状和角度几乎一模一样

图解飞鸽————华赛金奖照片《广场鸽接种禽流感疫苗》涉嫌造假事件调查报告



两只鸽子系拷贝合成的数学证明过程:

A.任意两只鸽子一模一样的概率趋于0;

B.相同的两只鸽子飞行姿态一模一样的概率趋于0;

C.相同鸽子在不同位置于镜头中成像相同的概率趋于0;

以上三个事件是小概率事件，多个独立事件同时发生的概率为各自发生概率的乘积，本例中这将是一个极小的概率。

在现实生活中，如果小概率事件接二连三地发生，则可以判定为“假”。

- 结论：

两只鸽子系“克隆”可经数学证明，只能以拷贝来解释。

这个拷贝最明显，引起大家关注，但实际与其它的拼合行为比，这个算是轻的了。

网络链接：http://www.xitek.com/forum/showthread.php?threadid=507096 No.8 “克隆鸽”

数字水印的研究方向

- 理论
  - 数字水印模型、隐藏容量、抗攻击性能等
- 算法
  - 研究具有更高性能的水印算法
- 标准
  - 真正起到数字版权管理的作用，还需要完善一系 列的标准和协议

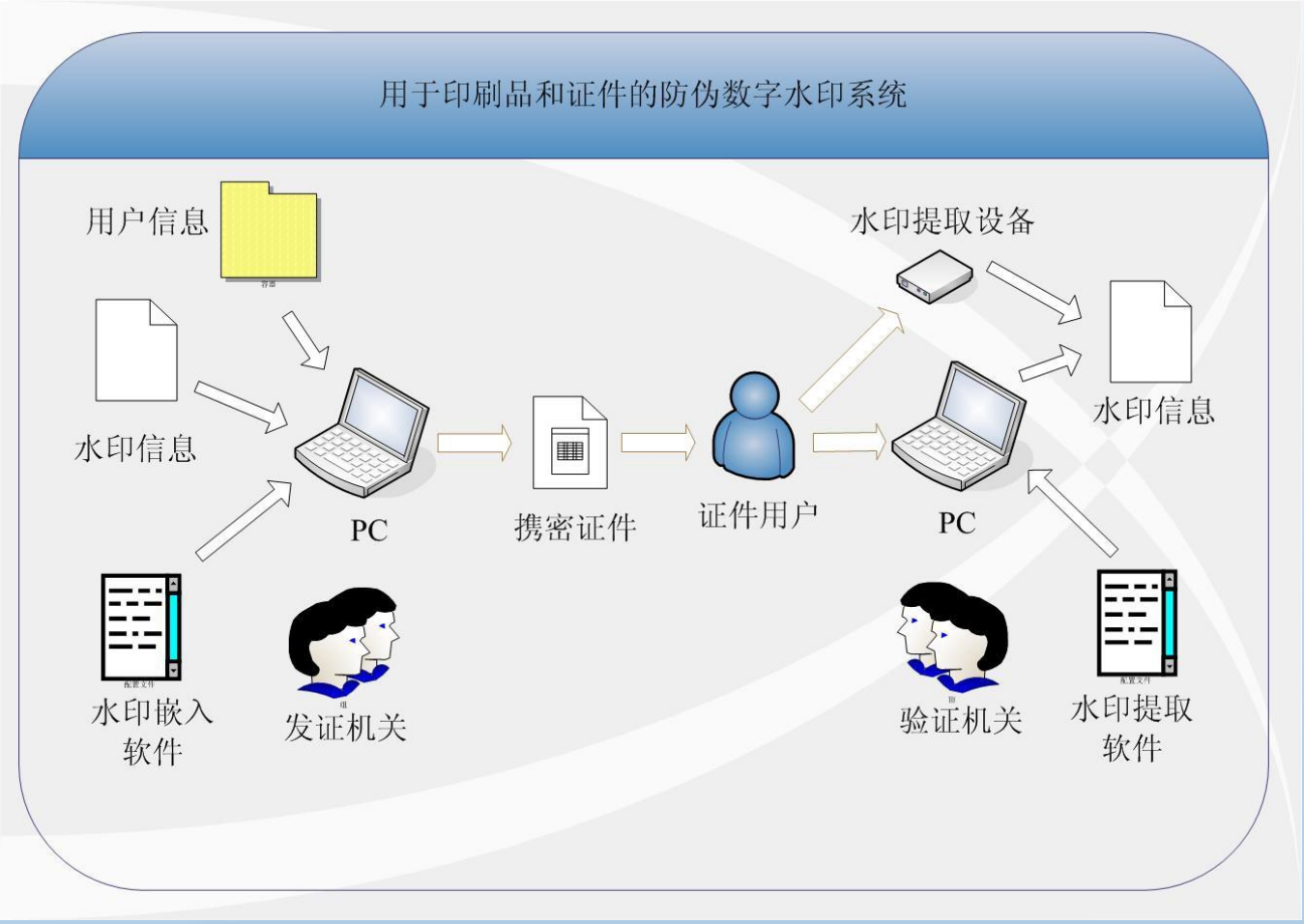
信息隐藏与数字水印的区别

	信息隐藏	数字水印
用途	用于保密通信	用于版权标识
前提	一般不知有信息隐藏（如　果已怀疑有隐藏信息，则　已经不安全）	可以公布有水印存在
主要攻击	隐写分析（分析是否正常　载体）	水印擦除
主要考核	透明性	鲁棒性

主要应用示例

- 用于印刷品和证件防伪的数字水印技术
- 地理信息水印系统
- 数字作品版权管理系统
- 互联网数字水印检测工具

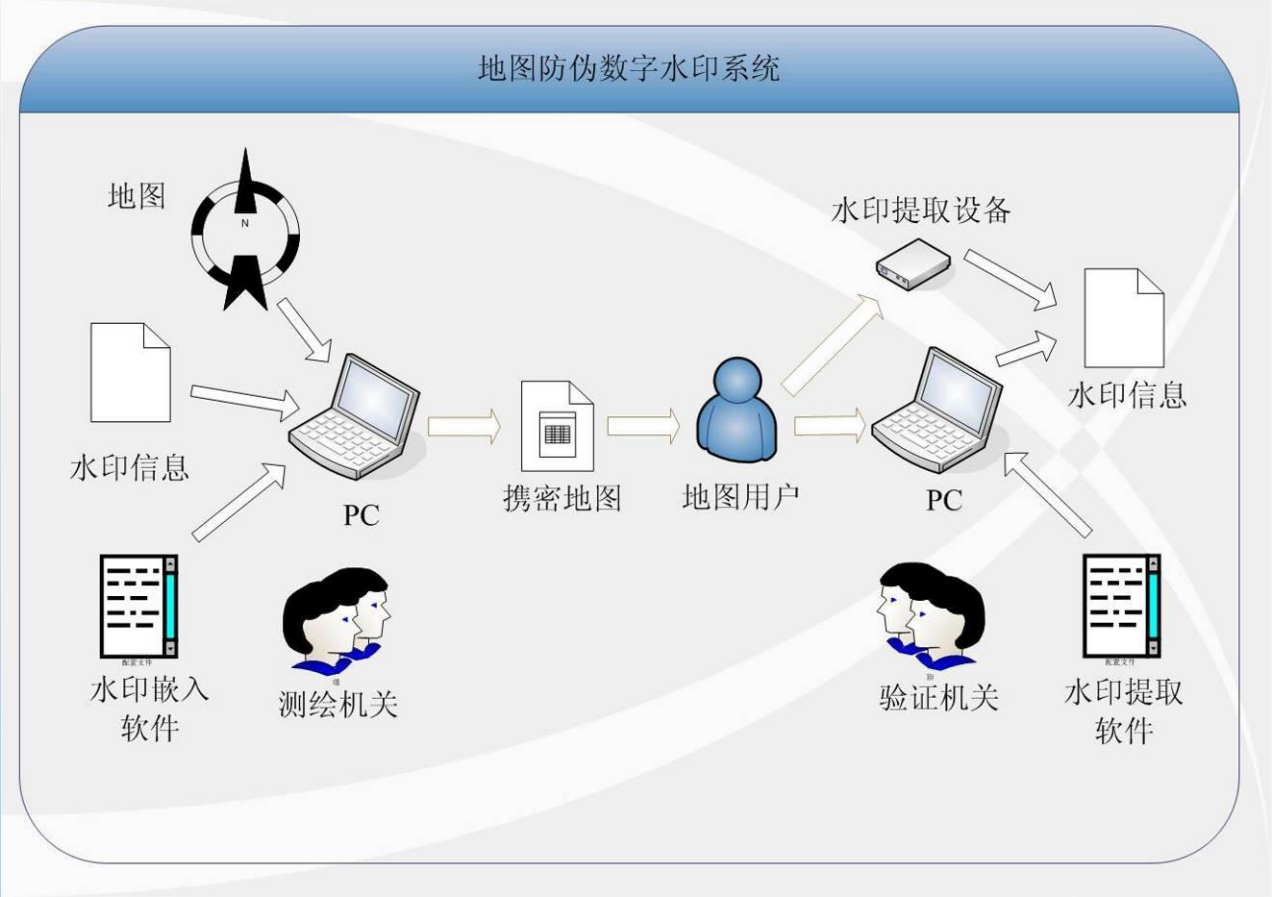
- **用于印刷品和证件防伪的数字水印技术**



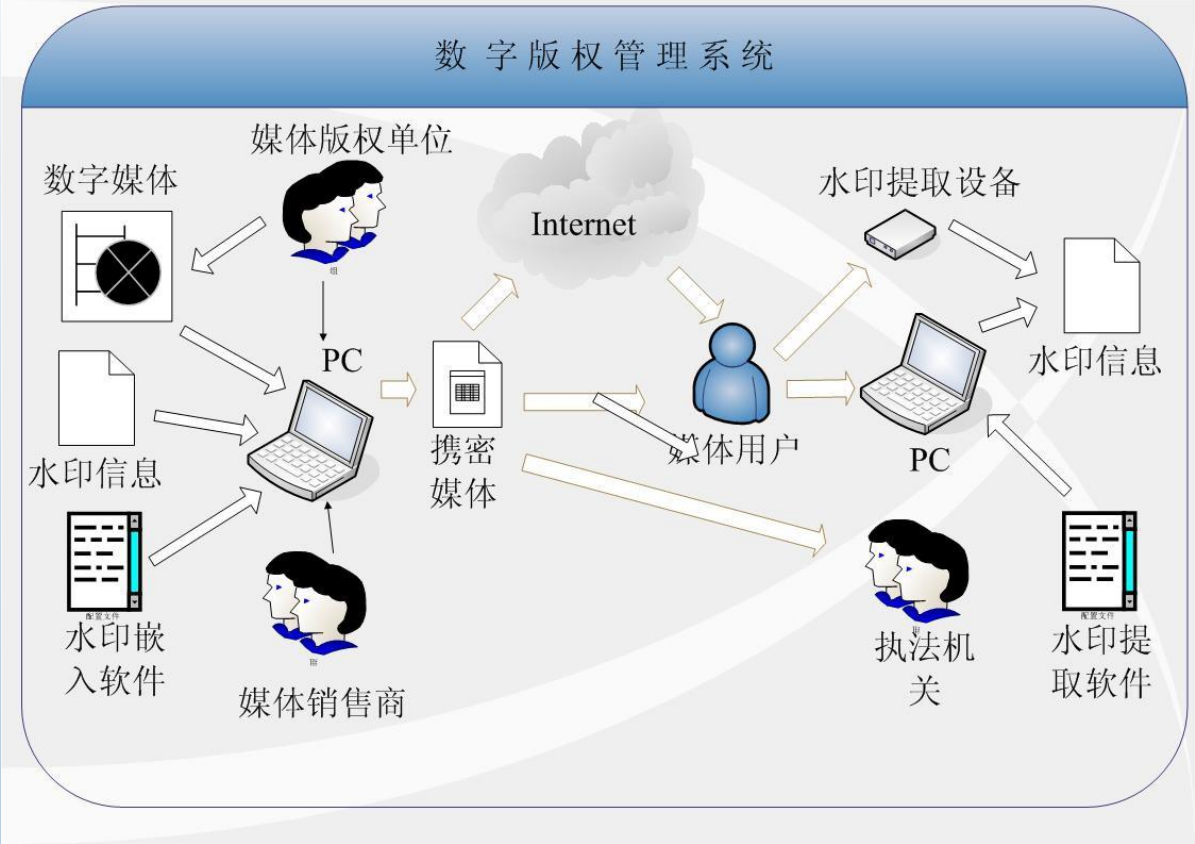
- **用于印刷品和证件防伪的数字水印技术**

证件防伪技术用于2006青岛 国际帆船赛证件制作系统（制作防伪证件6000多张）

- **地理信息水印系统**


地图防伪数字水印系统
地图
水印信息
水印嵌入软件
PC
测绘机关
携密地图
地图用户
水印提取设备
PC
验证机关
水印信息
水印提取软件

- **数字作品版权管理系统**


数字版权管理系统
媒体版权单位
数字媒体
Internet
水印提取设备
PC
水印信息
水印信息
携密媒体
媒体用户
PC
水印嵌入软件
媒体销售商
执法机关
水印提取软件

- **互联网数字水印检测工具**