信息隐藏技术

Information Hiding Technique

主讲人: 王宏霞

E-mail:hxwang@swjtu.edu.cn

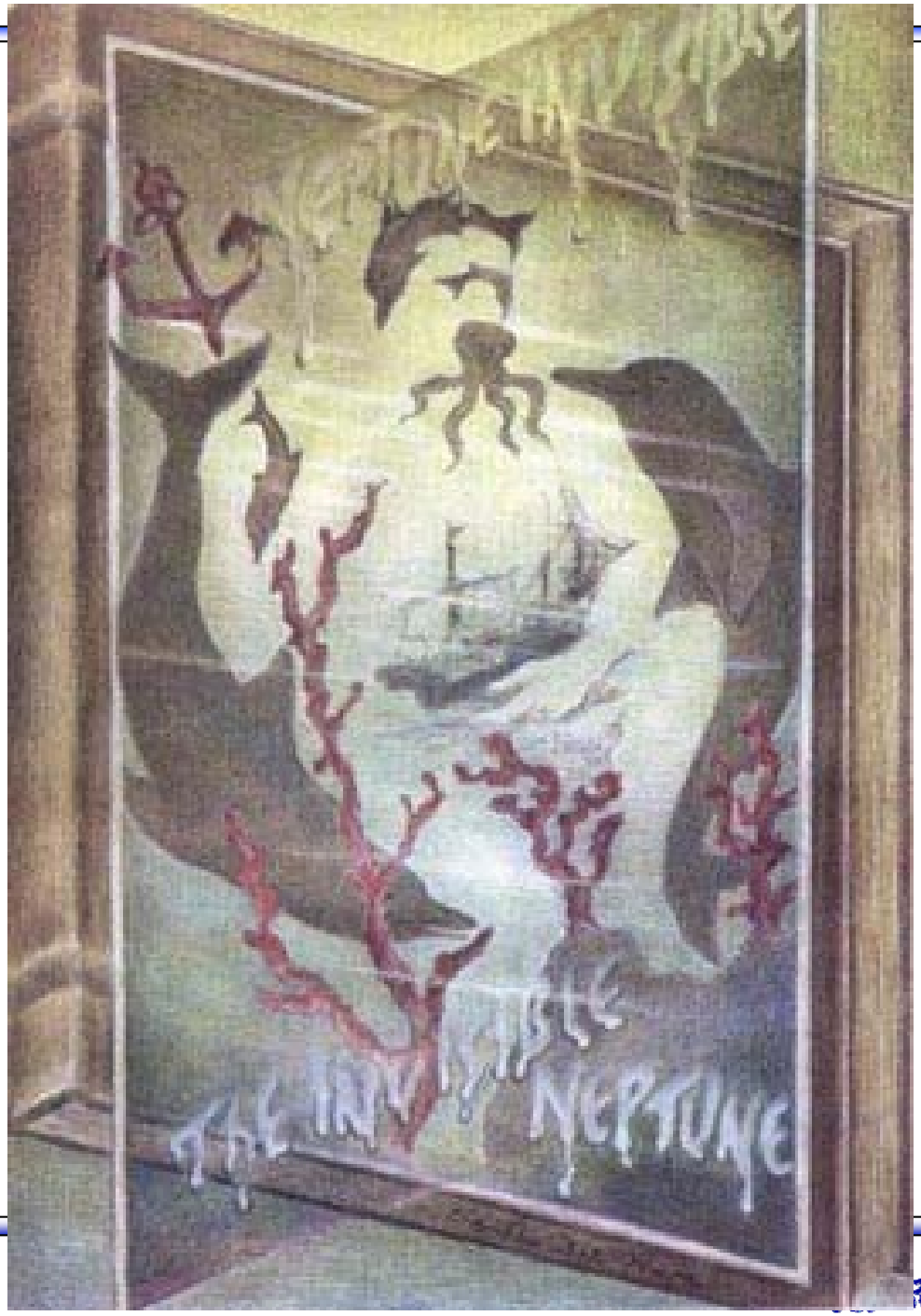
2018/3/18

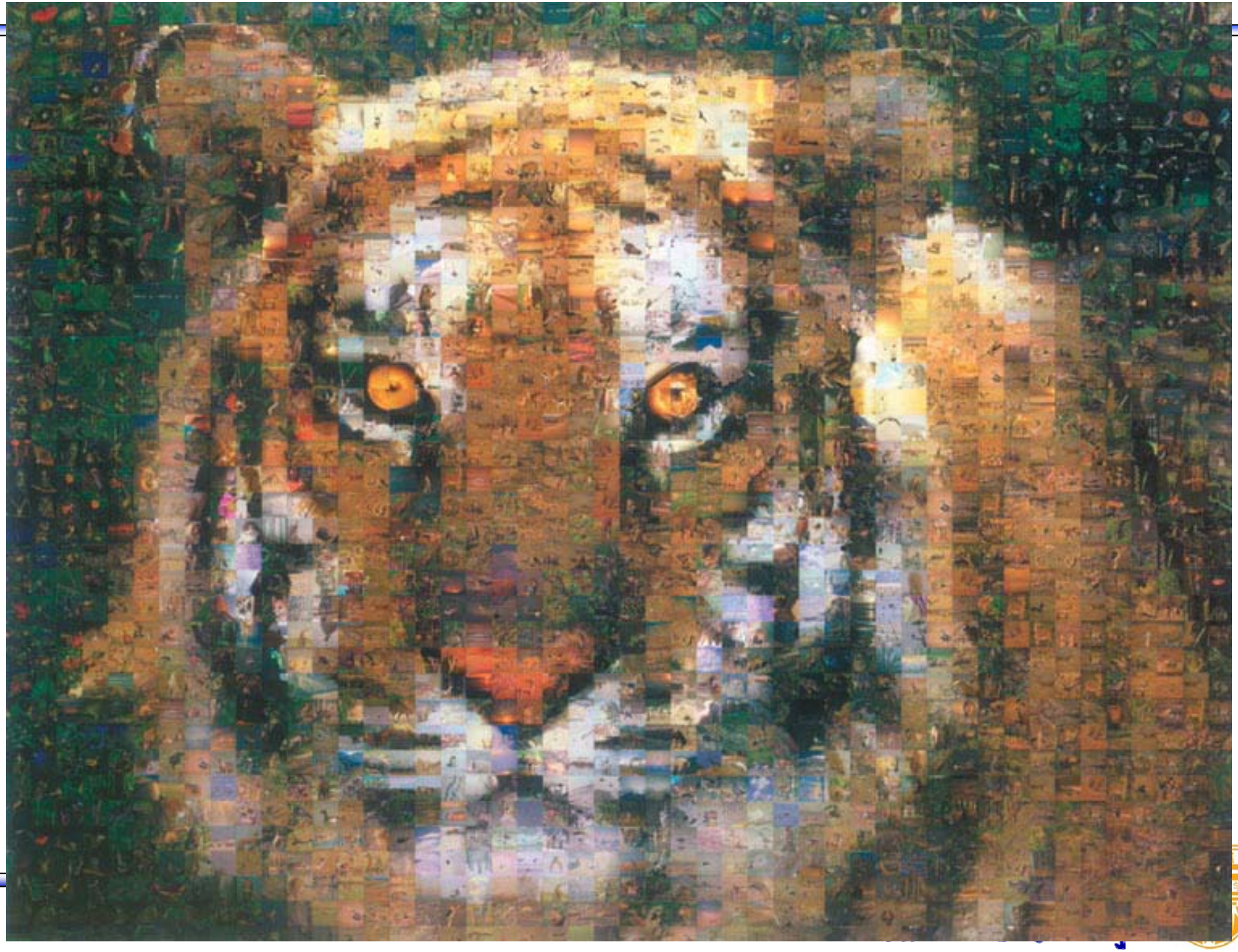
第一章　绪论


八目妖 haha168.com

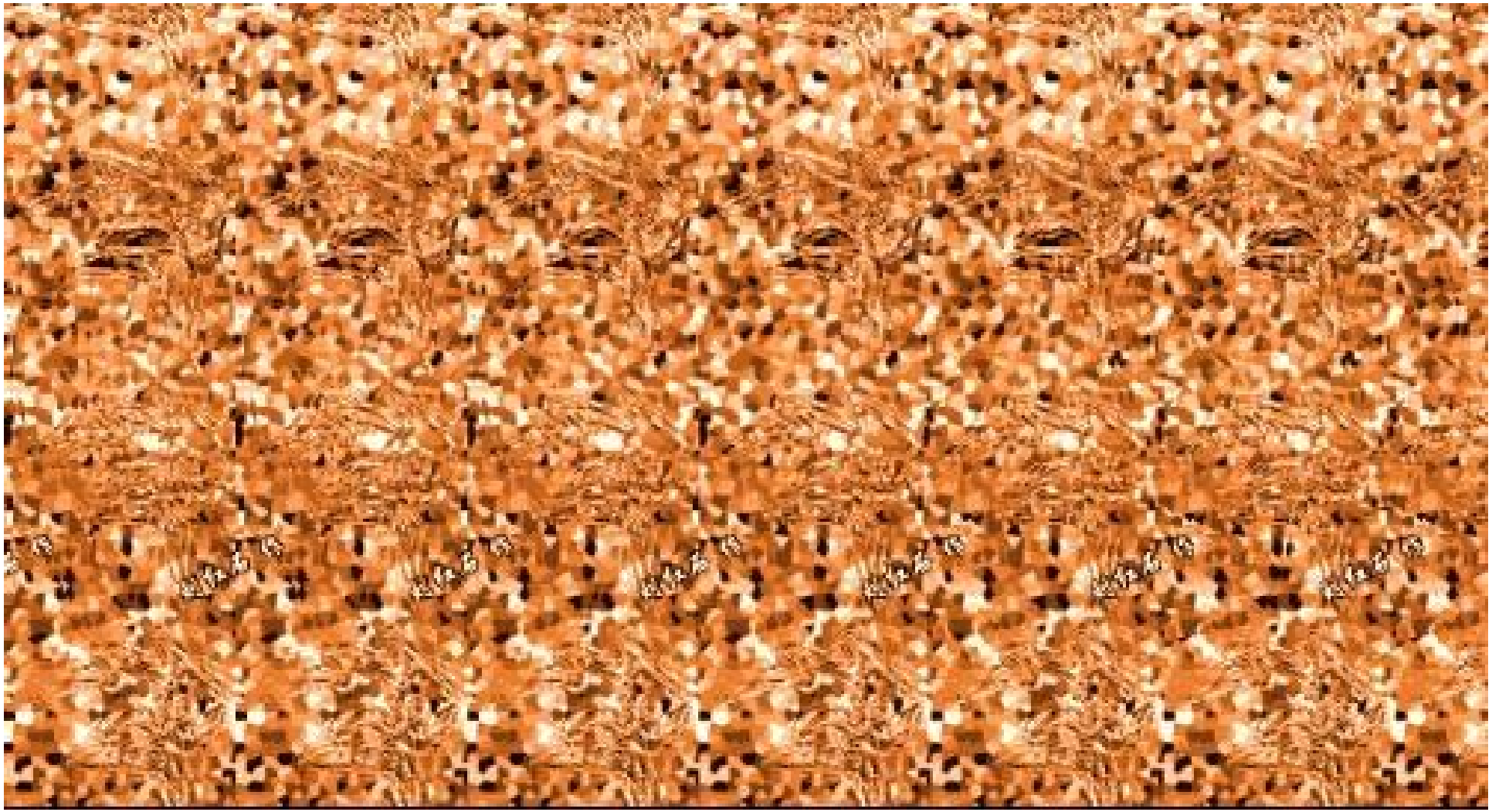
爱因斯坦吗？我看到的可是三个MM洗澡～

你能找到保卫海洋的海神尼普顿的像吗？





奥运五环



推荐书籍和文献

- 书籍:
  1. 曹云飞，王宏霞，熊玲. 信息隐藏理论与实践，国防工业出版社，2018.
  2. 王朔中，张新鹏，张开文. 数字密写和密写分析，清华大学出版社，2005.
- 文献:
  IEEE/IET, SDOS和中国的CNKI数据库

- 网址:
  - 台湾中正大学多媒体暨网络安全实验室 http://140.134.50.88/
  - 台湾国立中兴大学资讯科学系网络多媒体实验室 http://nmlab.cs.nchu.edu.tw/
  - 中国科技大学多媒体技术与网络通信实验室 http://202.38.75.33/
  - 台湾长荣大学科技工程与管理系 http://www.cvig.org/
  - 台湾成功大学-多媒体与人机通讯实验室 http://chinese.csie.ncku.edu.tw/
    韩国: http://www.ijcsns.org
  - 美国State University of New York at Binghamton
    http://dde.binghamton.edu/download/feature_extractors/,
    http://dde.binghamton.edu/download/ensemble

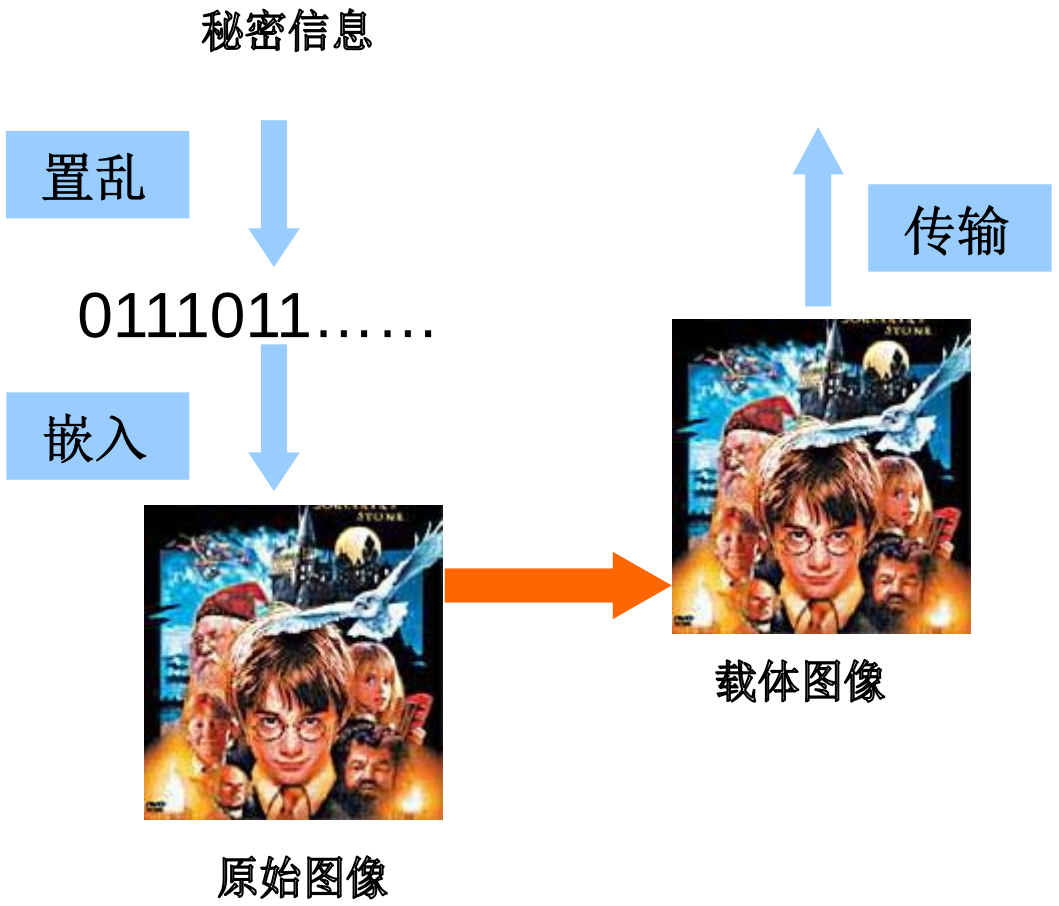
信息隐藏技术术语

- 信息隐藏是利用人类感觉器官对数字信号的感觉冗余，将一个信息（称为待隐藏信息或秘密信息,Secure Message）隐藏在另一个公开信息（称为遮掩信息或载体,Cover Message）中，信息因此而受到保护.
- 秘密信息(Secure Message): 版权信息、秘密数据、序列号...
- 载体信息(Cover Message): 图像、视频、音频、文本...
- 信息隐藏系统一般由密钥 (Key) 控制，即通过嵌入算法 (Embedding Algorithm) 将秘密信息隐藏于公开信息中，而隐藏载体则通过信道 (Communication Channel) 传递，在接收端用检测器从载体中提取或检测秘密信息。

信息隐藏技术术语

- 由于在隐藏后外部表现的只是遮掩信息的外部特征，故并不改变遮掩信息的基本特征和使用价值。
- 信息隐藏方法的最大特点是：除了被通知的有关方面以外的任何人都不知道秘密信息存在这个事实，这就较之单纯的加密方法更多了一层保护，使得需要保护的消息由“看不懂”变为了“看不见”。

信息隐藏技术通信模型



信息隐藏模型发送端

信息隐藏技术通信模型

载体图像

检测

是否含有秘密信息？

提取

0111011……

反置乱

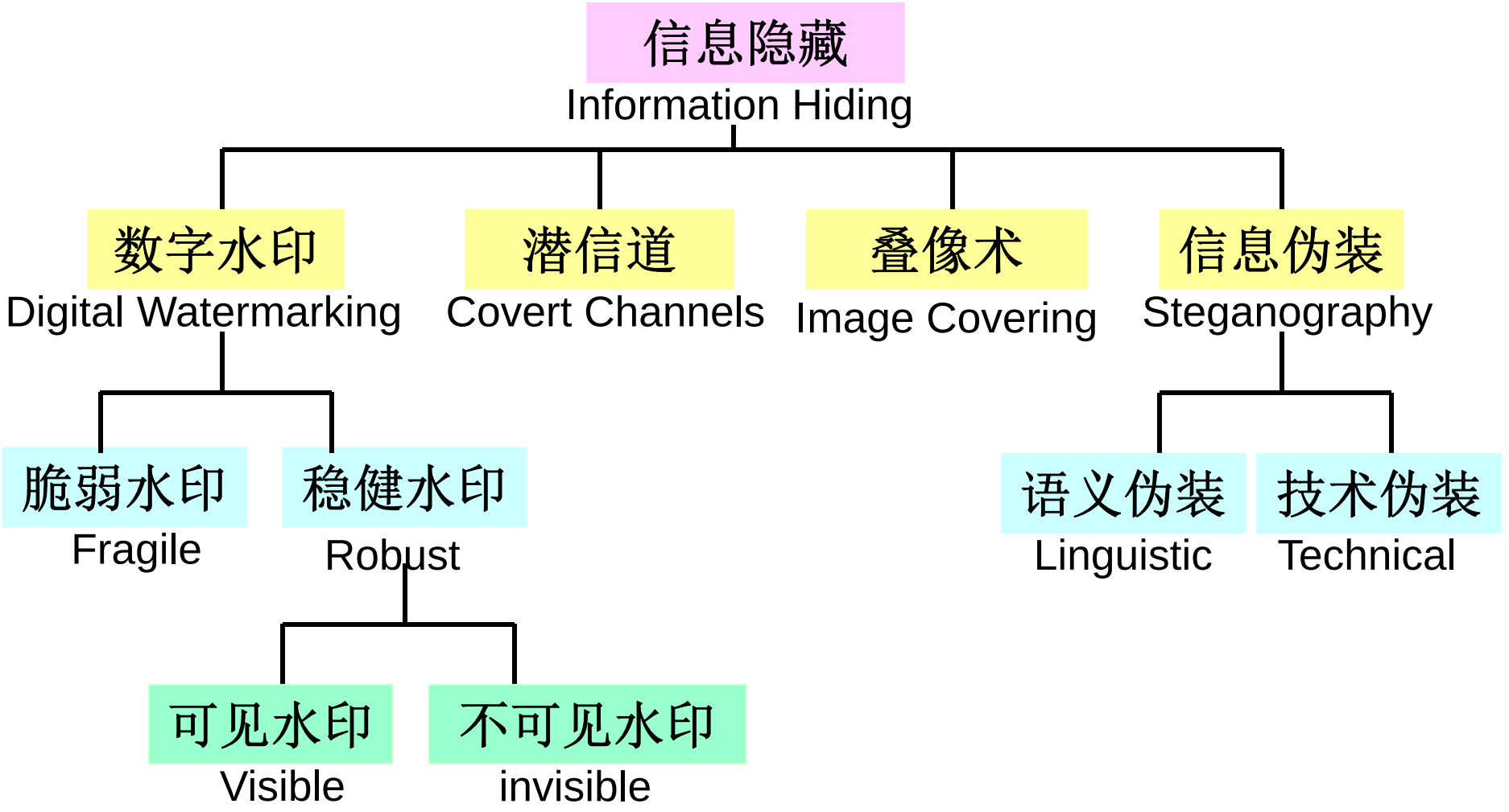
秘密信息

信息隐藏模型接收端

信息隐藏与传统密码技术关系

- 传统加密技术的局限性
  - 明确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
  - 加密后的文件因其不可理解性也妨碍了信息的传播
  - 随着电脑硬件的迅速发展，破解技术日益成熟
- 信息隐藏与密码技术的关系
  - 密码技术仅仅隐藏了信息的内容，而信息隐藏不但隐藏了信息的内容而且隐藏了信息的存在；
  - 密码技术与信息隐藏技术并不是互相矛盾、互相竞争的，而是互补的。

信息隐藏技术分类


信息隐藏
Information Hiding
数字水印
Digital Watermarking
潜信道
Covert Channels
叠像术
Image Covering
信息伪装
Steganography
脆弱水印
Fragile
稳健水印
Robust
语义伪装
Linguistic
技术伪装
Technical
可见水印
Visible
不可见水印
invisible

信息隐藏技术的应用

- 在Web网上对授予著作权的资料进行自动监控
  - 一个自动程序搜索Web网，寻找带有版权标记的资料，通过这种手段来识别可能的非法使用.
- 数据保密
  - 对于一些秘密数据防止非法用户的截获与使用. **Demo……**
  - 在商业、金融方面的应用日益上升。如电子商务中的敏感数据，双方秘密协议互递，网上银行交易等
- 数据完整性的验证
  - 确认数据在网络传输中是否被篡改过. **Demo……**
- 边缘信息的嵌入
  - 扩充数据包括对主信号的描述或参考信息、控制信息以及其它媒体信号等。例如，在某一频道内收看电视，可以通过信息隐藏方法在所播放的同一个电视节目中嵌入更多的镜头以及多种语言跟踪，使用户能够按照个人的喜好和指定的语言方式播放。
- 电子证件/票据防伪

数字作品版权保护


WWW服务器
本地磁盘
嵌入申请
嵌入报告与水印信息
WWW浏览器
本地磁盘
(1)
(4)
(3)
传输网络
(2)
等待嵌入水印的媒体
WWW浏览器
WWW服务器
本地磁盘
水印服务器站点
申请人站点

数字作品版权保护

原始作品

隐藏版权标识后的作品

版权标识

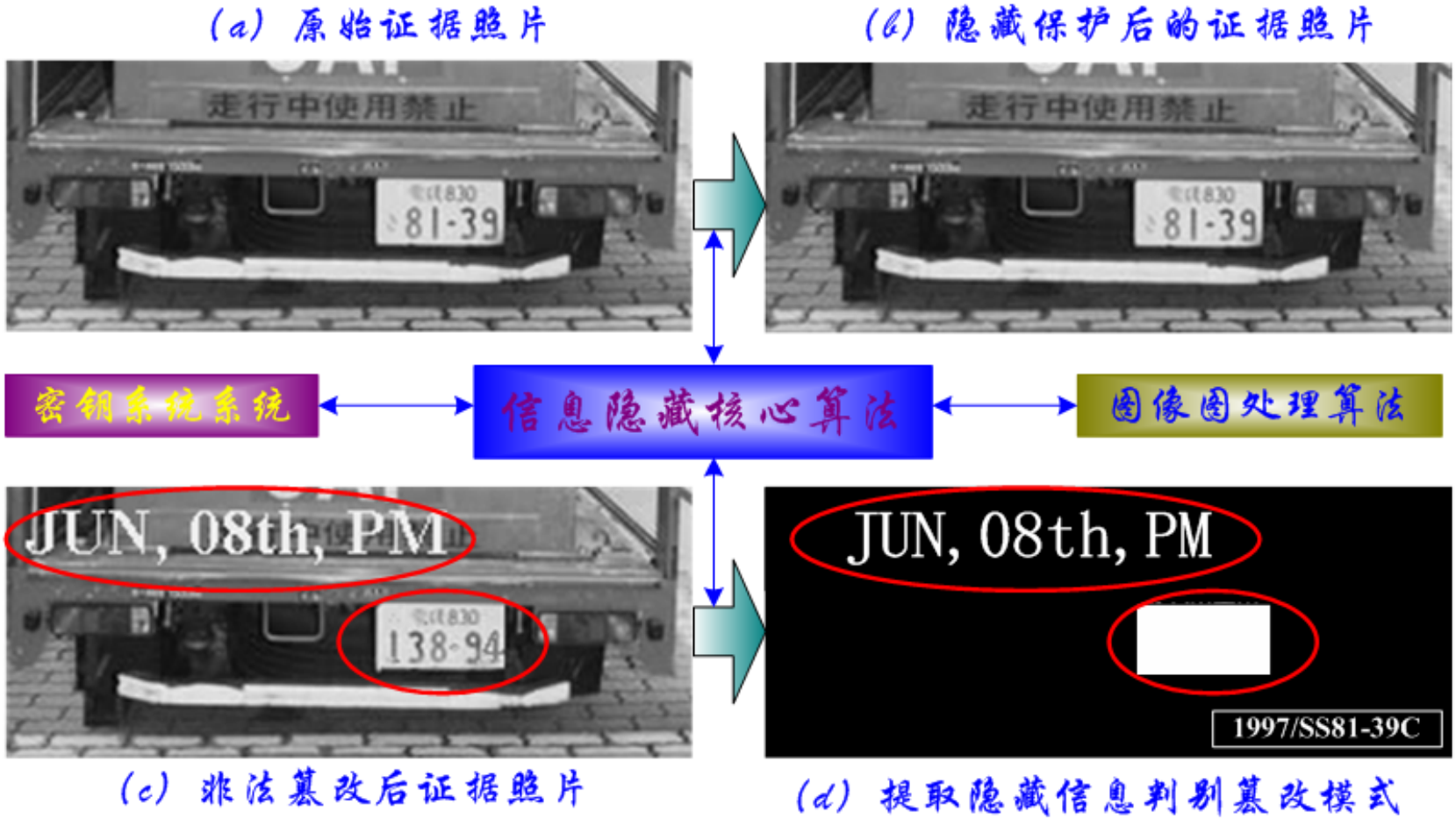
数据完整性的验证


可读域数据
传输/存储级数据（包括加密）
可读域数据
媒体文件服务器
远程终端服务器
输出设备
媒体
数据
采集
0
1
3
1001010101...1001010
传输网络及
接入通道
4
5
6
7
传统加
密体系
2
A
B
C
D
各类潜在非法入侵者
这是一份很
重要的文件
8
内容接收者
怎样才能保证内
容可靠？？？
表面似乎看不
出任何异常…
A：加密系统攻击者
B：网络黑客/非法接入
C：系统内部协同作案者
D：非正常手段获得解密版数据者
问题：我们的数据内容可靠么？

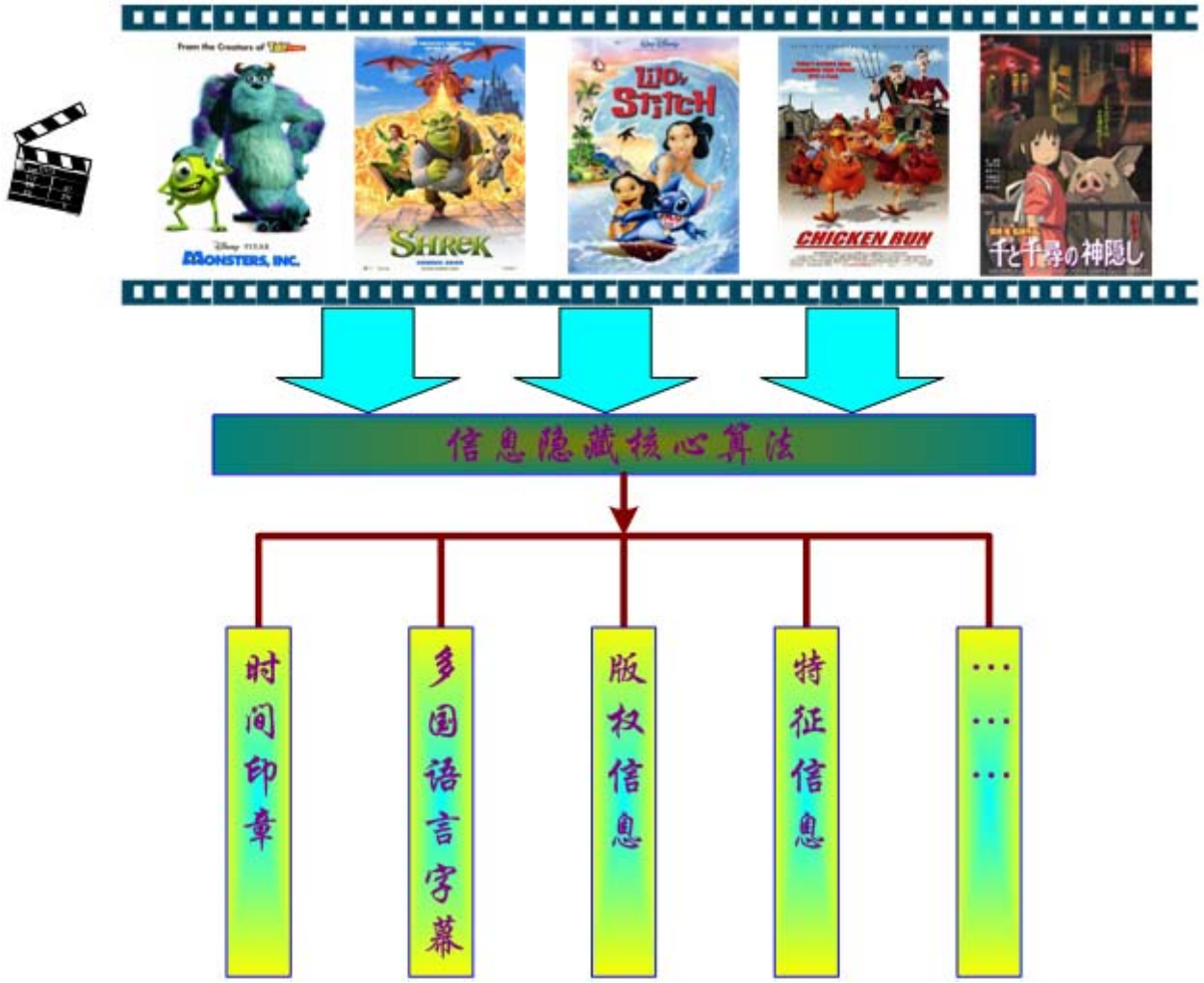
数据完整性的验证


可读域数据
传输/存储级数据（包括加密）
可读域数据
媒体文件服务器
10010110l...1001010
远程终端服务器
媒体数据采集
传输网络及接入通道
输出设备
0
1
2
3
4
5
6
7
8
传统加密体系
附加密钥模块
自动水印嵌入系统
A
B
C
D
各类潜在非法入侵者
附加密钥模块
自动水印验证系统
他们的任何改动都会留下痕迹！！
内容接收者
特性：
*减少人员对重要数据的直接接触
*保证数据加密前和解密后的安全性
水印不可见
多层密钥保护
水印无法伪造
水印系统也有密钥和权限控制！
内容可靠性多了一个依据！
解决方案：数字水印使媒体数据多了一层保护

数据完整性的验证


(a) 原始证据照片
(b) 隐藏保护后的证据照片
走行中使用禁止
81-39
密钥系统系统
信息隐藏核心算法
图像图处理算法
JUN, 08th, PM
138-94
JUN, 08th, PM
1997/SS81-39C
(c) 非法篡改后证据照片
(d) 提取隐藏信息判别篡改模式

边缘信息的嵌入



西南交通大學

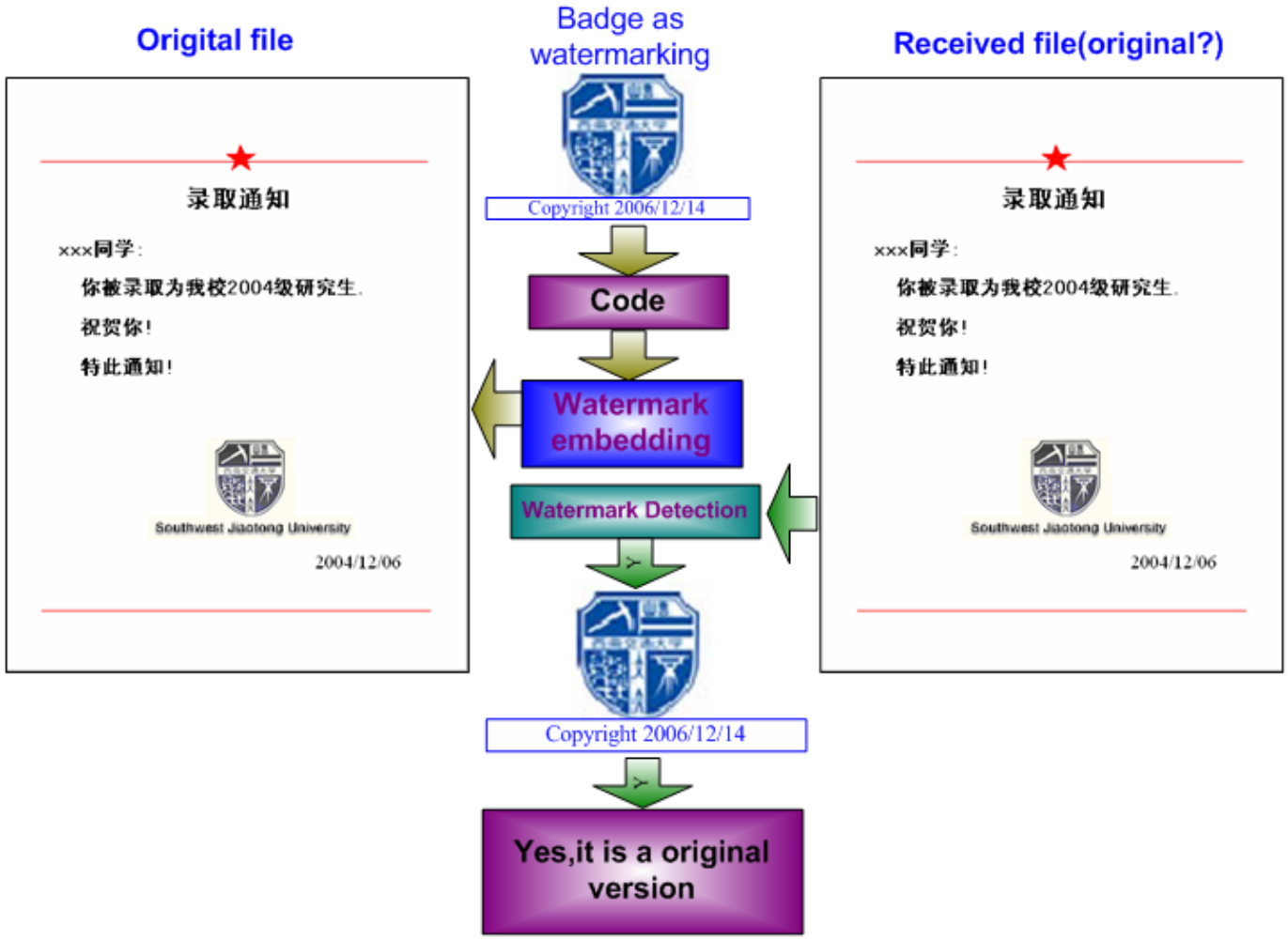
电子证件防伪

西南交通大學

电子证件防伪

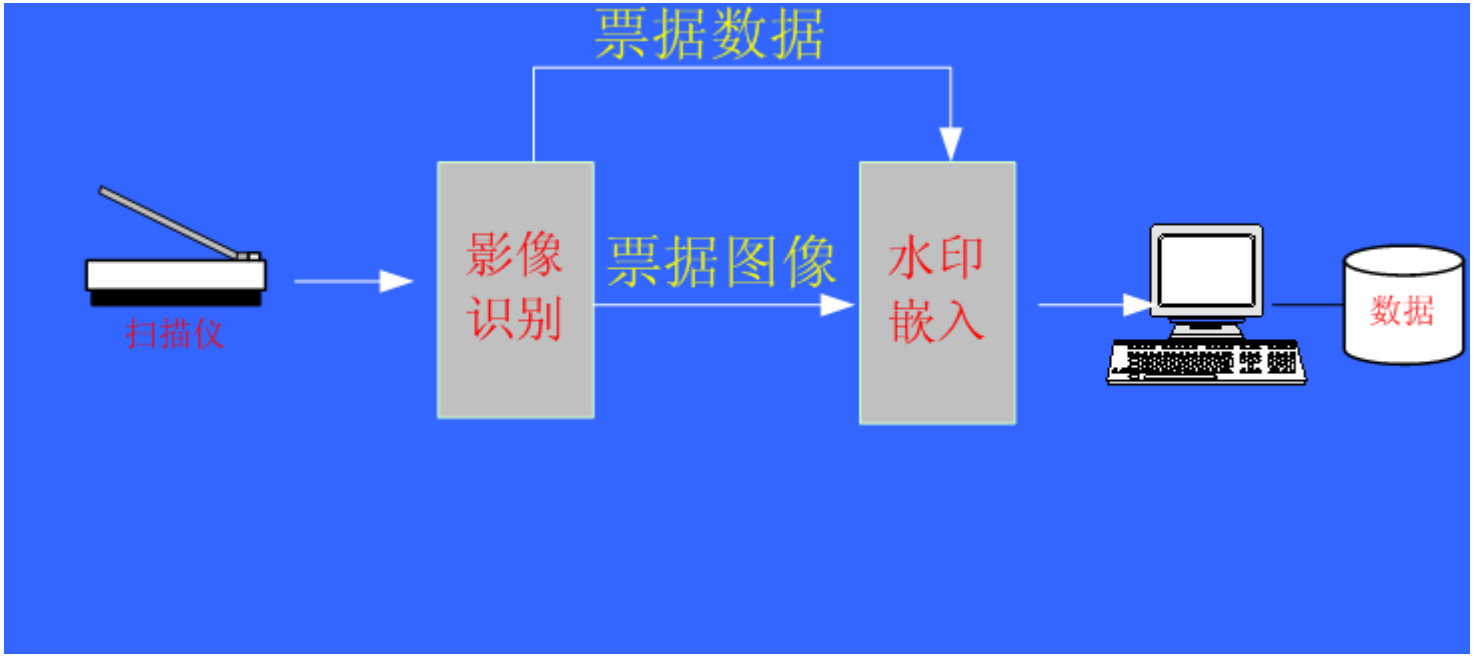
西南交通大学

电子通知书防伪



西南交通大學

商务交易中的票据防伪



信息隐藏技术的研究现状

- 国际信息隐藏学术研讨会（International Workshop on Information Hiding）已在美国、德国、英国、加拿大、荷兰等不同国家举办了十几届。IWDW（International Workshop on Digital-forensics and Watermarking ）从02年起已成功举办**16**届**(07**年在广州，**12**年在上海，**16**年在北京）.
- 近几年来，我国学术界对此前沿领域也极为重视，全国信息隐藏学术大会已举办**13**届，第**14**届全国信息隐藏学术研讨会（CIHW2014）于**2018**年**3**月在华南理工大学召开（**2010**年**9**月在成都）。
- IEEE图像处理国际会议IEEE International Conference on Image Processing（ICIP），IEEE声学与信号处理国际会议IEEE International Conference on Acoustics, Speech, and Signal Processing （ICASSP）

信息隐藏技术的研究现状

- 国内外科研机构和公司已开发出商品化软件和供研究用的免费软件
  - 美国Adobe system公司在Adobe Photoshop 中安装了数字水印；
  - IBM公司在其数字图书馆研究计划中也采用了可见数字水印技术；
  - 新近出现的MP4乐曲中采用了名为“Solana”技术的数字水印，可方便地追踪和发现盗版发行行为，并且任何针对MP4的非法解压行为，都可能导致MP4原文件的损毁；
  - 德国Fraunhofer Institute开发出了一种用来跟踪P2P（Peer-to-Peer）网络上的盗版**MP3**音乐文件的水印软件系统；
  - 2003年7月，日本冲电气工业公司开发出了在打印技术的基础上，综合使用图像处理与数字水印技术的Val-Code新技术，当电子文件打印到纸张上时，该技术可将检测篡改的点阵图形作为文件的底纹一起打印；
  - 我国华旗资讯自主研发了具有内容保真和版权保护的数字水印数码相机；
- 目前研究信息隐藏多以图像为载体, 而声音、视频、文本较少。
- 目前，对于信息隐藏应用在数字产品的著作权保护方面（或称为数字水印）的研究较多。

涉及信息隐藏技术的期刊

- 国际期刊: IEEE Trans. on image processing / Multimedia / Signal Processing / Information Forensics and Security /Information Theory / Journal Selected Areas Communications /Circuits and System for Video Technology / Consumer Electronics / Proceedings of IEEE; IEE Electronics Letters; IEICE Trans. on Fundamentals of Electronics Communications and Computer Sciences / Communications
- 国内期刊: 中国科学，电子学报, 通信学报, 软件学报, 计算机学报, 系统仿真学报, 计算机辅助设计与图形学学报, 计算机工程等
- 国际会议: IEEE ICIP/ ICASSP (International Conference on Acoustics, Speech and Signal Processing) /CAS、ACM Multimedia

信息隐藏技术所涉及的知识领域

- 多媒体技术：多媒体编解码（JPEG、TIFF、GIF、BMP、PNG、WAV、MP3、AAC、AVS、MPEG等），图像处理（图像处理工具的使用-Photoshop、像素、亮度、色度、DCT、DWT、DFT、缩放、旋转、滤波等）音频（声音处理工具的使用-Audio Editor/SoundForge/CoolEdit Pro、声音编辑、人类声学模型、音频掩蔽效应、子带声音处理、采样等），视频（视频处理工具的使用-Video Editor、MPEG标准）
- 通信理论（隐藏容量理论分析-信息论，PSNR、调制、滤波、噪声污染、扩频、BER）
- 计算机：编程实现
- 信息安全：密码技术、系统安全性分析