信息安全导论

第十章 信息隐藏技术

黄 玮

本学期剩余5次课时的安排

- 2012.11.30　信息隐藏技术
- 2012.12.7　版权管理与数字水印技术
- 2012.12.14　信息安全等级保护与信息系统安全工程
- 2012.12.21　信息安全管理与信息安全法规
- 2012.12.28　课程串讲复习

温故 密码学的传统应用：数据安全和通信安全

- 对称加密
- 公钥加密
- 数字证书
  - —对称加密
  - —公钥加密
  - —消息鉴别
  - —散列算法
  - —数字签名
- PKI
  - —数字证书

机密性

完整性

身份认证

授权

不可抵赖性

- 数字媒体技术发展的需要

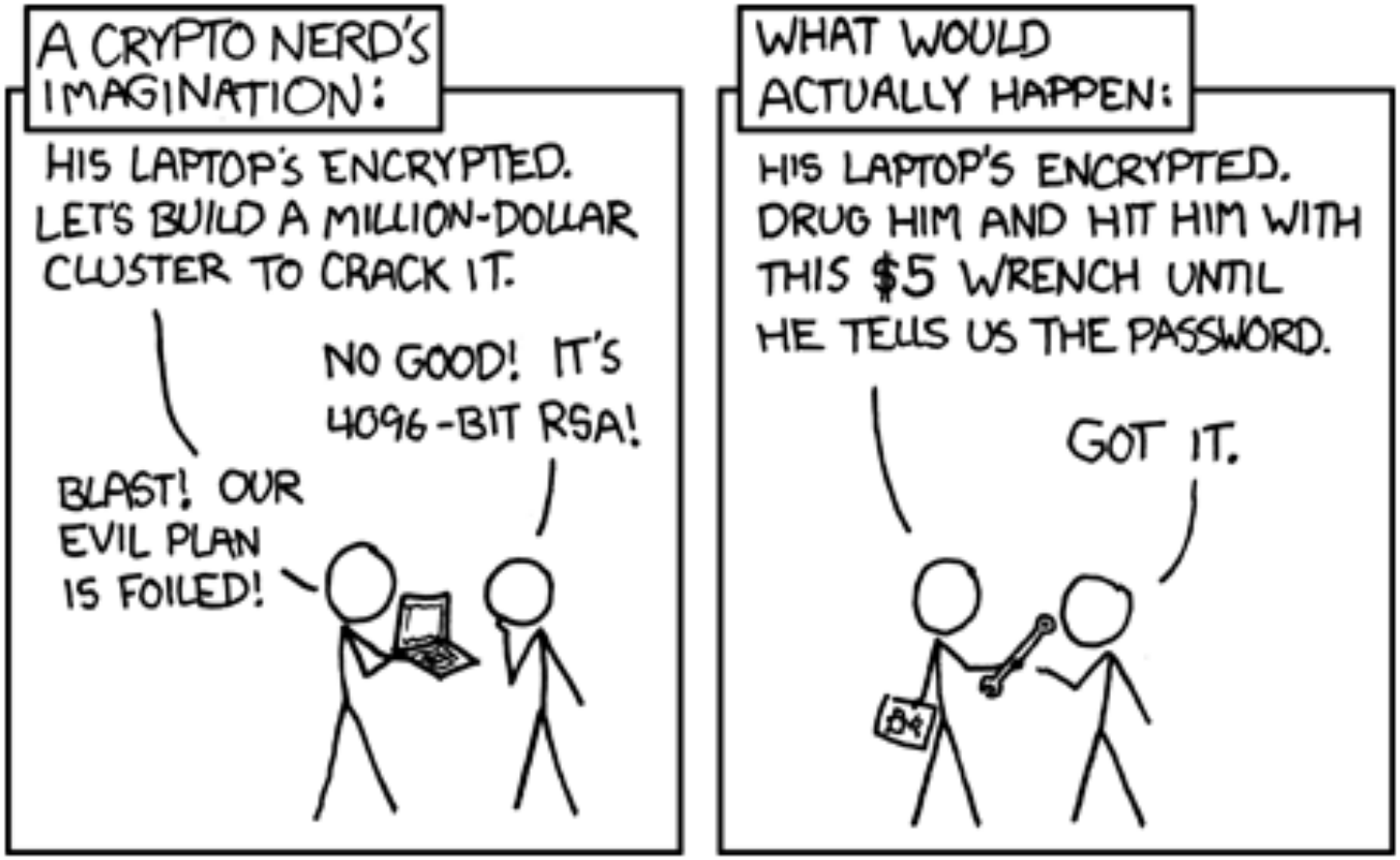
内容安全

本章内容提要

- **信息加密与信息隐藏**
- 信息隐藏概述
- 信息隐藏与通信
- 信息隐藏的应用与演示

信息加密与信息隐藏

为什么有了加密还需要研究信息隐藏?




优酷
스테가노그래피(Steganography)
==隐写术（Steganography）
把特定信息（文件）隐藏在照片或者音乐中的技术=-

最“朴素”的信息隐藏方法


A'LA'IH, DO'NEH'LINI,
DO'NEH'LINI, A'LA'IH,
A'LA'IH, DO'NEH'LINI,
DO'NEH'LINI, DO'NEH'LINI,
A'LA'IH, A'LAIH,
DO'NEH'LINI, A'LA'IH,
DO'NEH'LINI, DO'NEH'LINI,
DO'NEH'LINI...
FOR ADDED SECURITY, AFTER WE ENCRYPT THE DATA STREAM, WE SEND IT THROUGH OUR NAVAJO CODE TALKER.
...IS HE JUST USING NAVAJO WORDS FOR "ZERO" AND "ONE"?
WHOA, HEY, KEEP YOUR VOICE DOWN!

信息加密与信息隐藏

- **信息加密**
  - —对秘密信息本身进行保护
  - —信息的传递过程是暴露的

- **信息隐藏**
  - —掩盖秘密信息存在的事实
  - —表面上看是A，其实真正传递的信息是B

林乌信我无机事，
息精息气养精神。
宫墙隐嶙围野泽，
天水藏来玉堕空。

本章内容提要

- 信息加密与信息隐藏
- **信息隐藏概述**
- 信息隐藏与通信
- 信息隐藏的应用与演示

信息隐藏的研究领域

- 信息隐藏　　守
  - —在信息载体中隐藏尽可能多的信息
  - —不能引起任何可察觉的变化
    - 感观变化
    - 信息统计分析变化
- 信息隐藏分析　攻
  - —在看似正常的信息载体中找出隐藏其中的秘密信息，篡改或破坏隐藏其中的秘密信息

信息隐藏的载体分类

- 图像
- 视频
- 音频

} ⟶ 感观冗余度

- 数据集合
  - —文本
  - —二进制数据
    - – Word / Excel / EXE …

信息隐藏基本思想

- 利用人类感知系统的冗余
- 利用计算机处理系统的冗余
- 利用各种潜信道

信息隐藏的支撑技术

- 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
- 人类感知理论
  - —视觉理论
  - —听觉理论
- 现代通信技术
- 密码技术

信息隐藏的基本方法分类

- 时域（空域）替换技术
- 变换域技术
- 扩展频谱技术
- 统计方法

信息隐藏算法设计的安全性需求

- 非恶意破坏
  - —信息载体在传输过程中叠加了噪声
  - —有损压缩
- 恶意破坏
  - —消除隐藏的秘密信息

恶意破坏举例

- 数字图像

  —图像加噪、低通滤波、有损压缩、图像剪切、图像拼接、图像大小变化、图像旋转、打印扫描等。

- 数字视频

  —加噪、视频压缩编码、丢帧、插帧、帧重组、视频流剪切和拼接等。

- 数字音频

  —加噪、滤波、语音压缩编码、数模模数转换、重采样、采样率变化等。

- 数据集合

  —数据跨平台的格式转换，数据删除、数据添加等。

信息隐藏的应用领域

- 广义信息隐藏
  - —在某种载体中嵌入数据
- 两个分支
  - —信息隐藏
    - 伪装式隐蔽通信
  - —数字水印
    - 数字产品的版权保护（数字版权管理DRM）

将密码学与信息隐藏相结合，就可以同时保证信息本身的安全和信息传递过程的安全

信息隐藏问题描述

- 囚犯问题

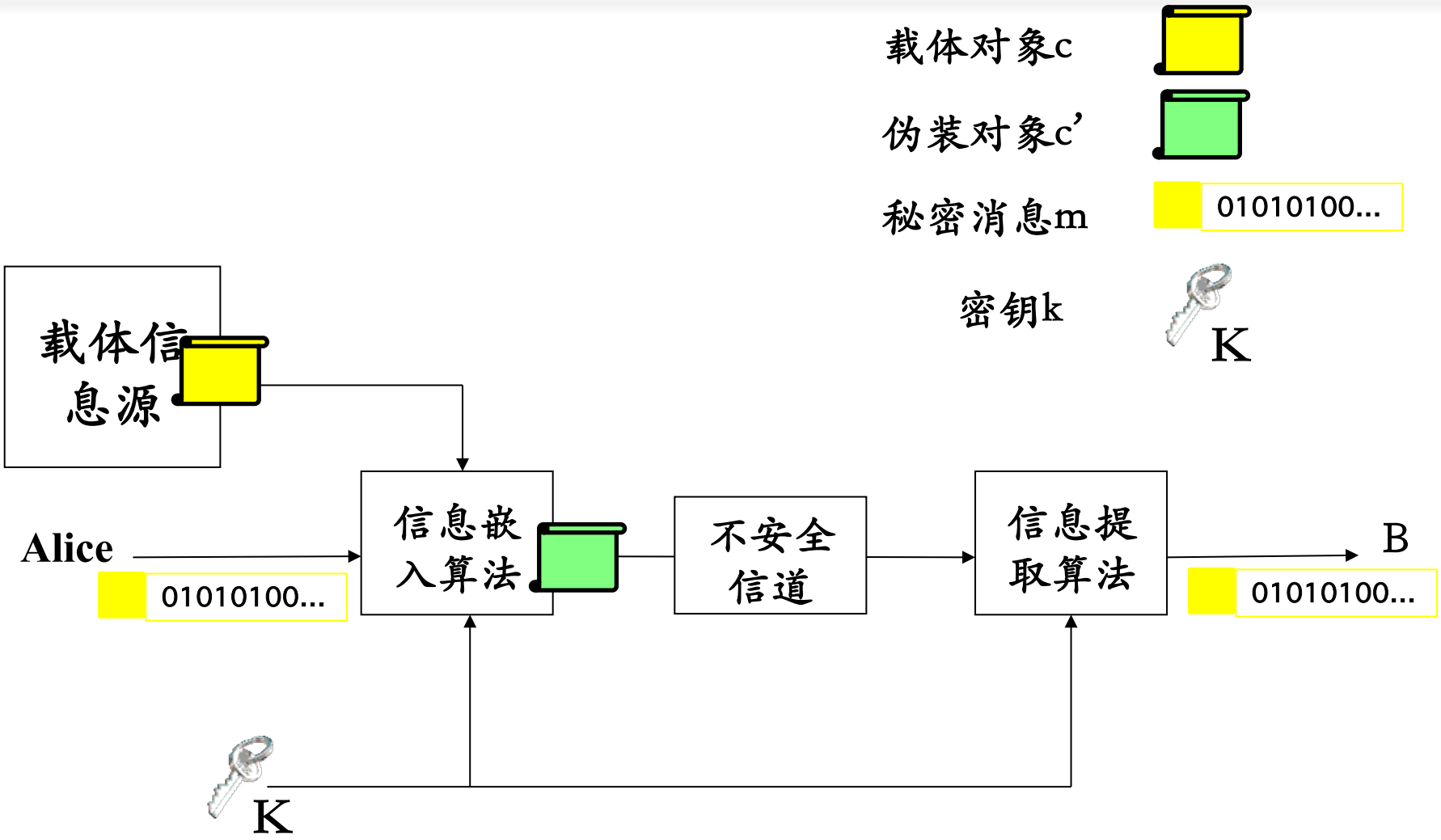
  —两个囚犯A和B被关押在监狱的不同牢房，他们想通过一种隐蔽的方式交换信息，但是交换信息必须要通过看守的检查。因此，他们要想办法在不引起看守者怀疑的情况下，在看似正常的信息中，传递他们之间的秘密信息

- 看守者

  —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

信息隐藏的原理框图


载体对象c
伪装对象c'
秘密消息m
01010100...
密钥k
K
载体信息源
Alice
01010100...
信息嵌入算法
不安全信道
信息提取算法
B
01010100...
K

术语解释

- A打算秘密传递一些信息给B，A需要从一个随机消息源中随机选取一个无关紧要的消息c，当这个消息公开传递时，不会引起怀疑，称这个消息c为**载体对象**
- 把需要秘密传递的信息m隐藏到载体对象c中，此时，载体对象c就变为**伪装对象**c’
- 秘密信息的嵌入过程需要密钥，此密钥称为**伪装密钥**

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
- 伪装对象与载体对象无法区分，无论从感观上，还是从统计分析上
- 信息隐藏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

信息隐藏的基本方法

- 信息载体选择
  - —图像/音频/视频/二进制文件
- 信息嵌入位置确定
  - —文件头部、文件尾部、文件任意位置
- 信息嵌入算法
  - —利用冗余特性：覆盖、追加、重新编码
  - —利用潜信道：覆盖、追加
- 信息提取算法

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
  - —篡改隐藏信息
  - —破坏隐藏信息
  - —提取隐藏信息
- 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

攻击者：判断是否有隐藏

- **定义一个检验函数 $f: C \rightarrow \{0, 1\}$**

$$f(c)=\begin{cases}1 & c\text{中含有秘密消息}\\ 0 & \text{其它}\end{cases}$$

判断结果

- 实际有隐藏，判断有隐藏——正确
- 实际无隐藏，判断无隐藏——正确
- 实际无隐藏，判断有隐藏——错误

  ——误判
- 实际有隐藏，判断无隐藏——错误

  ——漏判

实用的信息隐藏系统

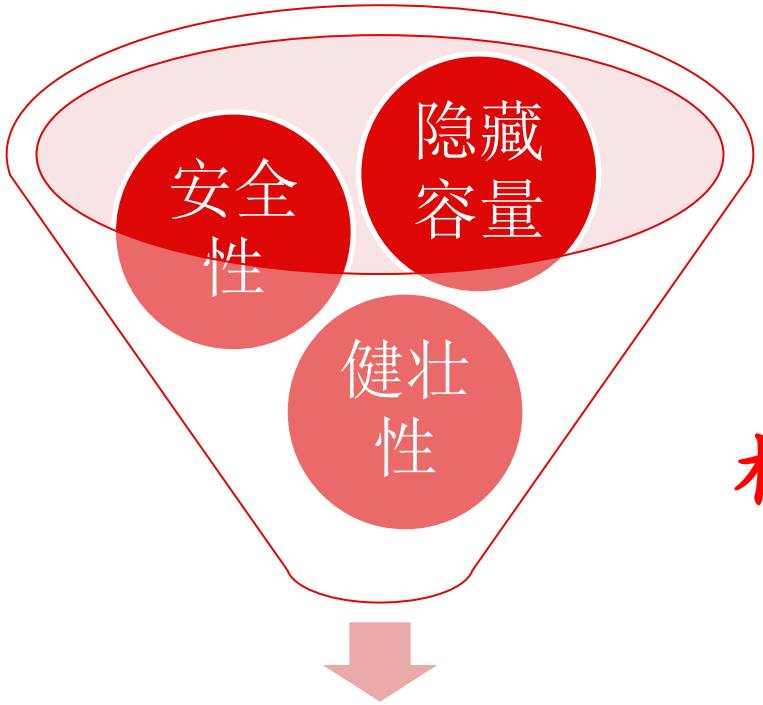
- 假设
  - —攻击者误判的概率为α
  - —攻击者漏判的概率为β
- 一个实用的信息隐藏系统应该尽可能使β最大
- 一个理想的信息隐藏系统应该有β=1
  - —所有藏有信息的载体都被认为没有隐藏信息而被放过，达到了信息隐藏、迷惑攻击者的目的

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，等等

信息隐藏的健壮性

- 伪装载体受到某种攻击后，仍然能够从中提取出隐藏信息，称为算法对这种攻击是健壮的



相互制约

本章内容提要

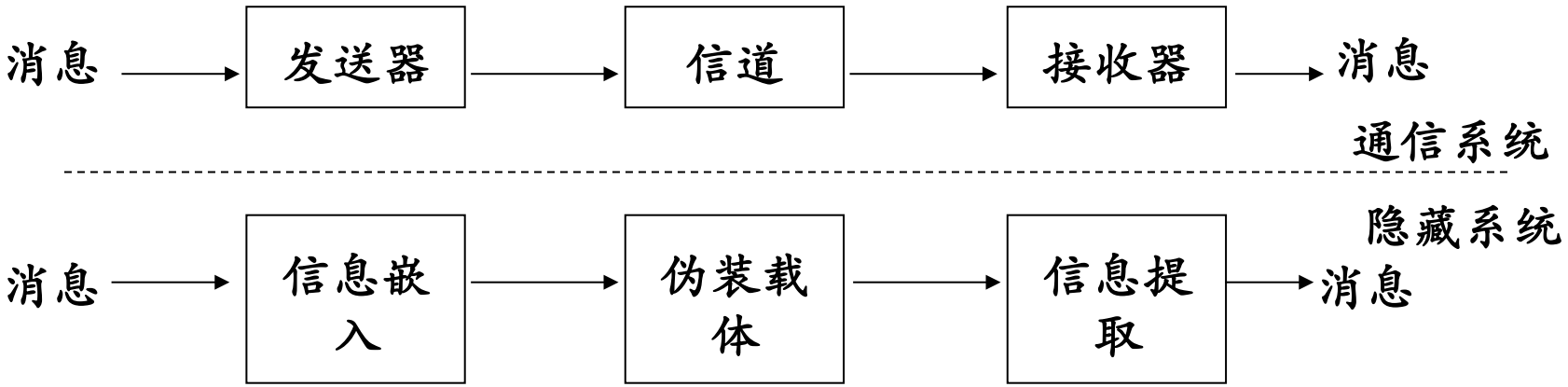
- 信息加密与信息隐藏
- 信息隐藏概述
- **信息隐藏与通信**
- 信息隐藏的应用与演示

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(1/3)

- 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(2/3)

- 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：感观约束

隐藏系统与通信系统的比较(3/3)

- 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）

通信模型分类——根据噪声性质分类

- 加性噪声信道模型
  - 设原始图像为I_0，待隐藏信息为W，隐藏后图像为I_1，接收端收到的图像为I_2，待隐藏信息经过特定的处理后加载到图像的空间域或变换域中，用$I_1-I_0=f(W)$表示，图像在信道中受到的处理用$I_2-I_1=P$表示
- 非加性噪声信道模型（几何变换）
  - 但有一些攻击不能用加性噪声表示，如图像的平移、旋转等，这些处理不仅影响象素值，而且还影响数据的位置。
  - 这类攻击信道表示为几何信道，并分为两类：针对整个图像的几何变换，包括平移、旋转、尺度变化和剪切，可以用较少的参数描述；另一类是针对局部的几何变换，如抖动等，需要更多的参数来描述

通信模型分类——按载体对检测器的贡献分类

- 将载体等效为噪声，认为载体未知
  - —将载体图像与信号处理、攻击同等对待。信息提取端将载体、信号处理和攻击都看作信道噪声和干扰
- 利用已知载体的信息
  - —如果将载体内容仅仅视为噪声，则忽略了“信息嵌入端完全知道载体的内容”的事实
  - —把载体内容视为信道边信息
  - —Cox认为这种模型与已知边信息的通信模型很类似
  - —寻找最佳嵌入方案，设计更有效的信息嵌入和提取方法：定义某种距离的度量，在允许干扰范围内，选择载体图像，使得检测概率最大

通信模型分类——按是否考虑主动攻击分类

- 主动攻击的建模难度很大，一些文献只考虑原始载体和某类信号处理对信息隐藏的影响（被动攻击）
- 利用博弈论思想考虑主动攻击的影响

  ——把信息隐藏看作信息隐藏者和攻击者之间的博弈过程，定义载体信号嵌入信息前后、受到攻击前后的距离，在这种距离定义条件下，嵌入过程和攻击过程分别受到约束，隐藏容量就是平衡点处的容量值

本章内容提要

- 信息加密与信息隐藏
- 信息隐藏概述
- 信息隐藏与通信
- **信息隐藏的应用与演示**

信息隐藏的应用(1/2)

- 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
  - —伪装式隐蔽通信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(2/2)

- 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

信息隐藏检测

- 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
- 信息隐藏的对立面——隐藏检测技术应运而生

信息隐藏演示实验

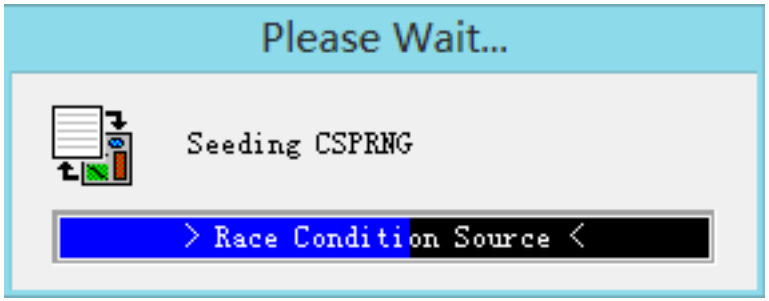
- 图像信息隐藏
  - —利用GIF图片的注释字段（文件头部）
    - http://weibo.com/1651460060/wr0qmmljqv
  - —JPG/PNG文件尾部追加数据（文件尾部）
    - Windows: copy /b a.jpg+b.zip c.jpg
    - *nix: cat b.zip >> a.jpg
  - —图像隐写术：openstego
  - —图像/音频隐写术：silenteye
- 视频信息隐藏
  - —openpuff

openpuff

- 专业信息隐藏工具
  - 基于硬件的随机数生成器
  - 可否认信息隐藏
  - 支持链式载体（最大支持256Mb隐藏数据）
  - 载体信息利用率选择
  - 支持16种现代密码学算法
  - 多层数据混淆（支持3个独立口令）
- 独有的安全和混淆特性
- 支持多种载体格式
  - 图片支持 (BMP, JPG, PCX, PNG, TGA)
  - 音频支持 (AIFF, MP3, NEXT/SUN, WAV)
  - 视频支持 (3GP, MP4, MPG, VOB)
  - Flash-Adobe 支持 (FLV, SWF, PDF)
- 绿色便携软件
- 免费软件
  - 核心加密库开源

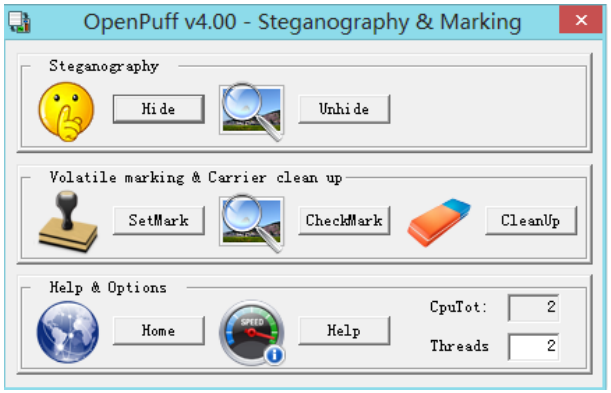
openpuff独有的安全和混淆特性

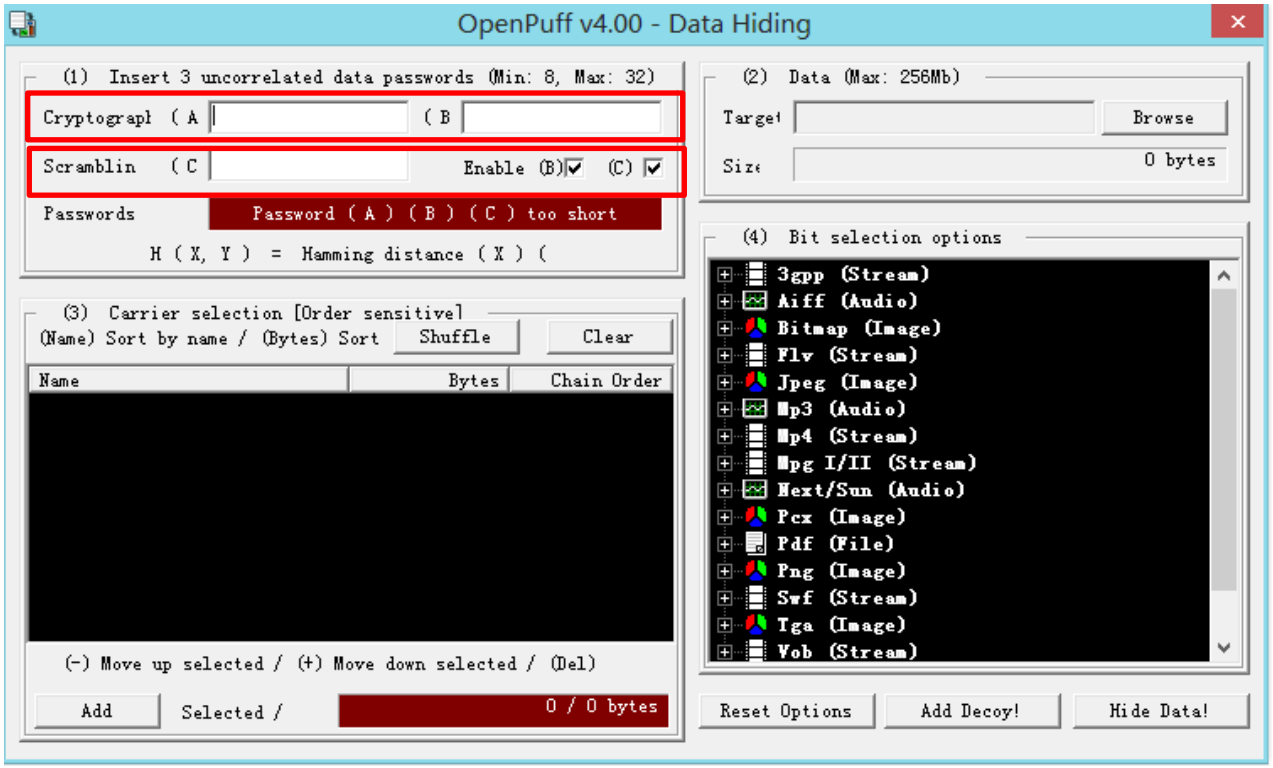
- 隐藏数据在注入信息载体之前，需要经过
  - —加密
    - 二次对称加密（16种候选加密算法、2个独立256bit加密密钥）
  - —扰乱
    - 密文被使用基于第三个独立密钥的CSPRNG产生的随机序列随机分块打乱
  - —白噪声化
    - 扰乱后密文被使用基于独立CSPRNG产生的白噪声序列随机填充
  - —自适应非线性编码
    - 白噪声混入后密文数据与原始信息载体一起被进一步使用非线性编码，对抗信息隐藏检测



openpuff使用截图

- 密码学加密密钥：A、B
- 随机扰乱算法种子值：C





参考文献

- silenteye : http://www.silenteye.org/
- openstego: http://openstego.sourceforge.net
- openpuff: http://embeddedsw.net/OpenPuff_Steganography_Home.html