

08

第8章 信息隐藏分析



隐写分析分类



信息隐藏分析的层次



隐写分析评价指标



信息隐藏分析示例



信息隐藏分析的层次(上)



隐写分析分类

1. 发现隐藏信息
2. 提取隐藏信息
3. 破坏隐藏信息

密码设计 与分析

密码设计

研制密码算法。

密码分析

在未知密钥的情况下，试图破译密码。

密码分析的目的：

破译密码；
寻找密码算法的漏洞，促进研制安全性更高的密码算法。

信息隐藏与分析

信息隐藏

研究信息隐藏算法。

隐藏分析

需要在载体对象、伪装对象和可能的部分秘密消息之间进行比较。

隐藏分析的目的：

防止隐写术的滥用；
寻找隐藏算法的漏洞，促进研制安全性更高的隐藏算法。

1. 发现隐藏信息(1)

信息隐藏技术主要分为这样几大类：
第一类：时域替换技术
第二类：变换域技术
第三类：其他常用的技术

正常的量化噪声应满足高斯分布，用秘密信息替换后（或者秘密信息加密后再替换），其分布就会发生变化

空间域低比特
替换方法

分析伪装对象低比特位的统计特性，来判断是否存在信息隐藏

1. 发现隐藏信息(2)

调色板图像

分析调色板有无异变换域的
隐藏方法

1. 发现隐藏信息(3)

较困难

变换域技术

针对具体隐藏算法，寻找
特定算法所产生的特征

1. 发现隐藏信息(4)

文件格式法

分析文件大小与数据大小
是否一致