
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

隐写分析分类

隐写与隐写分析

隐写

隐写（steganography）

目的：以表面正常的数字载体如静止图象、数字音频和视频信号等作为掩护，在其中隐藏秘密信息。额外数据的嵌入既不改变载体信号的视、听觉效果，也不改变计算机文件的大小和格式（包括文件头），使隐蔽信息能以不为人知的方式进行传输。

隐写分析

隐写分析（steganalysis）

隐写分析是针对图像、视频和音频等多媒体数据，在对信息隐藏算法或隐藏的信息一无所知的情况下，仅仅是对可能携密的载体进行检测或者预测，以判断载体中是否携带秘密信息。

早在2001 年初，震惊世界的9.11 事件发生半年多以前，美国报纸就曾刊登文章，指出本·拉登及其同伙可能利用某些网站上的大量数字图像秘密传递与其恐怖行动有关的信息如指令、地图、攻击目标的资料等。

有报道称，首先将科学家在隐写研究中取得的早期成果用于实践的就有基地和哈马斯等国际恐怖组织。

一些研究者开始对著名网站上数以百万计的图像展开搜索和检测，试图寻找可能存在的敌对隐蔽信息。

这些工作虽然未能找到隐蔽恐怖信息的确凿证据，却推动了隐写和隐写分析的研究。

隐写和隐写分析在军事、情报、国家安全方面的重要意义是不言而喻的。

设计高度安全的隐写方法是一项富于挑战性的课题。

对隐写的准确分析往往比隐写本身更加困难。

隐写分析分类

根据适用性分类：

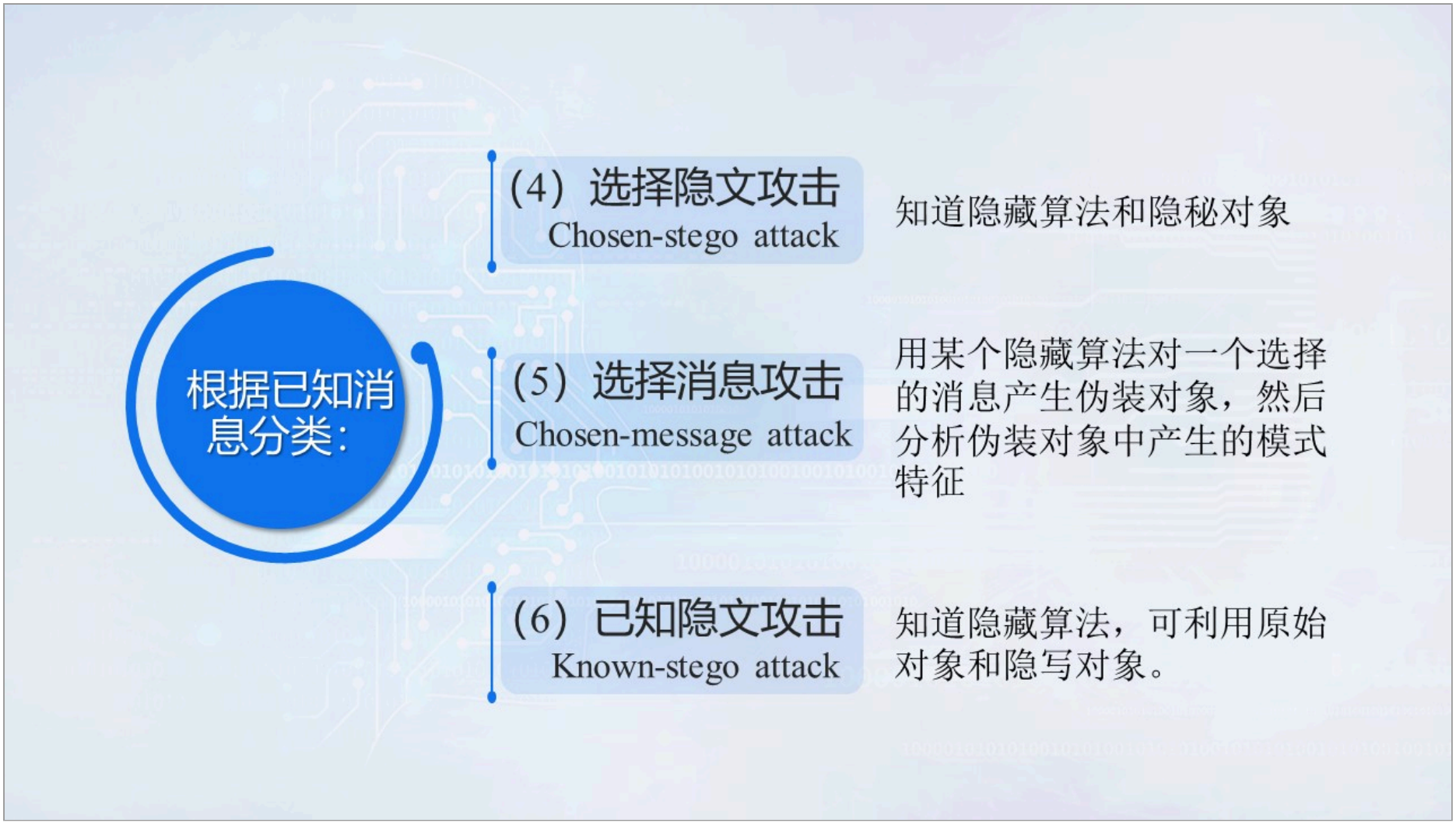
(1) 专用隐写分析

针对特定隐写技术或研究对象的特点进行设计

(2) 通用隐写分析

不针对某一种隐写工具或隐写算法的盲分析


根据已知消息分类：
(1) 唯隐文攻击
Stego-only attack
只有隐写对象可用于分析。
(2) 已知载体攻击
Known-cover attack
可利用原始的载体对象和隐写对象 。
(3) 已知消息攻击
Known-message attack
已知隐藏的消息。


根据已知消息分类：
(4) 选择隐文攻击
Chosen-stego attack
知道隐藏算法和隐秘对象
(5) 选择消息攻击
Chosen-message attack
用某个隐藏算法对一个选择的消息产生伪装对象，然后分析伪装对象中产生的模式特征
(6) 已知隐文攻击
Known-stego attack
知道隐藏算法，可利用原始对象和隐写对象。


根据采用的分析方法分类：
感官分析
用人眼、耳对伪装对象进行分析，判断是否可疑。
统计分析
对比正常载体的和伪装对象的理论期望频率分布。
特征分析
寻找特定隐藏算法所产生的固有特征。

根据最终的效果分类：

被动隐写分析：

仅仅是判断多媒体数据中是否存在秘密信息

尝试判断携密载体所采用的算法

主动隐写分析：

估算隐藏信息的长度

估计隐藏信息的位置

猜测隐藏算法使用的密钥

猜测隐藏算法所使用的某些参数

提取隐藏的秘密信息----终极目标