
03
第3章 信息隐藏基本原理


03
第3章
3.1 信息隐藏的概念
3.2 信息隐藏的分类
3.3 信息隐藏的安全性
3.4 信息隐藏的鲁棒性
3.5 信息隐藏的通信模型

信息隐藏的概念

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 。

名词

载体对象：

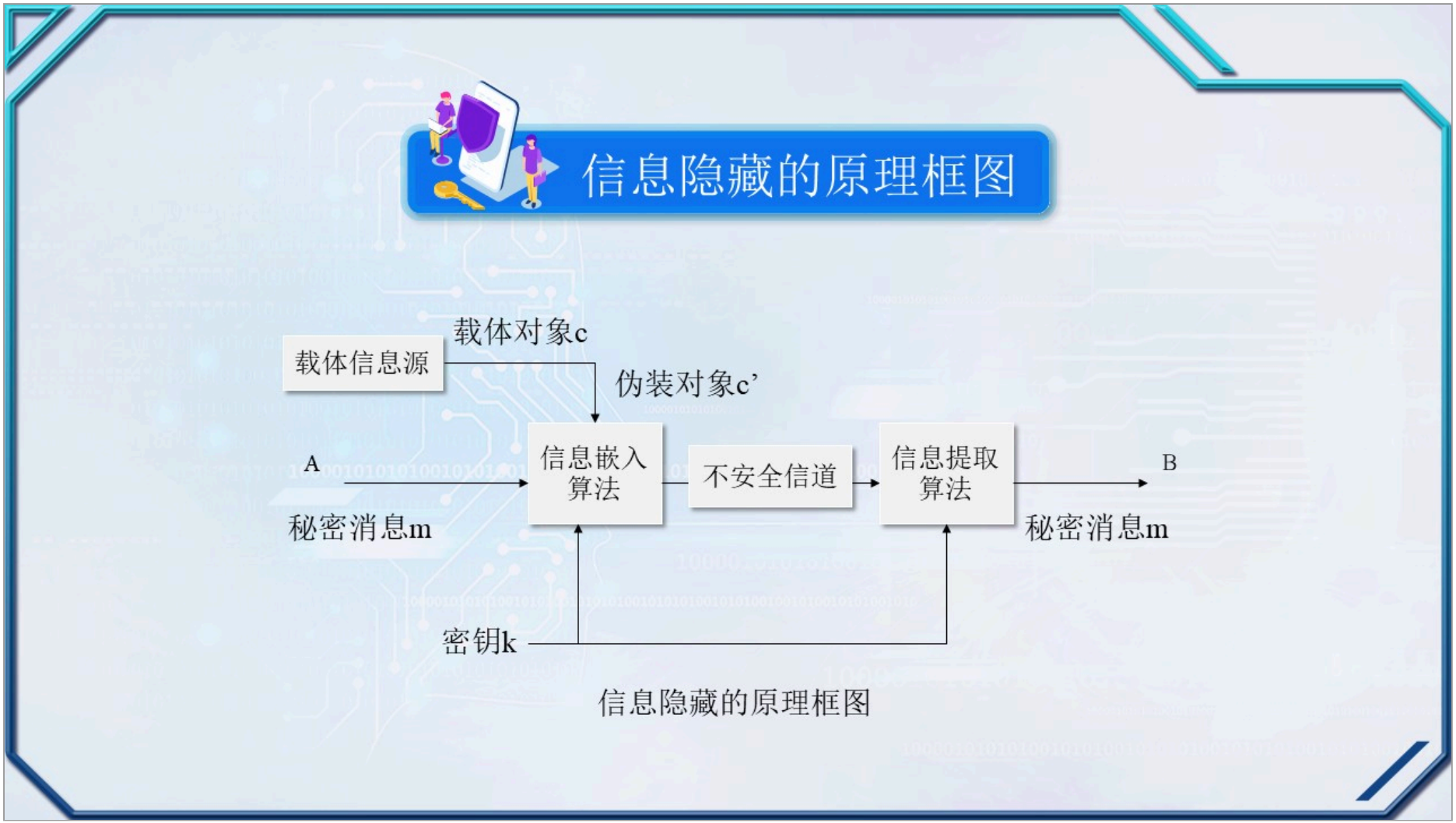
A打算秘密传递一些信息给B，A需要从一个随机消息源中随机选取一个无关紧要的消息c，当这个消息公开传递时，不会引起怀疑，称这个消息c为**载体对象**。

伪装对象：

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’**。

伪装密钥：

秘密信息的嵌入过程需要密钥，此密钥称为**伪装密钥**。


信息隐藏的原理框图
载体对象c
载体信息源
伪装对象c'
A
信息嵌入算法
不安全信道
信息提取算法
B
秘密消息m
秘密消息m
密钥k
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
- 伪装对象与载体对象无法区分，无论从感观上，还是从计算机的分析上
- **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