§7.1 信息隐藏技术

密码技术主要是研究如何将机密信息进行特殊的编码，以形成不可识别的密码形式（密文 ）进行传递；

信息隐藏，主要研究如何将某一机密信息隐藏于另一公开的信息中，然后通过公开信息的传输来传递机密信息。

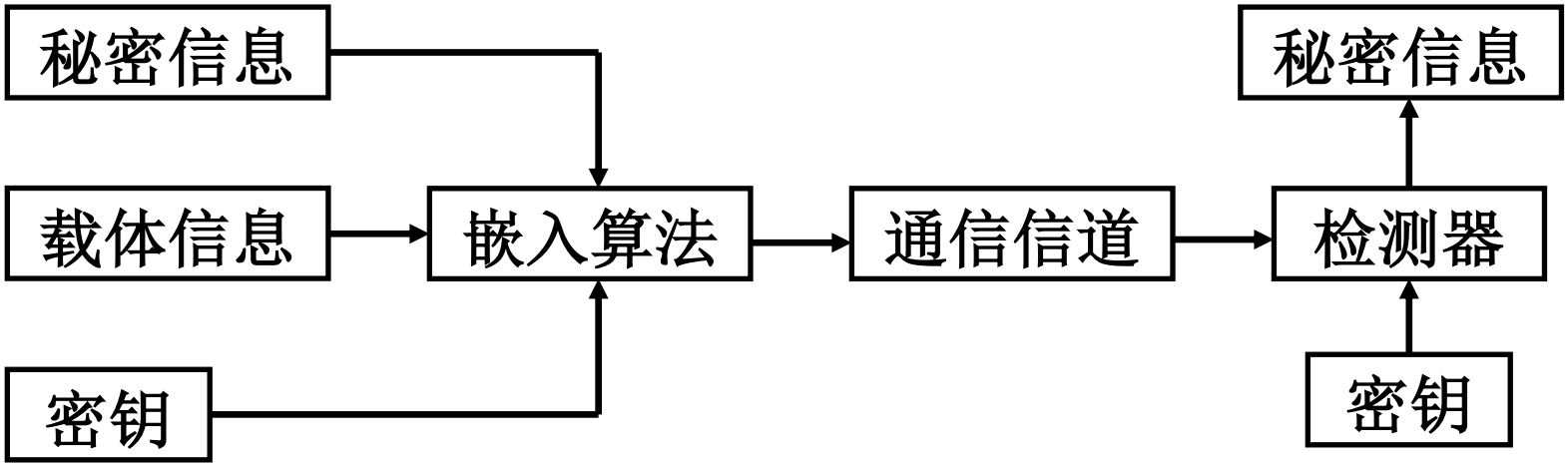
对加密通信而言，攻击者可通过截取密文，并对其进行破译，或将密文进行破坏后再发送，从而影响机密信息的安全；

对信息隐藏而言，攻击者难以从众多的公开信息中判断是否存在机密信息，增加截获机密信息的难度，从而保证机密信息的安全。

信息隐藏基本思想起源于古代的伪装术（密写术）。

§7.1 信息隐藏技术

信息隐藏的通用模型如下图所示。我们称被隐藏的信息为秘密信息，如版权信息、秘密数据、软件序列号等。而用于隐藏秘密信息的公开信息称为隐藏载体，如视频、图片、音频，文本文件等。



§7.1 信息隐藏技术

信息隐藏技术主要由下述两部分组成：

（1）信息嵌入算法，它利用密钥来实现秘密信息的隐藏；

（2）隐藏信息检测与提取算法，它利用密钥从隐藏载体中检测和提取出秘密信息。

在密钥未知的前提下 ，攻击者很难从隐藏载体中得到或删除，甚至发现秘密信息 。

§7.1 信息隐藏技术

信息隐藏技术特性：

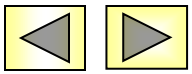
（1）鲁棒性（robustness）

（2）不可检测性（undetectability）

（3）透明性（invisibility）

（4）安全性（security）

（5）自恢复性



§7.1 信息隐藏技术

信息隐藏技术特性：

（1）鲁棒性（robustness）

指不因图象文件的某种改动而导致隐藏信息丢失的能力。

这里所谓“改动”包括传输过程中的信道噪音、滤波操作、重采样、有损编码压缩等。

（2）不可检测性（undetectability）

（3）透明性（invisibility）

（4）安全性（security）

（5）自恢复性

§7.1 信息隐藏技术

信息隐藏技术特性：

（1）鲁棒性（robustness）

（2）不可检测性（undetectability）

指隐蔽载体与原始载体具有一致的特性。如具有一致的统计噪声分布等，以便使非法拦截者无法判断是否有隐蔽信息。

（3）透明性（invisibility）

（4）安全性（security）

（5）自恢复性

§7.1 信息隐藏技术

信息隐藏技术特性：

（1）鲁棒性（robustness）

（2）不可检测性（undetectability）

（3）透明性（invisibility）

利用人类视觉或听觉系统属性，经过一系列隐藏处理，使目标数据没有明显的降质现象，而隐藏的数据却无法人为地看见或听见。

（4）安全性（security）

（5）自恢复性

§7.1 信息隐藏技术

信息隐藏技术特性：

（1）鲁棒性（robustness）

（2）不可检测性（undetectability）

（3）透明性（invisibility）

（4）安全性（security）

指隐藏算法有较强的抗攻击能力。即它必须能够承受一定程度的人为攻击，而使隐藏信息不会被破坏。

（5）自恢复性

§7.1 信息隐藏技术

信息隐藏技术特性：

（1）鲁棒性（robustness）

（2）不可检测性（undetectability）

（3）透明性（invisibility）

（4）安全性（security）

（5）自恢复性

经过一些操作或变换后，可能会使原图产生较大的破坏，如果只从留下的片段数据 ，仍能恢复隐藏信号，而且恢复过程不需要宿主信号，就是所谓的自恢复性。

§7.1 信息隐藏技术

信息隐藏与数据加密的区别：

（1）隐藏的对象不同

加密是隐藏内容，信息隐藏隐藏信息的存在性。

（2）保护的有效范围不同

加密的保护局限在加密通信的信道中或其他加密状态下；而信息隐藏不影响宿主数据的使用，只是在需要检测隐藏的数据时才进行检测，之后不影响其使用和隐藏信息的作用。

（3）需要保护的时间长短不同

用于版权保护的鲁棒水印要求有较长时间的保护效力。

（4）对数据失真的容许程度不同

多媒体内容的版权保护和真实性认证往往容忍一定程度失真，而加密的数据不容许一个比特的改变，否则无法脱密。