

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

文A



信息隐藏的鲁棒性



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

文A



鲁棒性

定义

设 Σ 是一个信息伪装系统, P 是一类映射: $C \rightarrow C$, 若对所有的 $p \in P$

(i) 对私钥信息伪装系统, 恒有:

$$D_K(p(E_K(c, m, k)), k) = D_K(E_K(c, m, k), k) = m$$

(ii) 对无密钥信息伪装系统, 恒有:

$$D(p(E(c, m))) = D(E(c, m)) = m$$

而不管如何选择: $m \in M$, $c \in C$, $k \in K$, 则称该系统为 P -鲁棒性的信息伪装系统



安全性和健壮性的平衡

安全性高，健壮性差

安全性高，说明伪装对象与载体对象从概率分布上无法区别，因此信息的隐藏必须利用载体的随机噪声，而随机噪声容易被破坏。

健壮性强，安全性差

健壮性强，说明信息隐藏与载体的特性结合在一起，不易被破坏，但会改变载体的某些特征，并且有可能改变概率分布。



保持 α -相似性

一般情况下，只能针对某一类特殊的映射具有健壮性，比如，JPEG压缩与解压缩、滤波、加入白噪声等。

理想的信息隐藏系统应该对所有的“保持 α -相似性”的映射具有健壮性。

保持 α -相似性：

映射 $p : C \rightarrow C$ 具有性质 $\text{sim}(c, p(c)) \geq \alpha$ 且 $\alpha \approx 1$ 。



隐藏在何处？

鲁棒性算法应该把需要隐藏的信息放置在信号感观最重要的部分。

当一幅人脸图像不被破坏到无法识别出人脸这样的严重程度之前，都能够恢复出隐藏信息。

将隐藏信息与载体的感观最重要的部分绑定在一起，其鲁棒性就会强很多。