

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



信息隐藏的安全性



信息隐藏的安全性

信息隐藏系统的安全性

系统自身算法的安全性
各种攻击情况下的安全性

攻击一个信息隐藏系统

证明隐藏信息的存在
提取隐藏信息
破坏隐藏信息

理论安全的：如果攻击者经过各种方法仍然不能判断是否有信息隐藏，那么这个系统可以认为是理论安全的。



衡量两个概率分布的一致性

熵

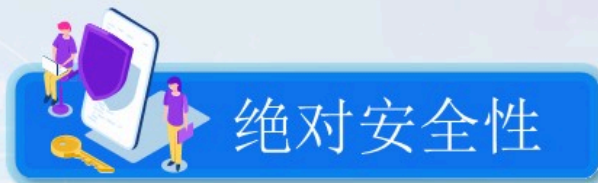
$$D(P_1 \parallel P_2) = \sum_{q \in Q} P_1(q) \log_2 \frac{P_1(q)}{P_2(q)}$$

P_1 和 P_2 : 定义在集合 Q 上的两个概率分布

P_1 : 真实概率分布

P_2 : 假设概率分布

- 当 P_1 与 P_2 完全相同时，熵D为零，说明假设的与真实的概率分布之间没有不确定性
- 当 P_1 与 P_2 不同时，D给出了假设的与真实的概率分布之间不确定性的衡量， P_1 和 P_2 之间差别越大，熵越大



绝对安全性

定义

设 Σ 是一个信息伪装系统， P_S 是伪装对象的概率分布， P_C 是伪装载体的概率分布。

- 若有： $D(P_C \| P_S) \leq \epsilon$ ，则称 Σ 抵御被动攻击是 ϵ -安全的。
- 若有： $\epsilon = 0$ ，则称 Σ 是绝对安全的。

结论

如果一个信息伪装系统嵌入一个秘密消息到载体中去的过程不改变 C 的概率分布，则该系统是（理论上）绝对安全的。



定理：存在绝对安全的信息伪装系统

构造性证明：

设 C 是所有长度为 n 的比特串的集合， P_C 是 C 上的均匀分布， e 是秘密消息（ $e \in C$ ）。

发送者随机选择一个载体 $c \in C$ ，产生伪装对象 $s = c \oplus e$ ， s 在 C 上也是均匀分布的，因此 $P_C = P_S$ ，并且 $D(P_C \| P_S) = 0$ 。



判断是否有隐藏

定义一个检验函数 $f: c \rightarrow \{0,1\}$

$$f(c) = \begin{cases} 1 & c \text{ 中含有秘密消息} \\ 0 & \text{其它} \end{cases}$$



判断结果

- ❁ 实际有隐藏，判断有隐藏——正确
- ❁ 实际无隐藏，判断无隐藏——正确
- ❁ 实际无隐藏，判断有隐藏——错误
 - ✓ 纳伪错误
- ❁ 实际有隐藏，判断无隐藏——错误
 - ✓ 弃真错误



实用的信息隐藏系统



对于一个 ε -安全的信息隐藏系统，假设：

攻击者犯纳伪错误的概率为 α

攻击者犯弃真错误的概率为 β

一个实用的信息隐藏系统应该尽可能使 β 最大

一个理想的信息隐藏系统应该有 $\beta=1$ ，即，所有藏有信息的载体都被认为没有隐藏信息而被放过，达到了信息隐藏、迷惑攻击者的目的。



ϵ -安全与概率 α 、 β 的关系

定理

设 Σ 是一个对付被动攻击者为 ϵ -安全的信息伪装系统，则攻击者检测不到隐藏信息的概率 β 和攻击者错误地检测出一个不是隐藏信息的概率 α 满足关系式： $d(\alpha, \beta) \leq \epsilon$ ，其中 $d(\alpha, \beta)$ 是按下式定义的二元关系熵：

$$d(\alpha, \beta) = \alpha \log_2 \frac{\alpha}{1-\beta} + (1-\alpha) \log_2 \frac{1-\alpha}{\beta}$$

特别地，若 $\alpha=0$ ，则 $\beta \geq 2^{-\epsilon}$

