

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



信息隐藏的分类



信息隐藏的分类



无密钥信息隐藏



私钥信息隐藏



公钥信息隐藏



无密钥信息隐藏

隐藏
过程

映射 $E: C \times M \rightarrow C'$

提取
过程

映射 $D: C' \rightarrow M$

C : 所有可能载体的集合

M : 所有可能秘密消息的集合

C' : 所有伪装对象的集合



双方约定嵌入算法和提取算法，算法要求保密



无密钥信息伪装系统

定义

对于一个五元组 $\Sigma = \langle C, M, C', D, E \rangle$ ，其中 C 是所有可能载体的集合， M 是所有可能秘密消息的集合， C' 是所有可能伪装对象的集合。 $E: C \times M \rightarrow C'$ 是嵌入函数， $D: C' \rightarrow M$ 是提取函数，若满足性质：对所有 $m \in M$ 和 $c \in C$ ，恒有： $D(E(c, m)) = m$ ，则称该五元组为无密钥信息伪装系统。



相似性函数

载体对象和伪装对象在感觉上不可区分，如何度量？

定义

设 C 是一个非空集合，一个函数 $\text{sim}: C^2 \rightarrow (-\infty, 1)$ ，对 $x, y \in C$ ，若满足：

$$\text{sim}(x, y) \begin{cases} = 1 & x = y \\ < 1 & x \neq y \end{cases}$$

则 sim 称为 C 上的相似性函数
相似度应尽可能接近1

文A



载体的选择

不同的嵌入算法，对载体的影响不同。

选择最合适的载体，使得信息嵌入后影响最小，
即载体对象与伪装对象的相似度最大。

$$c = \underset{x \in C}{\text{Max}} \quad \text{sim} (x, E(x, m))$$



私钥信息隐藏

Kerckhoffs准则:

密码设计者应该假设对手知道数据加密的方法，
数据的安全性必须仅依赖于密钥的安全性。

无密钥信息隐藏系统，违反了Kerckhoffs准则。



私钥信息隐藏

定义

对一个六元组 $\Sigma = \langle C, M, K, C', D_K, E_K \rangle$ ，其中 C 是所有可能载体的集合， M 是所有可能秘密消息的集合， K 是所有可能密钥的集合， $E_K: C \times M \times K \rightarrow C'$ 是嵌入函数， $D_K: C' \times K \rightarrow M$ 是提取函数，若满足性质：对所有 $m \in M$ ， $c \in C$ 和 $k \in K$ ，恒有： $D_K(E_K(c, m, k), k) = m$ ，则称该六元组为私钥信息隐藏系统。

私钥的传递：

密钥交换协议

文A



公钥信息隐藏

- ❁ 类似于公钥密码。
- ❁ 通信各方使用约定的公钥体制，各自产生自己的公开钥和秘密钥，将公开钥存储在一个公开的数据库中，通信各方可以随时取用，秘密钥由通信各方自己保存，不予公开。
- ❁ 公钥用于传递会话密钥。
- ❁ 会话密钥用来作为伪装密钥。



公钥信息隐藏(1)

A将自己的公钥隐藏在载体对象中发送给B

伪装对象1

B从伪装对象中提取出A的公钥

A从伪装对象中提取出隐藏的密文，再用A的私钥解密，得到会话密钥k

伪装对象2

B用A的公钥对自己随机产生的会话密钥k进行加密，并隐藏

A、B用会话密钥k作为伪装密钥，进行隐藏信息的交换

文A



公钥信息隐藏(2)

A用B的公钥对会话密钥k进行加密，隐藏在载体对象中

伪装对象1

B从伪装对象中提取出隐藏的密文，再用B的私钥解密，得到会话密钥k

A用会话密钥k实现私钥信息隐藏

伪装对象2

B用会话密钥k提取隐藏信息

文A



中间插入攻击

与公钥密码实现的密钥交换协议类似，用公钥信息隐藏进行密钥的交换，无法抵抗中间插入攻击。



中间插入攻击

A将自己的公钥隐藏在载体对象中发送给B

伪装对象1

B从伪装对象中提取出C的公钥
(误认为是A的公钥)

攻击者C

A从伪装对象中提取出隐藏的密文，再用A的私钥解密，得到会话密钥k

伪装对象2

B用C的公钥对自己随机产生的会话密钥k进行加密，并隐藏

A、B用会话密钥k作为伪装密钥，进行隐藏信息的交换。
此时C拥有密钥k，可以进行信息的监视和篡改

文A