

大数据行为分析与取证 从内容隐藏到行为身份隐藏

关于信息隐藏

加密通信：隐藏消息内容

隐写通信：不仅隐藏消息内容，还隐藏通信过程本身

例子

山西家书

跳舞的小人

信息隐藏的三重境界

见招拆招

一招致胜：特征+分类器

无招胜有招：对抗通用性统计监测，先隐藏后检测

三层对抗

破坏秘密信息

发现秘密信息

提取秘密信息

学术挑战

理论系统不完善

应用面对 AI、大数据创新不足

基于深度学习的隐写分析、隐写算法

AI可证安全隐写实例

语音合成隐写

生成图像隐写

隐写安全的本质：将信息藏到正常行为之中，本质是行为安全

追求与正常行为的不可区分性

大数据行为分析

检测四要素：人物时间地点行为

脸捕：人脸辨识技术

影析：遥感影像与数字地球、影像分析与行动指挥

人脉：关键人物脉络，从人物关系去分析

暗哨：分析公开数据，来获取关键信息

威胁溯源

大数据行为对抗