隐写文件的识别和解码工具——中国的Stegohunt——隐译

原创

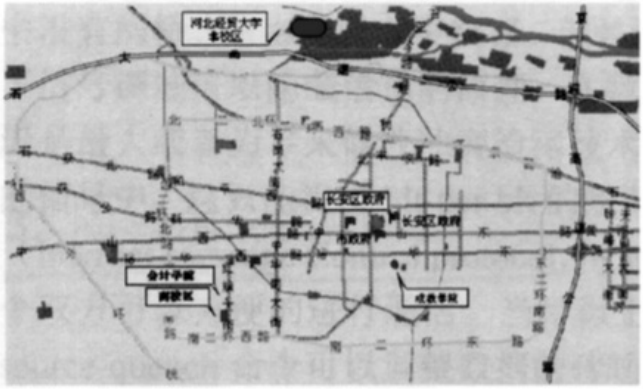
blueshark_tech 于 2021-07-22 15:10:01 发布 1004 收藏 1
文章标签： 安全 机器学习 网络安全

本文链接：https://blog.csdn.net/blueshark_tech/article/details/118891283

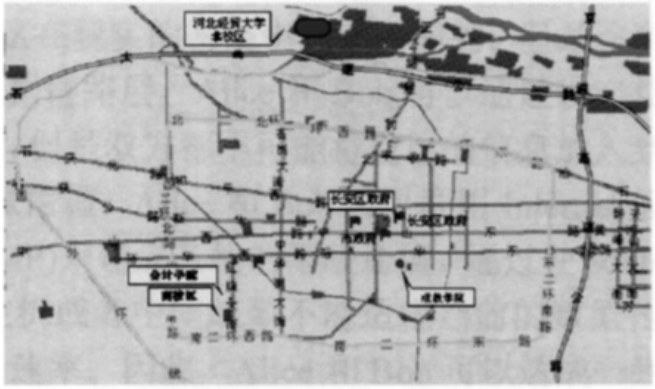
一、什么是隐写术？

隐写术是一门关于信息隐藏的技巧与科学，所谓信息隐藏指的是不让除预期的接收者之外的任何人知晓信息的传递事件或者信息的内容。

二、隐写术的使用



原始图片



嵌入密钥的图片

通常可以隐写的内容是很广泛的, 可以是音频、文章、图片或者任 何私密信息。所使用的载体可以是网上的任何一种媒介。隐写常见的 方式是将一个.txt者 .doc格式的文件或者是加密过的文件 、图片或者 密钥等镶嵌到其他伪装的载体中。如果将加密术和隐写术结合在一起, 发送的密文被第三方捕获的机率是很低的。隐写术中很重要的一个分 支是隐蔽通道,在前面所提到的隐写术,只是对某种媒介进行了隐写,而 其在网络中传输的过程并不安全,因为Internet是一个开放的环境, 那么 使用隐蔽通道则可以使隐写信息在安全的环境中传输，且达到很高的安全程度。

三、国内首款商用级隐写检测软件——隐写文件识别和解码工具（隐译）技术说明

福州蓝鲨信息技术有限公司研发的隐写识别和扫描解码工具——隐译，以国情出发，专为公检法公司企业服务，支持对图片、文档及压缩包及主流隐藏文件类型进行隐藏检测。找到隐写行为界定隐写证据。

1. 隐写文件库：

隐写文件库是使用隐写软件对载体文件嵌入秘密消息产生的载密文件的集合。它是隐译技术沉淀的支撑，提供了强大的测试平台。

隐写文件库包含以下几个方面：

①隐写软件库：当今主流的隐写算法已经超过数十种，而其中的分支高达数百种，我们通过合法技术手段从国内外各大中小型网站获取高达三百余种隐写软件，通过逆向手段将它们分类去重保存，确保隐译检测视野站在国际领先水平。

②载体文件库：隐写术的通用思想是使用密钥将秘密消息根据隐写信道嵌入载体文件得到载密文件。因此，载体文件的隐写信道的多样性需要得到保证。而载体文件库中存放了网站、手机、相机不同参数、不同比例的文件，以多样的隐写信道使得使用隐写术的成员无所遁形。

③载密文件库：使用不同的隐写算法自动生成隐写文件，使用十三大参数对隐写文件标记并分三档入库，根据评定检测算法的三种标准的综合的SACS（Steganalysis Assess Common Standard隐写评定通用标准），以达到高效的检测算法的测试效果。

说明：隐写评定检测标准SACS是一种GCS（Global Common Standard全球通用标准），它可以用来判断一种检测算法是否真正意义上的实际有效，有力保证隐写检测算法的高效性。

四、隐写文件的识别和解码产品市场行情

目前国内市场上关于这方面的技术只有两家，一家是国外Wetstone的产品“stegohunt”，另一家则是福州蓝鲨信息技术有限公司的“隐译”。前期由于该技术国内缺失，故stegohunt占据了市场，而四年前国内进行自主研发，打破了原有技术瓶颈和市场垄断。福州蓝鲨信息技术有限公司研发的产品——隐译，相较于stegohunt，无论从产品的性能、技术参数，易用性，以及客户的满意度来说都更加优秀。

竞品对比

对比项	蓝鲨信息	Stegohunt
隐写算法检测能力	70余种	80余种
隐写工具检测能力	500余种	450种
主流载体检测能力	支持主流工具生成载体检测	支持主流工具生成载体检测
产品稳定性	临界资源优化，支撑率良好	中文操作系统支持较差
训练样本集	一亿	数千万
产品来源	国产	美国，有潜在安全后门隐患
易用性	现代设计界面，易于使用	界面老旧，向导不友好，纯英文界面
复合型隐写检测结果	可以显示单文件叠加的多种隐写	只能显示一个隐写项
隐写算法信息	能够检测相应隐写算法的具体名称	只能显示“存在隐写”

五、试用申请流程

1.联系福州蓝鲨信息技术有限公司及其销售人员，

电话：0591-87573723 / 18649769781（陈*）；

2.提供用户信息，如：用户单位、申请人姓名、职务以及联系方式等内容；

3.与福州蓝鲨签订产品试用协议；

4.福州蓝鲨远程指导用户进行软件安装、试用激活和操作使用（无需培训）；

5.试用到期后归还福州蓝鲨；

六、关于蓝鲨

福州蓝鲨信息技术有限公司，简称蓝鲨，成立于2015年3月。公司主要业务为为公检法部门提供互联网协查取证与分析产品及其他定制化服务。

蓝鲨信息致力于为政企事业单位提供完善的信息安全解决方案。公司是第十一届G20峰会、第十一届厦门会晤、首届金砖三合一论坛的网络安全保障方之一。