哈尔滨工业大学
立项报告

项目名称：基于 CC_PEV 算法的图片隐写检测系统

项目负责人：卢兑玑 学号：L170300901

联系电话：82-1059395270

电子邮箱：nty0725@naver.com

院系及专业：计算学部

指导教师：职称：

联系电话：

电子邮箱：

院系及专业：计算学部

哈尔滨工业大学基础学部制表

填表日期：2021 年 07 月 21 日

一、项目团队成员（包括项目负责人、按顺序）

姓名	性别	所在院系	学号	联系电话	本人签字
卢兑玩	男	计算学部	L170300901		

二、项目简介

本项目主要有两部分组成：虚拟网关的搭建和图像隐写检测算法的实现。

将会通过用 python 语言模拟网关工作的过程，整个实验过程中将使用一台电脑作为信息的发送方，一台电脑作为虚拟网关检测，一台电脑作为信息的接收方。模拟整个网关的过程，其中 python 语言将会实现所有的检测过程。发送数据和接收数据也将使用 python 实现对所有文件的拆解、发送、接收、合并。

在隐写检测算法方面，将会从现有的算法基础上进行改进，得到更有效的算法。将使用一些深度学习方面的知识改进算法，使得算法具有更高的准确率。实验中将会对多种方式的隐写进行检测，判断出是否有隐写信息。

三、申请基础

项目小组的四名同学均来自计算学部，其中有三位同学编程基础较好，在编程方面比较有优势，研究出可行的图像隐写检测算法是可行的。所有的成员都对网关如何构建、如何工作的原理方面有一定的了解。在大一阶段课程内容较少，有时间去自学大量的知识，搭建虚拟网关也不是特别大的难题。

有信息对抗技术研究中心的韩琦老师和陈浩博士的指导，在遇到大的问题情况下可以向老师或者学长请求援助。在老师和学长的带领下，可以接触到一些实验室正在研究的技术，有机会将这些技术应用到自己做的项目中。

四、立项报告

（一）研究背景

网关无处不在。无论是互联网还是局域网，从一个网络向另一个网络发送信息都会经过一个关口，而这个关口就是网关。从学校、医院等公共机构到私有或是国有公司再到国家的各级机关，信息保密的重要性不言而喻，其中充当信息传递的审查者和拦截者便是网关。由此看来，网关就像是网络海洋中的海关。

对于整个国家来说，互联网安全的重要意义已经深入到了文化、经济甚至国防领域。而互联网安全重要性的日益提高，我们需要针对相关网络信息的漏洞做出具体的保护措施，保证能够最大限度地维护国家信息安全。

国家的总入口和出口网关承担了对整个互联网信息过滤的重任。正如贩毒者想尽一切办法将毒品带入国门，不法分子也总想着在网关的层层过滤下将国家的重要机密或不法信息传入传出互联网的国门。

如今的网关对传递的各类信息的过滤技术已较为成熟，而针对隐写检测的却相对较少，不法分子可以利用这个易被人忽视的途径，向网关外发送涉密信息而不被察觉，这轻则造成经济损失，重则泄露关键技术危害国家安全。

利用隐写技术达到入侵的目的也早有先例。在 2015 年就有俄罗斯黑客组织运用隐写术，借助 Twitter 中那些看似是照片的数据侵入了美国国防系统，并攻陷了国防部多台电脑。由此可见，针对图片隐写的检测势在必行。

（二）研究目的及意义

我们将通过研究图片隐写的算法，并检测图片的文件完整性和来源，编写出能够检测和过滤携带隐写信息和可疑图片的程序，再将其运用在模拟网关上。达到对图片的可信度评估和处理，从而维护互联网的安全。

（三）项目研究内容

1．研究图片隐写的算法

2．研究图片的完整性的检测方法

3．研究图片的局部处理的检测方法

4．研究对图片来源的分类处理

5．研究对图片可信度的评估办法

6．研究模拟网关的搭建和实现

（四）实施方案

1．对图片可信度检测并分类的实施方案

现行的基于图像的信息隐藏算法按嵌入域的不同，分为空域隐藏算法、变换域隐藏算法、语法结构隐藏和挂接算法。我们将针对其中的几种算法编写相应的写入隐藏信息软件，并将其模块化嵌入最终的检测软件中。

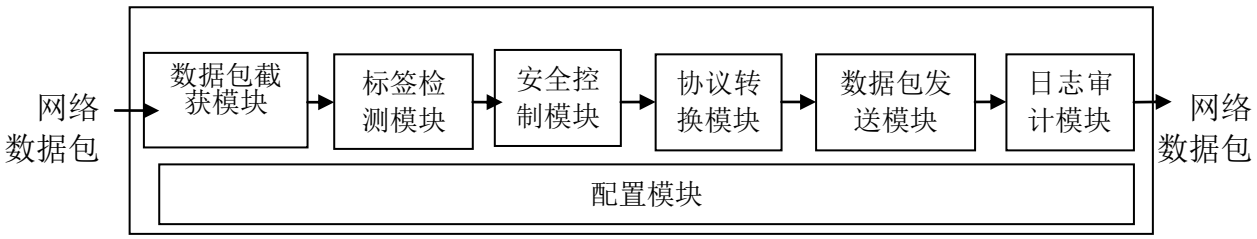
图片的可信度有很多的评价标准，在我们的检测体系中，图片是否携带隐写信息所占权重最高。图片属性中携带的详细信息也可以作为一种参考标准，如相机拍摄的照片，若未经处理便会储存拍摄时的相机型号、光圈、快门、作者甚至经纬度等信息。如果所传输的图片中含有这些信息，我们可以认为它是一个来源明确的信息；若该图片不含详细信息，则它的可信度会按一定权重削减。

图片等文件的完整性检测：计算机的各类文件都包含不同的文件头，这决定计算机会以什么样的方式来解读该文件。若将一个 jpg 文件直接修改后缀为 txt，打开后将是一堆乱码，反之也会出现无法打开的警告。而隐秘信息可能就通过这种方式被传播出去，我们要检测每个文件的文件头，若发现文件头缺失或文件头与文件后缀不符，可以按权重进行相应的处理。

如今图像处理软件盛行，经过刻意处理后传播的假图片也会对互联网产生恶劣的影响，我们要分析文件结构并检测图片是否经过局部处理，同样会对其按权重进行相应处理。

2．搭建模拟网关的实施方案

安全网关的模块化结构如图所示，主要包括数据包接收模块、标签检测模块、安全控制模块、协议转换模块、数据包发送模块、日志审计模块及配置模块。



首先根据数据流通规则及相关策略对网关进行相应配置，数据文件流经安全网关时由数据包接收模块接受并进行存储，并进行数据重组，再由标签检测模块检测该数据是否具有隐写标签：若有隐写标签，则由安全控制模块判断该标签是否合法有效，同时是否符合数据流通规则，若标签不符合数据流通规则，则将数据包丢弃并将日志传递给日志审计模块；若标签符合数据流通规则或无隐写标签，则调用其他检测模块进行检测，并进行可信度评价，若可信度较低则将数据包丢弃并将日志传递给日志审计模块；若可信度较高，则由数据包发送模块将该数据发送到目的主机。

网关内将设置接收缓冲区、发送缓冲区和存储区。数据包接收模块于接收缓冲区接收发送端的文件，接收完毕一个完整的文件便传入存储区，由网关模块进行处理，判断完毕后若具有一定可信度便传入发送缓冲区，由数据包发送模块发送至目的主机。这样便节省了文件在网关内滞留的时间。

（五）创新点

使用 python 模拟网关的工作过程，便于在小范围内做实验使用

将深度学习方面的知识应用于图像隐写检测的算法中

对传输的文件进行拆解后传输，加大传输效率

（五）进度安排

1．2017.12-2017.1.12（秋季学期末期）：在校期间完成 C，C++，数据结构与算法，编译原理四门课程的学习。

2．2018.1.13-2018.1.25（寒假前期）：初步了解 python,java 以及 matlab 语言的使用，并搭建开发所需要的语言环境同时搜集必要工具。

3．2018.1.26-2017.2.15（寒假中期）：搜集并学习已有隐写算法，并深入探讨检测方法的实现流程。

4．2018.2.16-2017.2.25（寒假后期）：着手分工实现程序的一小部分，并继续深入学习。

5．2018.2.25-中期答辩：完成中期检查所需各种材料的准备并继续编写。

6．中期答辩期间：计划完成对 2-3 种常见隐写算法的检测程序，并通过前期学习以及中期检查得到的结论，及时调整小组整个活动的流程及安排。

7．中期答辩至结题：完成并完善对已有隐写算法的检测方法，完成对图像完整度的检测，完成程序的 UI 设计以及模拟网关的实现，并在完善过程中深入探讨和研究，力求创新。

（六）中期及结题预期目标

1. 中期审核目标

1．完成编写图片隐写检测软件的前期知识储备工作；

2．尽力完成网关中一个或几个模块的编写（视工作进度和当时工作能力的调节，具有弹性）。

2. 结题预期目标

完成整个图片隐写检测网关的基本架构，完成代码的调试，使其能够运行。整个小组成员都对图片隐写和网关的运行机制有一个比较深的了解，为今后进一步学习其他模块的知识

打下良好的分析问题，学习知识，代码编写的基础

（七）经费使用计划

1．购置相关书籍及论文：350RMB

2．购置必要的开发工具：150RMB

（八）主要参考文献

[1] 郭艳格，图像隐写分析与检测，北京邮电大学：工程硕士研究生学位论文，2006.3.1

[2] 汪红星，沈勇，基于隐写标签的安全网关模型设计，江苏科技大学：工学硕士学位论文，2009.12

[3] 王岩岩，武亚菲，隐写术的应用及安全性研究[J]，计算机时代，2012 年 03 期

[4] 葛秀慧，胡爱华，田浩，王嘉祯，隐写术的研究与应用[J]，计算机应用与软件，2007 年 11 期

[5] 周治平，林家骏，王永志，基于调色板图像的隐写算法研究[J]，华东理工大学学报(自然科学版)，2006 年 12 期

指导教师意见： 课题组已经对问题进行了全面调研和分析，准备了数据和技术资料，提出了解决方案和思路，同意申请立项。 指导教师签名：韩琦　　年　　月　　日
院系审核意见： 院系负责人签名：　　年　　月　　日
学院专家组评审意见： 组长签名：　　年　　月　　日
学校认定意见及批准经费： 负责人签名：　　年　　月　　日