Steganography Project Proposal

Linden Crandall, Jonathan Mainhart, Zhihua Zheng

University of Maryland Global Campus

CMIS 495: Current Trends and Projects in Computer Science

Prof. Majid Shaalan

March 19, 2022

Introduction

Steganography is an information encoding technique that has been used throughout history to send secret messages without attracting attention. Ancient Greeks used to hide messages on the bare scalps of messengers then wait for the hair to grow back to safely deliver the message (Kleiman, 2011). During periods of war hidden messages were constantly generated and destroyed using different methods that evolved over time. Presently, steganography is widely used to add digital watermarks and conduct secret conversations. It is also a well-known method to embed malicious code used to steal sensitive data from users. To protect a user from a such situation, it is important to be able to detect and reveal secret data from a suspicious resource.

For this 8-week project, our team aims to build an image-based steganography application that can both encode secret conversations and reveal the secret data of an uploaded image from the user.

Problem

Privacy in personal communication is at an all time low. Everyday people need a way to communicate with each other without the fear of their messages being read by eavesdropping corporations and governments. Messaging services that claim to be encrypted have been hacked which may lead people to wonder whether any computer system is ever truly secure ("WhatsApp hack: Is any app or computer truly secure?").

Solution

To securely hide and reveal the secret data, our team will create an easy to use, GUI application which allows a user to encode a plain text message inside of an image file. The image can then be sent to a receiver who can decode the hidden message.
The application will be written in Python 3.9 and run on any system with Python 3.9 or newer installed.

Objectives

The application will have the following features:

1. The ability to select a locally saved image using a file picker
2. The ability to type a custom message to encode within the file
3. The ability to decode a message stored inside of a chosen file
4. The ability to rename a file when saving the image
5. The ability to overwrite a file when saving the image
6. The application will ensure the file size is adequate to contain the message before attempting to encode the message
7. The application will gracefully handle all file I/O errors.

References

BBC News. (2019, May 15). WhatsApp hack: Is any app or computer truly secure? https://www.bbc.com/news/technology-48282092

Greene, S. (2020, December), CompTIA Security+ SYO-610. *Lesson 16: Summarize the Basics of Cryptographic Concepts*. Pearson IT Certification.

Kleiman, D. (2011, August), The Official CHFI Study Guide (Exam 312-49*). Chapter 7: Steganography and Application Password Crackers.* Syngress.