**Project Proposal**

Jonathan Mainhart, Linden Crandall, Zhihua Zheng

University of Maryland Global Campus

CMIS 495: Current Trends and Projects in Computer Science

Prof. Majid Shaalan

March19, 2022

* **Introduction**

Steganography is an ancient practice that has been used to send secret messages without attracting attention. Historically, the ancient Greeks used to hide messages on the messenger’s bare scalp and waited for their hair to grow back to safely deliver the message (Kleiman, 2011). Especially throughout war periods, hidden messages were constantly generated and destroyed through different methods and evolved overtime.

Presently, steganography is widely used to add a digital watermark to the electrical properties and conduct a secret conversation. It is also a well-known method to embed malicious code 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 convert 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 use two keys, a public key, and a private key, to encrypt and decrypt the target data. This is also known as asymmetric encryption. Unlike symmetric encryption that only uses one public key to encrypt and decrypt the data, asymmetric encryption is much more secure because the private key will be kept a secret and only used to decrypt the data.

The application will be written in Python 3.9 and run on any system with Python 3.9 or newer installed.

* **Objectives**

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 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

5. The ability to overwrite a file

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 and alert the user

**Reference**

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.