Faculty of Engineering & Applied Science

SOFE 4840U - Project Abstract

Feb 06, 2023
Project Group 11

Name	Student ID
Ivan Bisol	**100701735**
Manreet Kaur	**100766207**
Gobikah Balaruban	**100742539**
Gutu Shiferaw	**100767090**

1. Project Background

Steganography is the process of hiding information within an object, such as an image, to conceal it from viewers. The data is concealed in a way that is unable to be detected by simply viewing and inspecting it with the human eye. This method of information hiding is useful as a regular viewer would not suspect a secret message to be hidden within the document/media that they are viewing. This differs from cryptography, as it hides the data rather than transforming it into something not understandable. Both techniques are useful for information hiding, but steganography is helpful in cases where information needs to be concealed without any suspicions.

Steganography is a method that has been used many times throughout history. There have been traces of steganography being used in ancient Greece and during the world war, where spies would use knitting with a secret message by leaving a hole for instance [1].

Steganography has been present for many centuries physically but now modern steganography is revolving around digital media. In the digital world, there are many ways to conceal messages using this method including text steganography, audio steganography, and image steganography. Recently, the use of steganography is becoming more and more significant with the amount of data traffic that occurs through the internet and social media networks [2].

Image steganography is done by hiding data, for example, an image, inside another image called the “cover image”. The cover image conceals the hidden data in a way that is not visible or suspicious to the viewer. In order to detect if there is hidden data and the details of the data, steganalysis is used.

Steganalysis is used to detect if an image is a steno image that has hidden data or a regular image. If the image is a steno image, it is analyzed to find out what information is hidden within the cover image.

2. Project Purpose and Objectives

The goal of this project is to build a Python application so that users can easily hide text messages or text files within image files. Users will also be able to use the same program to reveal any hidden messages contained within an encoded image.

Users will be able to encode/decode their messages either as plaintext or using AES-CBC encryption before encoding into the image. On decoding images, users will be asked if they want to receive the plaintext output or enter a key for decryption. Users will always be prompted to enter a key to not provide any insight into if the message has been encrypted or not.

We aim to accomplish implementation of all the above requirements by March 15th by efficiently delegating the workload across all members of the team.

Any additional ideas/features that we come across will be implemented by March 27th if feasible, however we don’t want to fall victim to feature creep so core functionality will remain within the same scope. During this time some members will also be assigned to work on the report and presentation of the final product.

3. Project Scope

As mentioned above the primary scope of our project is to have core functionality (encoding and decoding text within an image with optional encryption) fully functional by March 15th. The goal for that iteration of the project will be to encode both a .txt file into an image and a user inputted text message into a separate image as well as successfully decode the resultant image files.

Between March 16th and March 27th, we will aim to add additional functionality to the application such as batch processing or multiple encryption modes, however we will prioritize functionality and bug fixing over the implementation of new features. The goals for this iteration will vary depending on exactly which features we aim to implement.

4. Deliverables

A few major deliverables exist for this project. The first deliverable will be our initial program which will be submitted by March 16th. This initial build will provide the absolute core functionality of our project. The second deliverable will be our final build after any necessary maintenance and enhancements as per the project description and will be submitted by March 27th. The second deliverable will also consist of the final report detailing everything we've done for the project. The final deliverable will be the presentation and live demo of our product which will occur sometime between March 27th and 31st.

5. Project Timeline

We will spend roughly a week researching how to implement steganography with Python and what libraries will be needed to handle the image processing. Additionally, we will research how to properly implement the AES-CBC encryption with Python. After this research phase, we will spend roughly the next month actually designing and programming the Python script that we will use. Allotting this much time to the initial development will give us lots of float room in case things come up such as unforeseen issues or heavier workloads from other courses. At the end of the development phase, we will have a few days left to fix any major outstanding bugs before the due date of the first deliverable of March 16th.

Afterwards, we will repeat the same process of a development phase and a bug fixing stage with a reduced timeframe to hit our due date of the second deliverable by March 27th. As mentioned above, during this time part of the team will also be delegated to work on the presentation and report.

6. Project References

[1] Widerview, “Steganography: From its origins to the present,” *Telsy*, 28-Dec-2021. [Online]. Available: https://www.telsy.com/steganography-from-its-origins-to-the-present/#:~:text=The%20origins,as%20a%20book%20about%20magic. [Accessed: 05-Feb-2023].

[2] “Image steganography: A review of the recent advances | IEEE journals ...” [Online]. Available: https://ieeexplore.ieee.org/document/9335027. [Accessed: 05-Feb-2023].