COMPUTER NETWORK SECURITY

PROJECT SYNOPSIS:

STEGANOGRAPHY

Ganesh K. 01FB15ECS104

Mohammad Salamuddin 01FB15ECS175

SYNOPSIS

Introduction

Wiki: Steganography is the practice of concealing a file, message, image, or video within another file, message, image, or video. Steganography includes the concealment of information within computer files. In digital steganography, electronic communications may include steganographic coding inside of a transport layer, such as a document file, image file, program or protocol. Media files are ideal for steganographic transmission because of their large size. For example, a sender might start with an innocuous image file and adjust the color of every hundredth pixel to correspond to a letter in the alphabet. The change is so subtle that someone who is not specifically looking for it is unlikely to notice the change.

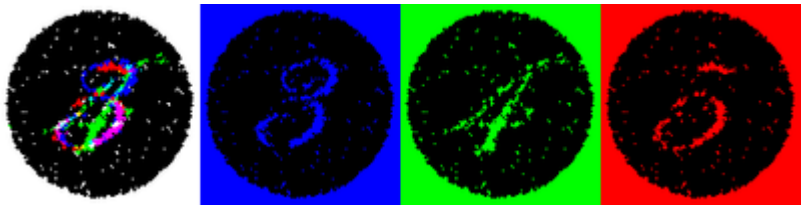


Figure 1 The same image viewed by white, blue, green and red lights reveals different hidden numbers.

Project Scope

The main aim of choosing this project is to get an in-depth knowledge as to:

- **What** Steganography is,
- **How** it is achieved and
- **Where** it is used.

In order to achieve these goals, we shall do the following:

- Do a **comparative study** on the existing steganographic techniques (three most popular ones).
    - Substitution Methods (Spatial-Domain)
    - Transform Domain Methods
    - Statistical Methods
- Study the various methods in which they can be **attacked** and how they try to **defend** it.
- Design a new steganographic method similar to existing techniques but tailored to a very specific use case. We shall also implement this and demonstrate.

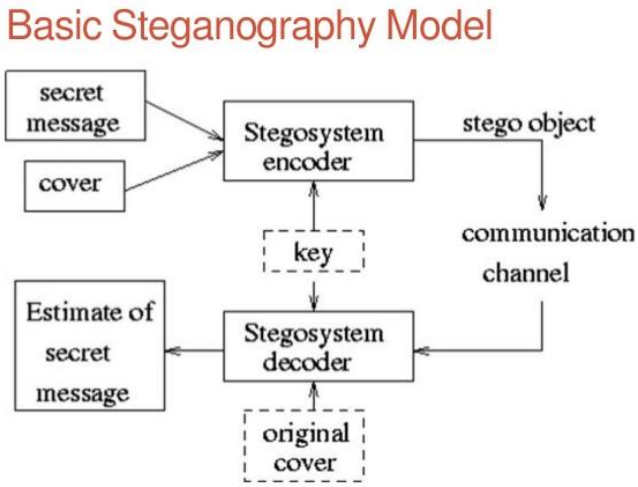
Methodology

Image Steganography (Data Embedding Algorithm):

- Extract the pixels of the cover image, Extract the characters of the text.

- Extract the characters from the Stego key. Choose first pixel and pick characters of the Stego key and place it in first component of pixel.
- Place some terminating symbol to indicate end of the key.
- Insert characters of text in each rst component of next pixels by replacing it.
- Repeat previous step till all the characters has been embedded.

For audio, we shall look into more approaches and try them before choosing which we shall go ahead with.



Papers

- *Image Steganography:*
  https://www.academia.edu/15184772/IMAGE_STEGANOGRAPHY

  This paper gives a fairly good Introduction as to what is digital Image Steganography. The paper presents an existing approach of image steganography using Least Significant Bit (LSB) algorithm and Discrete Cosine Transform (DCT) algorithm is to be used to compressed the images.

- *Comparative Study: (2010)*
  https://www.sciencedirect.com/science/article/pii/S0165168409003648

  This paper provides a state-of-the-art review and analysis of the different existing methods of steganography along with some common standards and guidelines drawn from the literature. This paper concludes with some recommendations and advocates for the object-oriented embedding mechanism.

- *Audio Steganography: (2017)*

  https://link.springer.com/article/10.1007/s11042-016-4113-8

This paper proposes an efficient steganography scheme based on sample comparison in Discrete Wavelet Transform (DWT) domain where the cover audio is decomposed into several multi sub-bands, and then selected coefficients of details are changed by a threshold value depending on the embedding cipher image bit.

- *Another Comparative Study: (2013)*
  https://arxiv.org/ftp/arxiv/papers/1401/1401.5561.pdf
  This paper is an attempt to analyse the various techniques used in steganography and to identify areas in which this technique can be applied

Approach

We aim in completing the project in three phases:

1. Understand the various methods (literature survey) of steganography by going through tutorials, existing tools and code. Study the recent developments in the field after mastering the basics.
2. Make a demo of usage of the tools and also find out the underlying algorithm and scan it for strengths and weaknesses. We shall focus mainly on Image and Audio steganography.
3. The final step shall be to make our own steganographic technique by incorporating all the knowledge we obtained so far and focus our attention on a specific use-case which will mostly be a multi-channel, multi-user steganography algorithm which will be designed and coded from scratch.

Milestones

We shall complete the projects in phases as mentioned above, here is the timeline:

- 12th March to 19th March: Phase 1
- 19th March to 26th March: Phase 2 (Midterm)
- 26th March to 15th April: Phase 3

Tools

1. Audio Steganography:
   - Coagula (Tool to make sound from Image)
   - Audacity (Open-Source software for recording and editing audio)
2. Image Steganography:
   - Xiao Steganography (Windows tool for Image Steganography)

Environment

We aim at sending and receiving steganographic data across two systems by sending images and audio between them and test the validity of the received data. In our approach, we shall try to add in more secure encryptions of the keys and patterns. To test this, we will launch a man-in-the-middle and attack and try to demonstrate the security.

References

- Youtube:
  - https://www.youtube.com/watch?v=TWEXCYQKyDc
  - https://www.youtube.com/watch?v=q3eOOMx5qoo
- Other:
  - http://www.instructables.com/id/Secret-Message-in-Audio/
  - https://steganosaur.us/dissertation/tools/cryptography
  - http://resources.infosecinstitute.com/steganography-and-tools-to-perform-steganography/#gref
- Code:
  - https://github.com/RobinDavid/LSB-Steganography
  - https://danielcardeenas.github.io/audiostego.html
  - https://www.mediafire.com/folder/muzrl9brx0z7f/Odds%26Ends

Work Split

- Ganesh K: Image steganography & custom algorithm
- Salam: Audio steganography & custom algorithm

Acknowledgement

- This project is developed as part of finals for Computer Networks Security.
- We would like to thank our professors, Dr. Alka Agrawal and Prof. Amulya G