Research Paper #2 - ‘A Review on Image Steganalysis techniques for attacking Steganography’

Learning Objectives:

- Understand and review the core concepts of steganography
- Understand the fundamentals of image steganalysis and techniques
- Create a summary of notes for reference

Overview

> *“Steganography is a data hiding technique that embeds the secret message inside a digital media for providing a method of invisible communication”*

- Steganography plays a critical role in cybersecurity, digital forensics, and intelligence operations.
- Steganography does not change the structure of the message itself to be concealed within a medium

> *“The method to detect steganography is called steganalysis.... “The role of steganalysis is to detect and estimate hidden data inside a digital file from observed data with little or no knowledge about the steganography method and/or its parameters.”*

- This paper will review the following steganalysis techniques

- Targeted Steganalysis:
  - Visual Attacks
  - Statistical Attacks
  - Structural Attacks
- Blind Steganalysis

Summary

Targeted Steganalysis

> *"...designed to evaluate mechanisms of particular embedding operations and fully utilizes the knowledge applicable to detect steganography"*

- This approach focuses on detecting a specific steganographic technique or tool

Visual Attacks

- The simplest form of steganalysis - involves detecting anomalies within the image using human observation or image processing tools
- Relies on steganographic techniques failing to adequately conceal the message - some odd features/distortions are left behind

> *"...visual attack depends on three factors holding true for being successful. The message must be embedded in a sequential order, its length must be less than the maximum size of the bit plane and it should not be encrypted."*

- If embedding is sequential, patterns may emerge.
- If the message is too long, it leaves stronger distortions.
- If the message is unencrypted, recognizable data structures might still be visible.

Statistical Attacks

> *"The statistical analysis of the images by some mathematical formula detects the presence of hidden data. Statistical attack is partially similar to visual attack. Generally the hidden message is more random than the original data of the image thus finding the formula to know the randomness reveals the existence of data."*

- Analyzes the statistical properties of an image to detect irregularities caused by steganography
- Based on the idea that steganographic embedding distorts pixel distributions - somewhat similar to visual attacks
- A specific type of statistical attack is Chi-Square Analysis, which measures statistical changes in pixel values (used for LSB detection)

Structural Attacks

> *"The attacker may detect the existence of secret message by examining the statistical profile of the bits or by identifying these characteristic structure changes. Structural attacks rarely analyse each image on its own merits. Instead, the images are scanned to see if they contain any of the known sideeffects for various steganographic algorithms."*

- Exploits the structural changes in an image file introduced by steganography
- Works by detecting format inconsistencies or metadata change
- Techniques:
    - RS Analysis: Detects LSB embedding by analyzing pixel relationships
    - Pair Analysis: Examines adjacent pixel pairs to find unnatural correlations

Blind Steganalysis

> *"Blind steganalysis is an approach is needed that is capable of identifying the probability of embedding, even when it is not sure how the information might have been embedded. Blind steganalysis does not require prior knowledge about details of the embedding operations."*

- An approach that attempts to detect hidden data without prior knowledge of the algorithm used - would be prevalent in machine learning models
- The most relevant blind steganalysis technique would be Supervised Learning-Based Steganalysis:
  - Uses a classifier trained on known stego and normal images
  - The classifier iteratively updates itself based on its predictions

Citations

Laskar, S., & Hemachandran, K. (2014). A Review on Image Steganalysis techniques for attacking Steganography. In ijert.otg. https://www.ijert.org/research/a-review-on-image-steganalysis-techniques-for-attacking-steganography-IJERTV3IS11136.pdf

ChatGPT Q&A

https://chatgpt.com/share/67d7e535-a2dc-8001-b96b-e61ba2c0ecf0