**Media Security Research Report – Covert Communication with Steganography**

**Jordan McDonald - 40063974**

**Sean Devlin**

**Paul Wright**

**Ryan Gribben**

1. **Introduction**

Steganography is the process of concealing images, video, audio, file or message within another type of media with the goal of allowing covert communication. The main requirement of steganography is to ensure the embedded message or media is statistically undetectable with less emphasis placed on the effect on the cover work. This indicates that watermarking requirements such as invisibility are not as important, therefore cover works are chosen which can hide the message effectively. However steganography also has concern about the fidelity of the cover image once the message is embedded, as plainly visible manipulated images will arouse suspicion. To balance this requirement certain steganography methods involve LSB substitution in order to maintain the fidelity of the cover image, to further support this textured images is often selected to hide the effects of embedding a message to the media.

In this research document multiple steganography methods have been implemented using a set of 800 images (bitmap) as the cover work, details of these techniques are presented in section two. The dataset will be inputted to a program that performs the various embedding techniques, it will then become possible to utilise a rich model based steganalysis program developed in [1]. The steganalysis program uses high-dimensional statistical image descriptors that have been shown to substantially improve classical (binary) steganalysis. The system is based on gradient boosting and utilizes a steganalysis-specific variant of regression trees as base learners. The research in this report will analyse the results of applying the embedded images against this program, from which comparisons and conclusions can be drawn about each steganography technique.

* 1. **General Project Approach**

Attack Type (or no attack)

Embedded Dataset

Stego-Embedding

Image Dataset

Output Data

Steganalysis project

Attacked Image

**1.2 Literature Review**

The general approach taken in [2] concerns the establishment of a new steganography technique that is robust against visual and statistical attacks while also maintaining a high message capacity. Known as F5 this method employs permutative straddling to uniformly spread out the changes over the whole steganogram and matric encoding to reduce changes therefore improving embedding efficiency. The paper in question also provides information for a series of information hiding techniques such as F3, F4 and Jsteg in order to consider the weaknesses of each and why F5 is a significant leap forward in the field.

The paper [3] instead of presenting a new method of hiding information takes a stance of providing an in-depth literature review of steganography and steganalysis. To fulfil this the paper presents details on various embedding algorithms such as various interpretations of outguess and the other methods mentioned in the prior paper, this helps provide a supplementary resource that was crucial in developing the algorithms in this research document. In addition to this the paper investigates various attacks that may be applied, these are a good test of robustness and can reflect what may occur in a real life context.

1. Summary of the Techniques

This section provides an in depth description of every steganography technique that has been applied to the dataset. Each subheading is appended with the person(s) in the group who implemented the technique and designates who is responsible for the analysis, embedding and extraction has been investigated in each section. As a side note as a side effect of the chosen papers possibly all covering one technique in various degrees the information provided here is a synthesis of the various source, however the intent behind the algorithms should provide a the same outcome.

* 1. LSB Embedding
  2. Jsteg Embedding (Jordan McDonald)
  3. F3 Embedding (Jordan McDonald)
  4. F4 Embedding
  5. F5 Embedding

Comparison

Conclusion

References

[1] J. Kodovský and J. Fridrich, Quantitative Steganalysis Using Rich Models, SPIE, Electronic Imaging, Media Watermarking, Security, and Forensics XV, San Francisco, CA, February 3-7, 2013.

[2] Andreas Westfeld, F5-A Steganographic Algorithm, IHW '01 Proceedings of the 4th International Workshop on Information Hiding, Pages 289-302

[3] Philip Bateman, Image Steganography and Steganalysis, http://chemistry47.com/PDFs/Cryptography/Steganography/Image%20Steganography%20and%20Steganalysis.pdf