Improved Steganography Algorithm

Daniel Hislop - 2317990H
Supervisor - Dr Ron Poet

Motivation

- Steganography is the practice of concealing information.
- The BPCS algorithm produces embedding signatures, meaning it is vulnerable to digital analysis.
- JPEG images are more likely to be found in the wild. The compression used in this process will lead to secret communication potentially being lost.
- Different techniques are required to account for lossy compression.

Overview

- Prioritised Requirements using the MoSCoW method.
- System architecture. Three Main components, the BPCS Tool, JPEG Tool and Detection Tool.
- Each tool is implemented as a command line application
- Development Language - Python
- Libraries Used - Pillow, OpenCV, Numpy, Argparse, Plotly, Sphinx

System Evaluation

- Systematic approach to evaluation
- BPCS Tool
- Algorithm Comparison - Visual and digital detection phases
- JPEG Compression - Mean square error and peak signal to noise metrics
- JPEG Steganography - LSB, TLSB and TLSBRandom algorithms.
- Detection Tool - Three remaining cases evaluated.

Conclusion

- BPCS Tool - Correctly performs embedding and extraction operations
- Variable complexity modification reduced rate of digital detection, RBEO has no effect
- JPEG Tool - Quality of images sufficient. Steganography techniques not as suitable for secret communication
- Detection Tool - Implementation of four detection cases

Future Work

- Implement modifications that better address the steganalysis technique used in the detection tool
- Addition of a GUI
- Address Limitations of visual detection evaluation phase
- Add JPEG steganography support for 24-bit colour images.
- Create novel encoder rather than rely on OpenCV to create image.

Thank you for listening!