Bits and Pieces: Steganalysis for Least Significant Bit Replacement

Macy Neblett[2], Madelaine Quistgaard[4], Amanda Rae[3], Kahlil Sample[1], Anna Steffensmeier[3], Dr. Jennifer Newman[3], Stephanie Reinders[3]
Albany State University[1], Fayetteville State University[2], Iowa State University[3], Upper Iowa University[4]
Iowa State University Research Experience for Undergraduates

Introduction

Steganography is the process of hiding a message, or *payload*, inside of a digital image, or *cover* in a way that is imperceptible to the human eye. An image with hidden data is referred to as a *stego*. Steganalysis is the study of detecting whether an image contains hidden data.

Creating Stego Images

We created stego images using the following:

- Payloads: bit-strings of zeros and ones
- Covers: 256-grayscale png images
- Embedding rates: 10%-90%
- Embedding algorithms:
    1. Lexicographical Least Significant Bit (LSB) Replacement
    2. Random LSB Replacement

LSB replacement embeds a payload in a cover by replacing the least significant bits of the cover's pixel values with the payload bits.

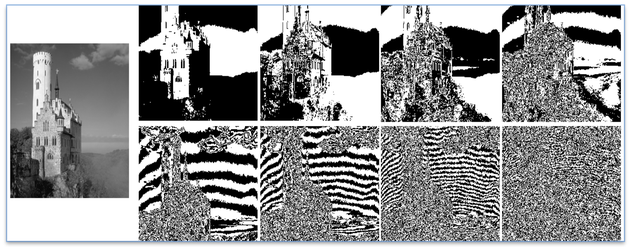

Figure 1: The eight bit planes from most significant bit to least significant bit[4]

Materials and Methods

This research is divided into three main parts:

1. Creating stego images
2. Applying chi-square attack to determine whether an image is stego or cover
3. Generating receiver operating characteristic (ROC) curves to measure the accuracy of the chi-square attack

This is all accomplished using the computer program MATLAB.

Chi-Square Attack

A chi-square goodness-of-fit test is used to determine how well the model reflects the observed data.[1] During LSB embedding, the pixel values within one pair {2k, 2k+1} k=0,1,…,127 remain locked in that pair. In a stego the expected number of pixels with value 2k denoted $h[2k]$ is the average of the number of pixels with value 2k and 2k+1 denoted $\overline{h}[2k]$. This characteristic allows us to use a chi-square goodness-of-fit test with test statistic below.

$$S = \sum_{k=0}^{127} \frac{\left(h[2k] - \overline{h[2k]}\right)^2}{\overline{h[2k]}}$$

Results

We applied the chi-square goodness-of-fit test to the first one percent of pixels, then the first two percent of pixels and so on to 100%. We obtained a p-value for each percentage tested and displayed all one hundred p-values in a "P-Graph." We created P-Graphs for each cover and stego image.

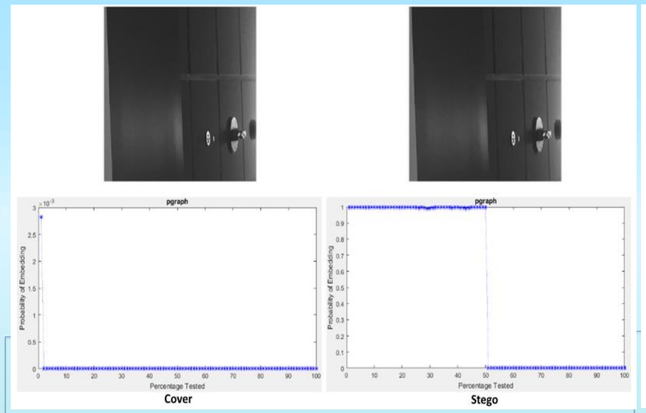

Figure 2: Lexicographical LSB Replacement with P-Graphs
A cover image will have p-values at zero, whereas the stego has p-values at one where the image is embedded. The p-values drop to zero when the image is no longer embedded with the message.

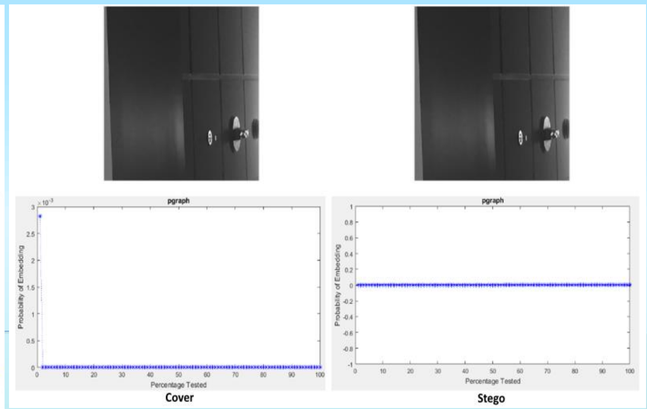

Figure 3: Random LSB Replacement with P-Graphs
Both the cover and the stego images' p-values are at zero. This demonstrates that the chi-square attack is not effective for detecting stego images that were embedded randomly.

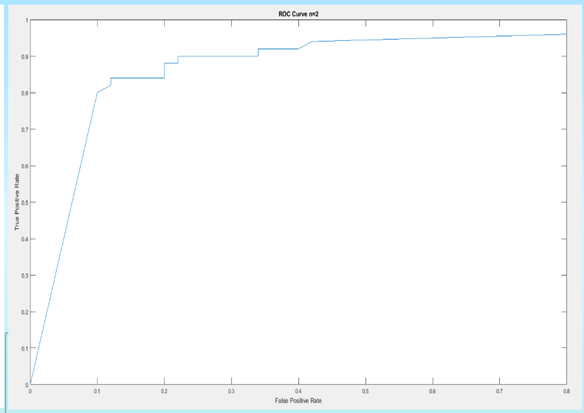

Figure 4: ROC Curve
A receiver operating characteristic curve is used to show the overall accuracy of a test. The ROC curve is created by plotting the true positive rate against the false positive rate.

Conclusions

The p-graphs generated from the chi-square attack show that the chi-square attack is effective in detecting stego images that were embedded in the least significant bit lexicographically. The p-graphs also demonstrate that this method is not effective for detecting stego images that were embedded using other methods. The ROC curves generated from the p-values of the cover and stego images demonstrates the accuracy of the chi-square attack. This research lays the foundation for future studies into other methods of detecting stego images that were embedding using non-lexicographical LSB replacement.

References

[1]Chi-Square Goodness of Fit Test. (n.d.). Retrieved July 24, 2017, from http://www.stat.yale.edu/Courses/1997-98/101/chigf.htm
[2]Fridrich, J. (2010). *Steganography in digital media: principles, algorithms, and applications*. Cambridge: Cambridge University Press. Print.
[3]Mandal, J. K., Satapathy, S. C., Sanyal, M. K., & Bhateja, V. (2017). *Proceedings of the First International Conference on Intelligent Computing and Communication*. Singapore: Springer Singapore. Print.
[4]P. Buonora and F. Liberati. A format for digital preservation of images: a study on JPEG 2000 file robustness. *D-Lib Magazine*, 14(7/8), August 2008.

Acknowledgements

Center for Statistics and Forensic Evidence (CSAFE); National Institute of Standards and Technology (NIST); Sam Tyner, Statistics Department, Iowa State University; Joe Papio, Statistics Department, Iowa State University.

This work was partially funded by the Center for Statistics and Applications in Forensic Evidence (CSAFE) through Cooperative Agreement #70NANB15H176 between NIST and Iowa State University, which includes activities carried out at Carnegie Mellon University, University of California Irvine, and University of Virginia.