StegFinder, a Forensic Tool to Detect Messages Hidden in Images

Seth Pierre[1], Abby Martin[2], Wenhao Chen, Li Lin, Roy Maxion*, Yong Guan, Jennifer Newman[3]

Iowa State University, *Carnegie Mellon

[1]shpierre@iastate.edu, [2]abby2@iastate.edu, [3]jlnewman@iastate.edu

Background & Goals

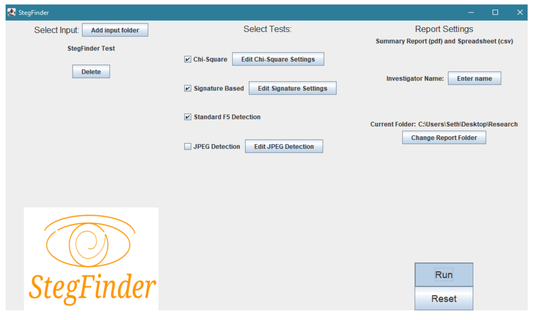
Steganography is the science and art of hiding a message in an innocent-looking image called a stego image.
• The use of steganography in images is on the rise.
• Stego images are created by coding applications that make visually undetectable changes to the image.
• Mobile steganography apps make steganography easy for users to create stego images, while detection is typically challenging.

Current Freeware Tools can detect stego images created by apps or other programs
- McAfee Steganography Defense initiative: web-based, very limited
- StegExpose: limited to only bitmap image formats, limited detection methods
- VSL: poor user interface, report not informative
- None of these tools are created specifically to target stegos created by mobile apps.

Goal: Create an efficient and useful forensic tool for investigators to detect stego images from mobile apps.
- StegFinder is a GUI software that is an initial step towards this goal.
- User friendly, runs reliably on Windows and MacOS (in progress).
- It can process 1-5,000 images for detection.
- A report is generated giving a summary as well as details of the analyzed results (in progress).

User Interface for StegFinder

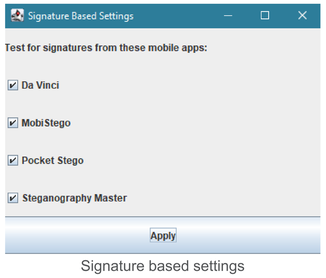
StegFinder is programed in Java with an Eclipse IDE, using six libraries in addition to from the standard ones. During creation and testing of StegFinder we have used data from the StegoAppDB to verify that the program detects stegos properly.



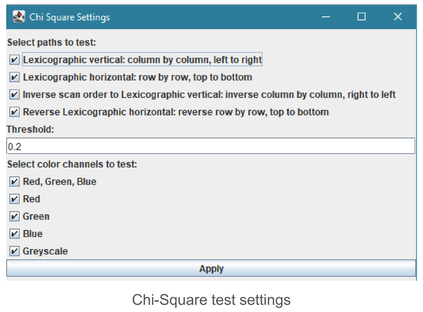
StegFinder home screen

- Currently StegFinder operates as a GUI
- It allows three folders to be selected to input images.
- Users customize test and settings be used
- Easy to reset to default settings

- Additional screens appear when clicking “Edit Settings”, in the middle column of the home screen



Signature based settings



Chi-Square test settings

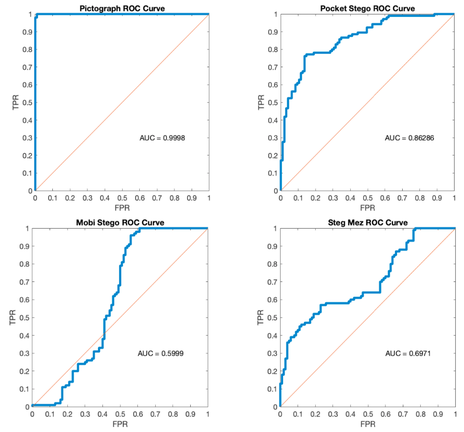
StegFinder Detection Techniques

- Two detection techniques to detect stegos: statistical method and signature method.
- StegFinder uses the file format of the image to apply detection methods.

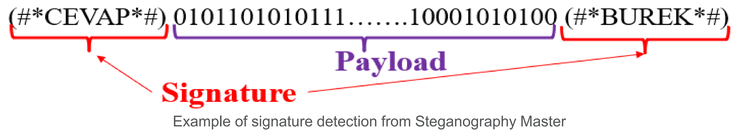
Bitmap formatted images – TIFF, BMP, PNG
- Uses the Chi-square test and signature detection
- Chi-Square: goodness-of-fit applied to pixel intensity distribution to match with expected stego intensity distribution

JPEG formatted images
- Uses signatures in PixelKnot: need password
- F5: Looks for specific string of characters in header of file.

Signature detection
- Looks for specific strings in the headers, pixel LSB locations, Exif metadata etc. put in by developer
- StegFinder test 5 mobile apps for signature detection



Chi-Square ROC Curves from StegFinder



Example of signature detection from Steganography Master

Reports

Summary report in pdf file

Example of first page of pdf report

Detailed statistics in a csv file

	Test Results								
Image Name	Chi-LeftToRight-RGB	Chi-LeftToRight-Green	Chi-BottomToTop-RGB	Chi-BottomToTop-Green	Chi-RightToLeft-RGB	Chi-RightToLeft-Green	Sig-Davinci	Sig-Mobi	Sig-StegMaster
265748.PNG	0.0024	0.0031	0.0027	0.0123	0.0047	0.0388	FALSE	FALSE	FALSE
62b5_z.png	0.3720	0.1285	0.9134	0.8625	0.6467	0.5994	FALSE	FALSE	FALSE
265749.PNG	0.0026	0.0027	0.0030	0.0143	0.0058	0.0422	FALSE	FALSE	FALSE
c0f25_z.png	0.0100	0.0073	0.0749	0.0867	0.0078	0.0094	FALSE	FALSE	FALSE
a35a_z.png	0.0588	0.0317	0.0576	0.1495	0.0521	0.1823	FALSE	FALSE	FALSE
c9109_z.png	0.0380	0.0924	0.0247	0.0323	0.0268	0.0409	FALSE	FALSE	FALSE
6986_z.png	0.0203	0.0106	0.0695	0.0409	0.0513	0.0465	FALSE	FALSE	FALSE
612578.PNG	0.0085	0.0037	0.0025	0.0048	0.0014	0.0030	FALSE	FALSE	FALSE
c258da5.png	0.0267	0.1821	0.0541	0.2675	0.0252	0.0201	FALSE	FALSE	FALSE

Example of csv output

Future Direction

Future Direction:
- Add more detection methods
- Comprehensively debug the software
- Develop an API for StegFinder
- Improve report document and contents

References

- Martin, A., Lin, L., Chen, W., Pierre, S., Guan, Y., Newman, J. A response to the threat of Stegware. American Academy of Forensic Sciences (AAFS), 2021. February, 2021. Virtual Presentation.
- Newman, J., Lin L., Chen W., Reinders S., Wang Y., Wu M., Guan Y. “StegoAppDB: A steganography apps forensics image database,” IS&T Int’l. Symp. on Electronic Imaging, Media Watermarking, Security, and Forensics 2019, Burlingame, CA, pp. 536-1-536-12 (12), 2019.

This work was funded (or partially funded) by the Center for Statistics and Applications in Forensic Evidence (CSAFE) through Cooperative Agreements 70NANB15H176 and 70NANB20H019 between NIST and Iowa State University, which includes activities carried out at Carnegie Mellon University, Duke University, University of California Irvine, University of Virginia, West Virginia University, University of Pennsylvania, Swarthmore College and University of Nebraska, Lincoln.