IOWA STATE UNIVERSITY

A Response to the Threat of Stegware

Abby Martin, Li Lin, Wenhao Chen,
Seth Pierre, Yong Guan, Jennifer Newman

Iowa State University, Ames IA
Department of Electrical and Computer Engineering
Department of Mathematics

csafe
Center for Statistics and Applications in Forensic Evidence

Steganography Introduction

- Practice of concealing a message (payload) within a cover image
- “Hidden in plain sight”

Cover

+

Payload text

=

Stego

Real-World Steganography Threats

- Operation Shady RAT – 2006, one of the first large-scale attacks of steganography in malware*
  - Downloaded HTML pages or JPEG images with hidden commands allowing access to local files*
- Facebook embeds hidden data in downloaded images**
- OceanLotus APT group – has used steganography to hide payload in malicious emails***

*Stegware – the latest trend in cybercrime, SIMARGL website. Link https://simargl.eu/blog/technical/stegware-the-latest-trend-in-cybercrime.
**Facebook Embeds 'Hidden Codes' To Track Who Sees And Shares Your Photos, Forbes, July 2019.
Link https://www.forbes.com/sites/zakdoffman/2019/07/14/facebook-is-embedding-hidden-codes-to-track-all-your-uploaded-photos-report/?sh=52b2c1961592.
***OceanLotus APT Uses Steganography to Shroud Payloads, ThreatPost, April 2019.
Link https://threatpost.com/oceanlotus-apt-uses-steganography-to-shroud-payloads/143373/.

Goal: create a free, easy to use steganalysis tool

- Steganography - used for passing messages secretly, can be used for dishonest purposes
- best steganography detection tools behind a paywall
- Open source, free steganalysis tools
  - Difficult to use
  - Inaccessible to many users
  - Use limited techniques

csafe
Center for Statistics and Applications in Forensic Evidence

Scope

- Reverse Engineered 8 Apps from the Google Play Store or the App Store
  - 6 spatial embedding
    - MobiStego, PocketStego, Steganography-Meznik, Pictograph, Da Vinci, and Steganography Master
  - 2 JPEG embedding
    - PixelKnot and Passlok
  - Current tools focuses on the spatial embedding
  - PixelKnot – 100k+ downloads, current tools cannot detect

McAfee Steganography Defense Initiative*

Entirely web-based (-)

1 image selected for evaluation at a time (-)

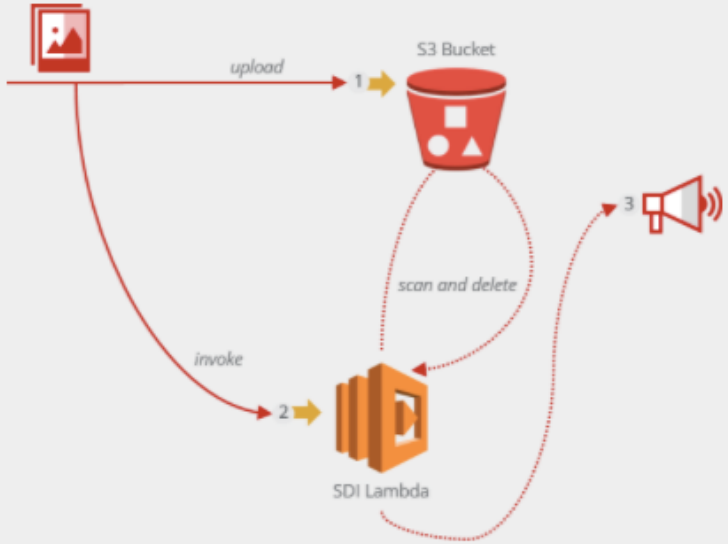
TRY IT OUT

Simple to use, but difficult to understand results (+/-)

We are constantly improving detection capabilities, keep coming back for updated results

Drop here an image file to analyze for steganography

(*) This is a constrained service, make sure the selected image is not larger than 1024x768 and the size is less than 1 MB



RESULTS

Suspicious: No - We can't find significant traces of steganography in this image
Confidence Level: Low
Score: 100.67968157389761
Scan Time: 6760 ms
Errors: false

No explanation of embedding algorithms tested or identified (-)

(**) Processing time might vary between 1 and 25 seconds depending on multiple factors such as your current location, file size and format, and service load. Depending on the image format and amount of concealed data, this Beta tool may not always detect steganography.

Image restricted to 1024 x 768 with size less than 1 MB (-)

* https://www.mcafee.com/enterprise/en-us/downloads/free-tools/steganography.html

McAfee Steganography Defense Initiative

RESULTS

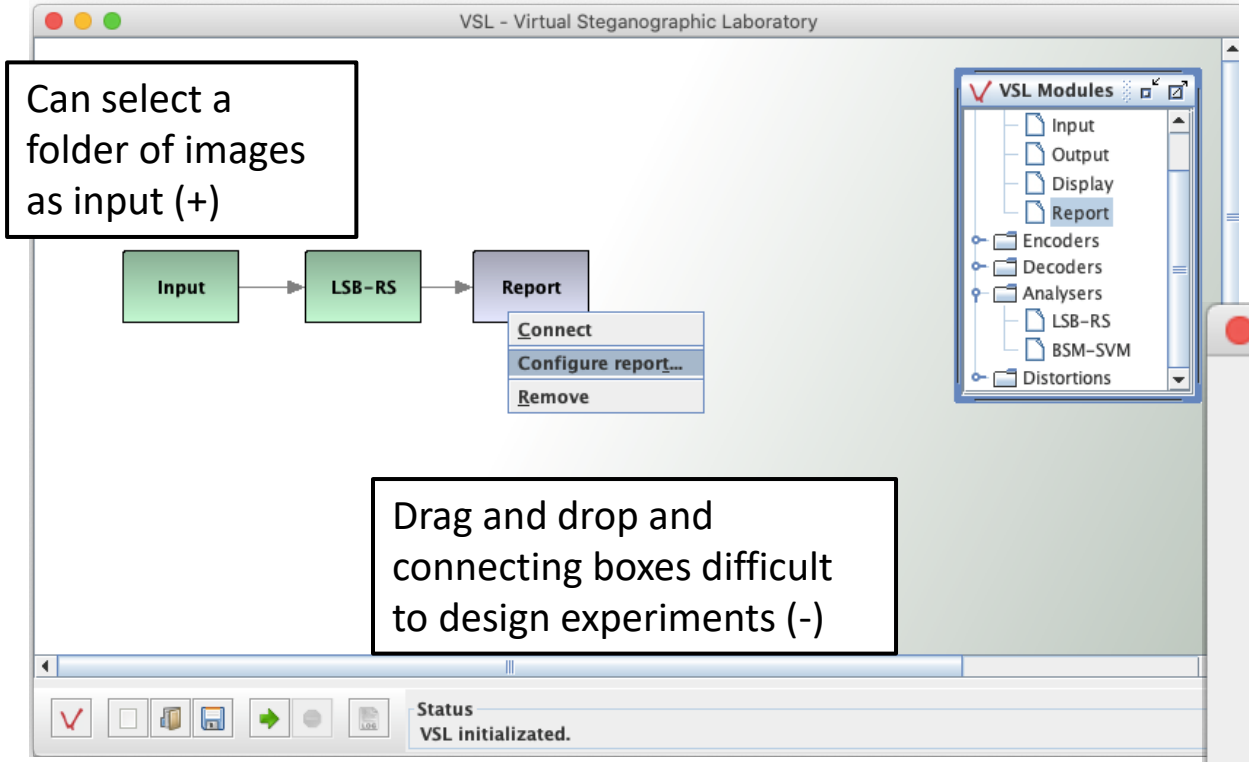
Suspicious: Yes - Image might be concealing data using steganography
Confidence Level: Low
Score: 1000
Scan Time: 598 ms
Errors: false

(**) Processing time might vary between 1 and 25 seconds depending on multiple factors such as your current location, file size and format, and service load. Depending on the image format and amount of concealed data, this Beta tool may not always detect steganography.

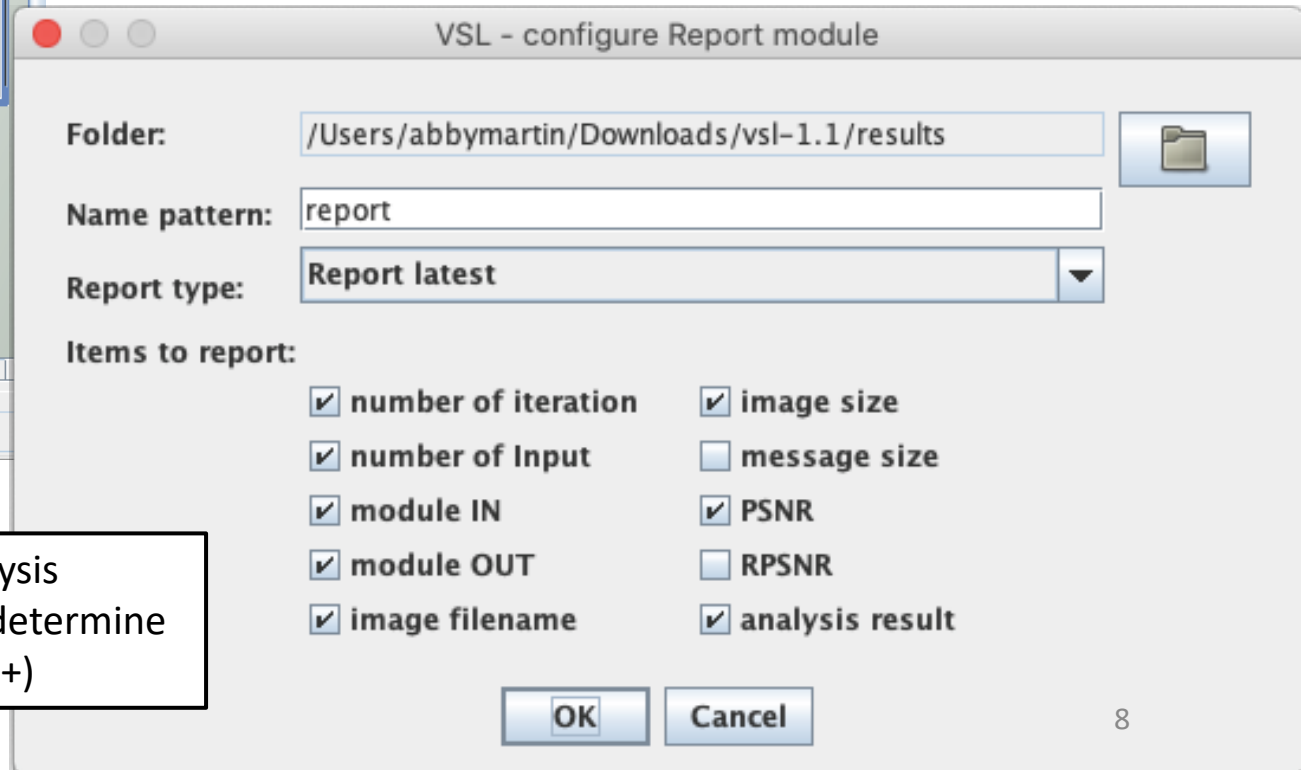
VSL – Virtual Steganographic Laboratory

Can select a folder of images as input (+)

Java program with a GUI (+)



Drag and drop and connecting boxes difficult to design experiments (-)



Performs 2 steganalysis methods (user can determine which tests to run) (+)

VSL – Virtual Steganographic Laboratory*

- 1 line .csv results for each image (-)
- No label for data in each column (-)

	A	B	C	D	E	F	G	H	I	J	K	L
1	0	0	Input	LSB-RS	/Users/abby	1280x960	0	Estimated message size [B]:13400.867925139932				
2												
3												

*http://vsl.sourceforge.net/

StegExpose*

- Can select a folder of images as input (+)
- Results in .csv file include data for all images with clear headers (+)
- Processes only spatial domain, like PNG and BMP but not JPEG (-)
- Command line interface (-)
- Performs 4 steganalysis methods for each test (-)
  - User cannot determine which test to run (-)
  - User requires expert knowledge (-)

*https://github.com/b3dk7/StegExpose and https://arxiv.org/abs/1410.6656

StegExpose – Output Example

	A	B	C	D	E	F	G	H	I
1									
2	File name	Above stego threshold?	Secret message size in bytes (ignore for clean files)	Primary Sets	Chi Square	Sample Pairs	RS analysis	Fusion (mean)	
3	284598.JPG	FALSE	958	0.005123606	5.48E-04	0.02095071	0.022492712	0.012278725	
4	281386.JPG	FALSE	4835	0.081109726	0.083434562	0.034853155	0.029710251	0.057276924	
5	282857.JPG	FALSE	255	0.001556796	0.014181947	6.11E-04	0.0014959	0.00446152	
6	300840.JPG	FALSE	933	0.016228149	0.01753191	0.007379759	0.005664217	0.011701009	
7	273845.JPG	FALSE	1931	0.014320603	0.005720457	0.024131811	0.027134046	0.017826729	
8	316763.JPG	FALSE	878	0.01811262	0.005058481	0.009297059	0.010071228	0.010634847	
9	275005.JPG	FALSE	13073	NaN	0.018690814	0.089997303	0.087291931	0.065326683	
10	302266.JPG	FALSE	634	0.009836109	0.008052615	0.005167686	0.006446773	0.007375796	
11	284017.JPG	FALSE	555	0.00661696	0.016470589	0.001325162	0.002973589	0.006846575	
12	297043.JPG	FALSE	1021	0.021921626	0.003893836	0.010450683	0.011738511	0.012001164	
13	317657.JPG	FALSE	224	0.004716274	0.005219445	0.003005638	0.002170714	0.003778018	
14	269202.JPG	FALSE	1353	0.014766575	0.018128894	0.014390629	0.012226422	0.01487813	
15	281966.JPG	FALSE	1119	0.004830486	0.042422189	0.005189996	0.005278733	0.014430351	
16	261662.JPG	FALSE	1140	0.014126441	8.81E-04	0.019406499	0.016870804	0.012821087	
17	273266.JPG	FALSE	2772	0.029851826	0.005708502	0.031146482	0.029178695	0.023971376	
18	276478.JPG	FALSE	321	0.001539458	3.26E-04	0.003318019	0.006358429	0.002885383	
19	317079.JPG	FALSE	103	0.00229411	0.001214501	3.77E-04	0.002433275	0.001579658	
20	290664.JPG	FALSE	4006	0.031993337	0.049809867	0.020857106	0.021896288	0.031139149	
21	304005.JPG	FALSE	986	0.018523887	0.005521241	0.012695226	0.010802055	0.011885602	
22	298204.JPG	FALSE	887	0.021479483	0.004616699	0.006386527	0.007902735	0.010096361	
23	278482.JPG	FALSE	675	0.001492524	0.007263427	0.011931586	0.013784569	0.008618027	
24	272420.JPG	FALSE	662	0.01602584	0.002128061	0.008828943	0.008285	0.008816961	

results

Ready 150%

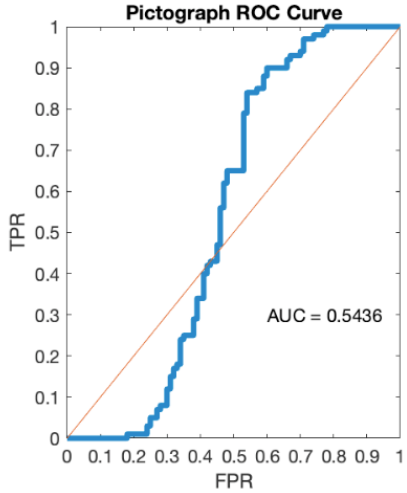
StegExpose – Output Example

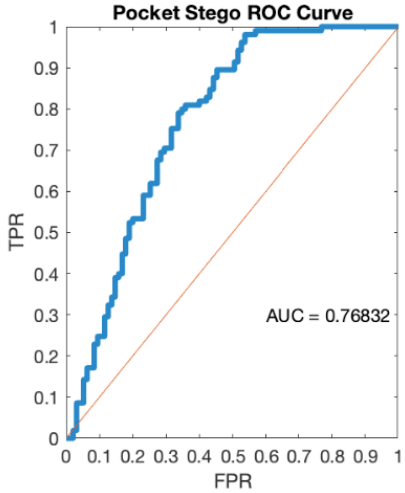
	A	B	C	D	E	F	G	H	I
1									
2	File name	Above stego threshold?	Secret message size in bytes (ignore for clean files)	Primary Sets	Chi Square	Sample Pairs	RS analysis	Fusion (mean)	
3	284598.JPG	FALSE	958	0.005123606	5.48E-04	0.02095071	0.022492712	0.012278725	
4	281386.JPG	FALSE	4835	0.081109726	0.083434562	0.034853155	0.029710251	0.057276924	
5	282857.JPG	FALSE	255	0.001556796	0.014181947	6.11E-04	0.0014959	0.00446152	
6	300840.JPG	FALSE	933	0.016228149	0.01753191	0.007379759	0.005664217	0.011701009	
7	273845.JPG	FALSE	1931	0.014320603	0.005720457	0.024131811	0.027134046	0.017826729	
8	316763.JPG	FALSE	878	0.01811262	0.005058481	0.009297059	0.010071228	0.010634847	
9	275005.JPG	FALSE	13073	NaN	0.018690814	0.089997303	0.087291931	0.065326683	
10	302266.JPG	FALSE	634	0.009836109	0.008052615	0.005167686	0.006446773	0.007375796	
11	284017.JPG	FALSE	555	0.00661696	0.016470589	0.001325162	0.002973589	0.006846575	
12	297043.JPG	FALSE	1021	0.021921626	0.003893836	0.010450683	0.011738511	0.012001164	
13	317657.JPG	FALSE	224	0.004716274	0.005219445	0.003005638	0.002170714	0.003778018	
14	269202.JPG	FALSE	1353	0.014766575	0.018128894	0.014390629	0.012226422	0.01487813	
15	281966.JPG	FALSE	1119	0.004830486	0.042422189	0.005189996	0.005278733	0.014430351	
16	261662.JPG	FALSE	1140	0.014126441	8.81E-04	0.019406499	0.016870804	0.012821087	
17	273266.JPG	FALSE	2772	0.029851826	0.005708502	0.031146482	0.029178695	0.023971376	
18	276478.JPG	FALSE	321	0.001539458	3.26E-04	0.003318019	0.006358429	0.002885383	
19	317079.JPG	FALSE	103	0.00229411	0.001214501	3.77E-04	0.002433275	0.001579658	
20	290664.JPG	FALSE	4006	0.031993337	0.049809867	0.020857106	0.021896288	0.031139149	
21	304005.JPG	FALSE	986	0.018523887	0.005521241	0.012695226	0.010802055	0.011885602	
22	298204.JPG	FALSE	887	0.021479483	0.004616699	0.006386527	0.007902735	0.010096361	
23	278482.JPG	FALSE	675	0.001492524	0.007263427	0.011931586	0.013784569	0.008618027	
24	272420.JPG	FALSE	662	0.01602584	0.002128061	0.008828943	0.008285	0.008816961	

results +

Ready 150%

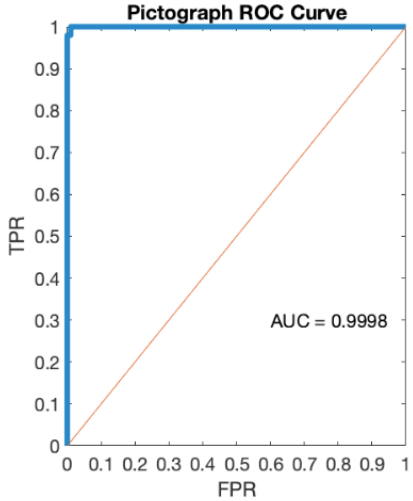
Matlab Plots

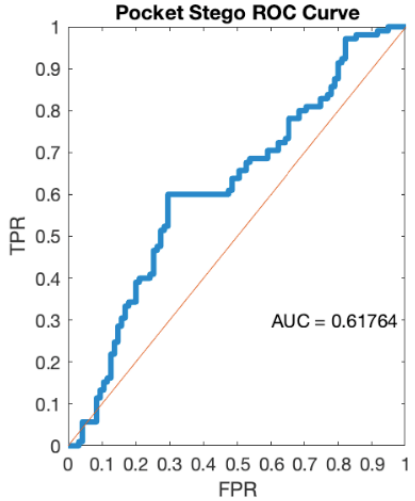




StegExpose Fusion Mean Results

- 100 cover images and 100 stego images
- Combination of 4 tests
- Only statistic used for evaluation of threshold





StegExpose Chi-Square Results

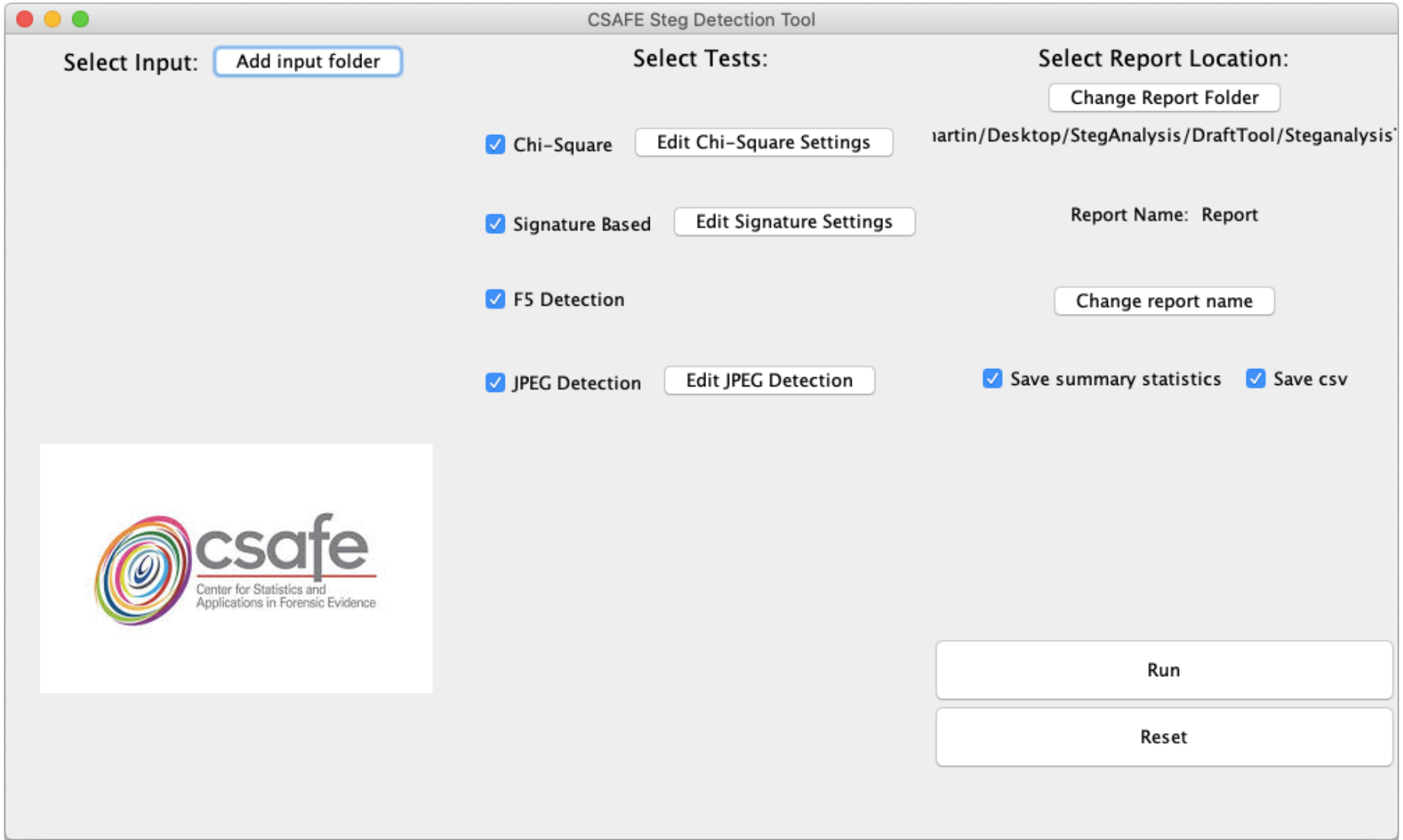
- 100 cover images and 100 stego images
- Performs significantly better for Pictograph

CSAFE Steg Detection Tool

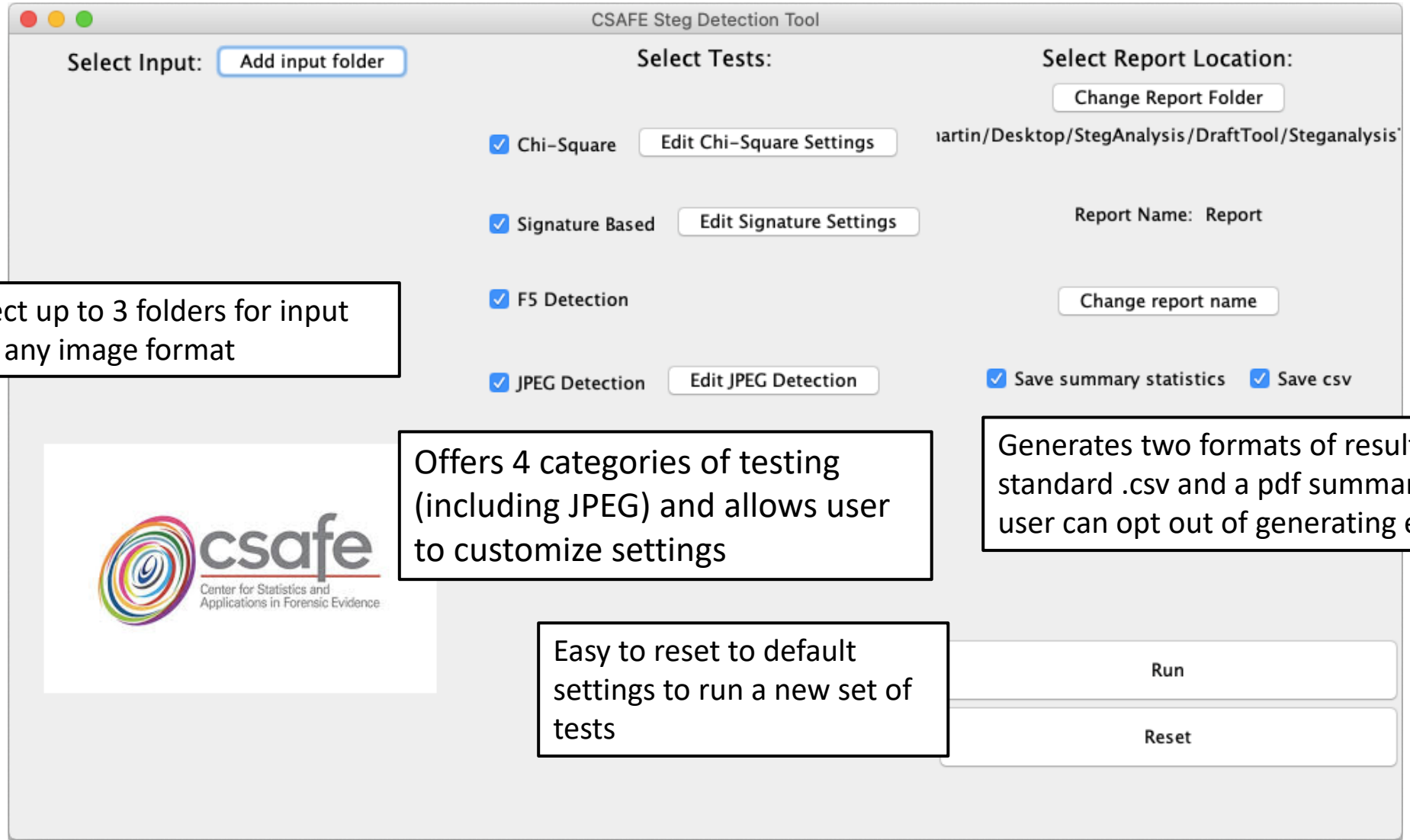
- GUI implementation
- Intuitive to operate
- Interpretable report in addition to a single, labelled .csv file
- Performs a variety of steganalysis methods, and allow the user to select which to run and parameters
- Processes of large sets of images easily

csafe
Center for Statistics and Applications in Forensic Evidence

CSAFE Steg Detection Tool



CSAFE Steg Detection Tool



Can select up to 3 folders for input
Accepts any image format

Offers 4 categories of testing (including JPEG) and allows user to customize settings

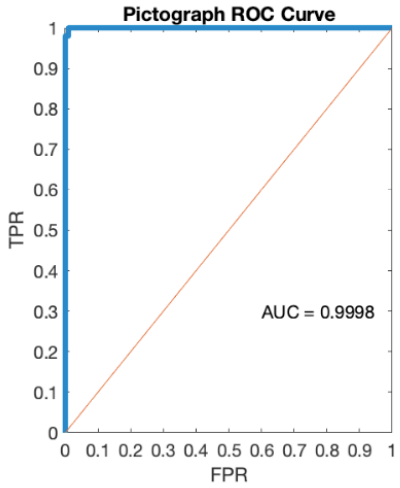
Generates two formats of results, standard .csv and a pdf summary, and user can opt out of generating either

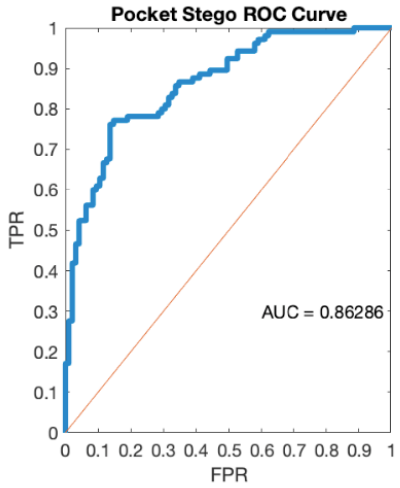
Easy to reset to default settings to run a new set of tests

CSAFE Steg Detection Tool

	A	B	C	D	E	F
1	Image Name	Chi-LeftToRight-RGB	Chi-LeftToRight-Green	Sig-Davinci	Sig-Mobi	Sig-StegMaster
2	/Users/abbymartin/Desktop/Assortment/265748.PNG	0.002395729	0.003119954	FALSE	FALSE	FALSE
3	/Users/abbymartin/Desktop/Assortment/stego_6666458261_e455d262b5_z.pn		0.128499314	FALSE	FALSE	FALSE
4	/Users/abbymartin/Desktop/Assortment/265749.PNG	0.002571864	0.002725523	FALSE	FALSE	FALSE
5	/Users/abbymartin/Desktop/Assortment/clean_7232193260_c2fd8c0f25_z.png	0.009962056	0.007267591	FALSE	FALSE	FALSE
6	/Users/abbymartin/Desktop/Assortment/clean_7231623538_f51db2a35a_z.png	0.05877201	0.031747764	FALSE	FALSE	FALSE
7	/Users/abbymartin/Desktop/Assortment/clean_7232220662_3d42c69109_z.pn	0.037963372	0.09240086	FALSE	FALSE	FALSE
8	/Users/abbymartin/Desktop/Assortment/clean_7232202430_d38b6d6986_z.pn	0.020347485	0.010554636	FALSE	FALSE	FALSE
9	/Users/abbymartin/Desktop/Assortment/612578.PNG	0.008460901	0.003680186	FALSE	FALSE	FALSE
10	/Users/abbymartin/Desktop/Assortment/clean_7235972310_8c25258da5.png	0.026697564	0.182082511	FALSE	FALSE	FALSE
11	/Users/abbymartin/Desktop/Assortment/612579.PNG	0.009179385	0.003680186	FALSE	FALSE	FALSE
12	/Users/abbymartin/Desktop/Assortment/846531.PNG	0.006031289	0.014629352	FALSE	FALSE	FALSE
13	/Users/abbymartin/Desktop/Assortment/846533.PNG	0.005629399	0.016119947	FALSE	TRUE	FALSE
14	/Users/abbymartin/Desktop/Assortment/clean_7234473324_bb8a82b5bd.png	2.91E-04	3.77E-05	FALSE	FALSE	FALSE
15	/Users/abbymartin/Desktop/Assortment/846532.PNG	0.005726428	0.015389714	FALSE	TRUE	FALSE
16	/Users/abbymartin/Desktop/Assortment/clean_7232206610_b8cfded120_z.png	0.100724817	0.114267965	FALSE	FALSE	FALSE
17	/Users/abbymartin/Desktop/Assortment/195688.PNG	0.004829148	0.0222082	FALSE	FALSE	FALSE
18	/Users/abbymartin/Desktop/Assortment/clean_7228718722_1cf25dff3e_z.png	0.039267846	0.107851466	FALSE	FALSE	FALSE
19	/Users/abbymartin/Desktop/Assortment/846535.PNG	0.007341794	0.0217039	FALSE	TRUE	FALSE
20	/Users/abbymartin/Desktop/Assortment/clean_7235558256_3099066753.png	0.031068078	0.064081654	FALSE	FALSE	FALSE
21	/Users/abbymartin/Desktop/Assortment/846534.PNG	0.0071134	0.018836055	FALSE	TRUE	FALSE
22	/Users/abbymartin/Desktop/Assortment/195686.PNG	0.004573079	0.024630413	FALSE	FALSE	FALSE
23	/Users/abbymartin/Desktop/Assortment/clean_7221186570_82a10bc040_z.png	0.073688361	0.080730233	FALSE	FALSE	FALSE
24	/Users/abbymartin/Desktop/Assortment/195687.PNG	0.004419625	0.021339742	FALSE	FALSE	FALSE
25	/Users/abbymartin/Desktop/Assortment/195685.PNG	0.003980416	0.022924317	FALSE	FALSE	FALSE
26	/Users/abbymartin/Desktop/Assortment/195684.PNG	0.00398992	0.024566193	FALSE	FALSE	FALSE

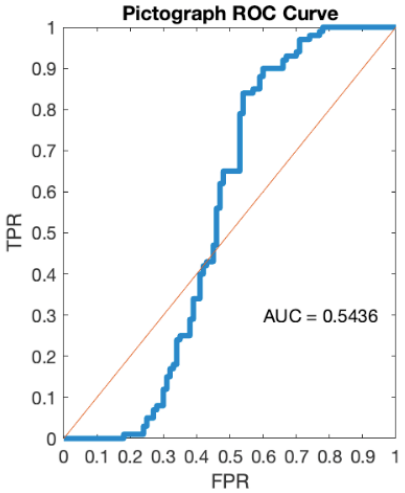
Results Comparison

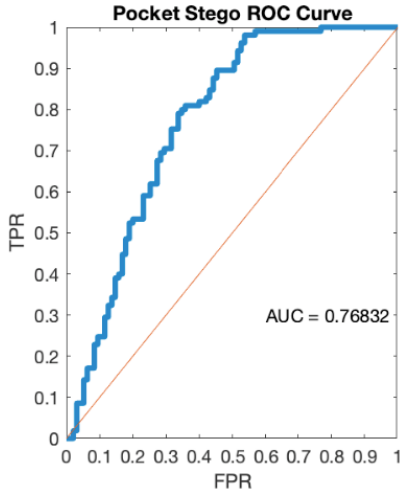




CSAFE Steg Detection Tool Results

- 100 cover images and 100 stego images
- Can select different scan orders

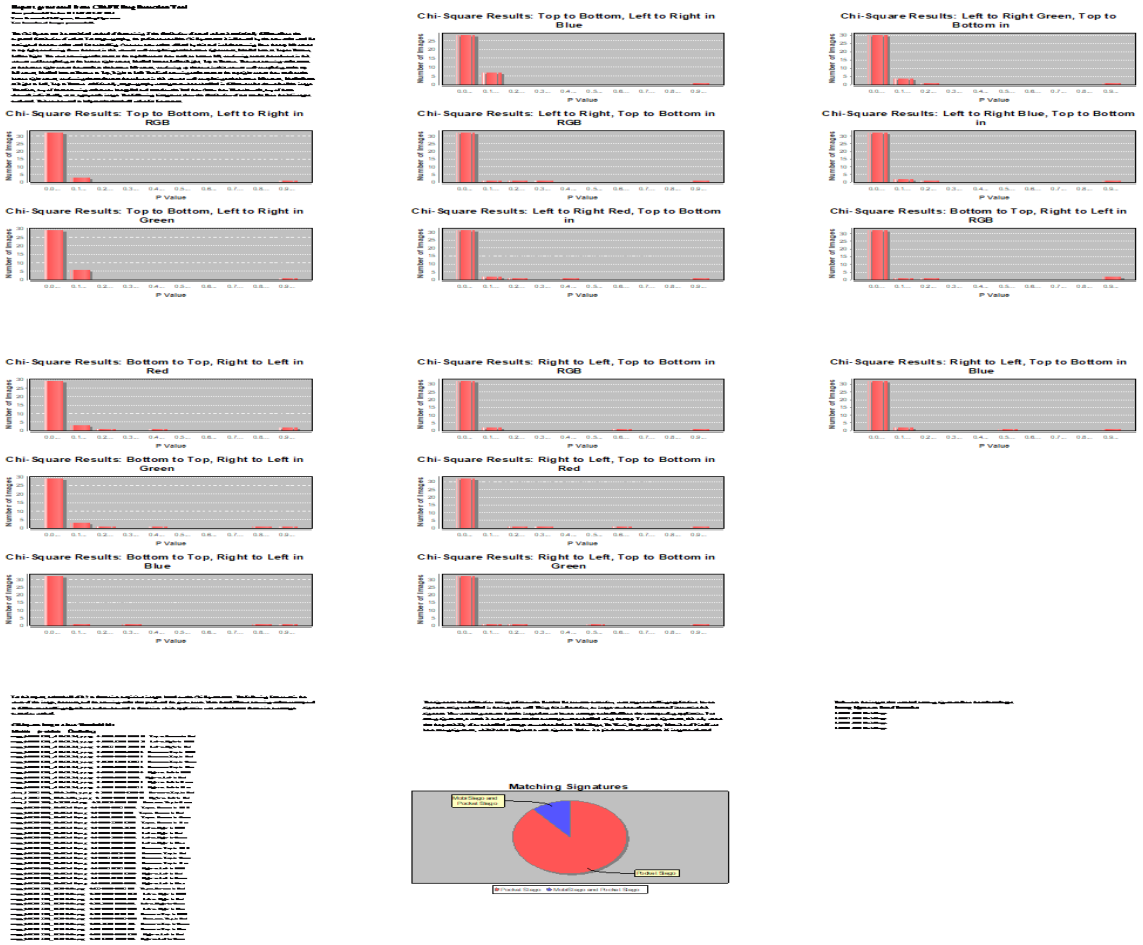




StegExpose Fusion Mean Results

- 100 cover images and 100 stego images
- Combination of 4 tests
- Only result used for evaluating with threshold

CSAFE Steg Detection Tool Report



CSAFE Steg Detection Tool Report

Report generated from CSAFE Steg Detection Tool

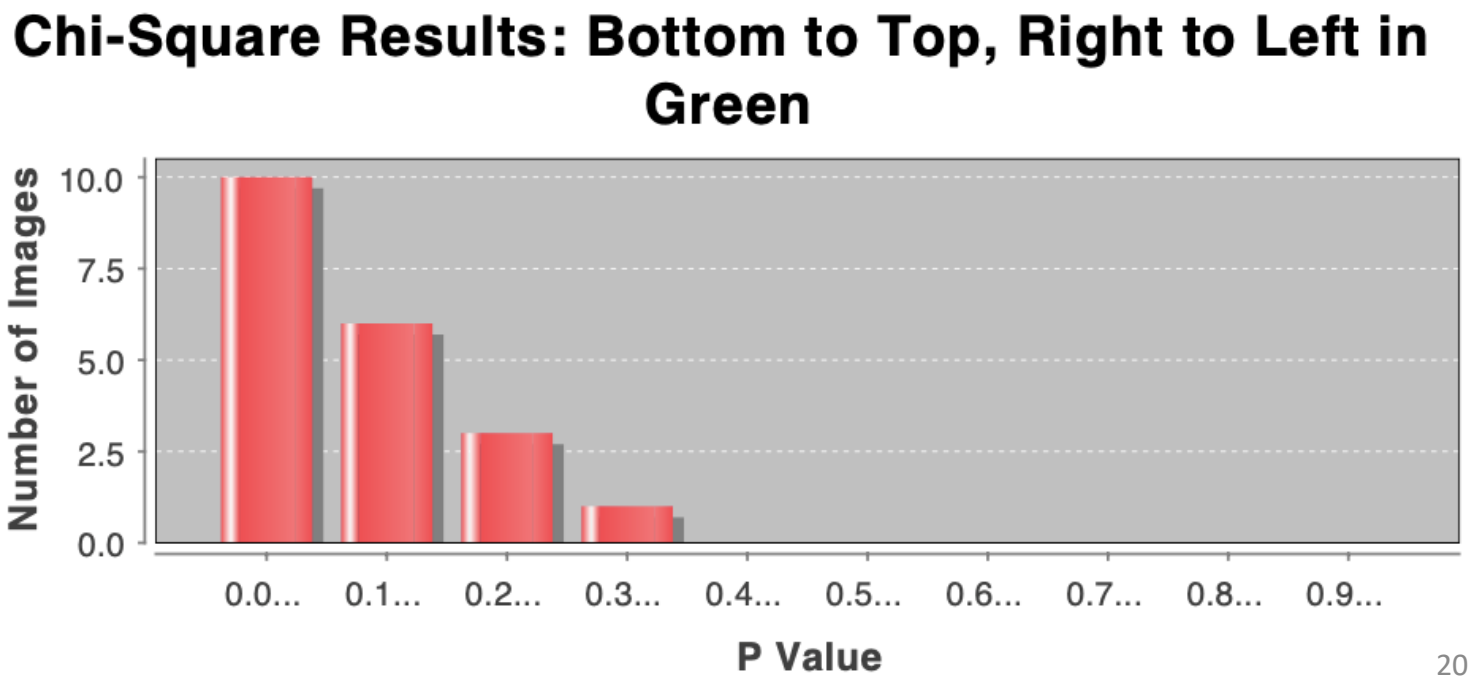
Date produced: Tue Jan 19 10:53:16 CST 2021

Tests Executed: Chi-Square, Matching Signatures

Total number of images processed: 20

The Chi-Square test is a statistical method of determining if the distribution of actual values is statistically different from the expected distribution of values. For steganography, the performance of the Chi-Square test is influenced by the scan order used for testing and the scan order used for embedding. Common sca
to top right, continuing down the rows in this manner until
Left to Right. The next scanning order starts at the top left c
manner until completing at the bottom right corner, labelled
at the bottom right corner then reads to the bottom left corn
left corner, labelled here as Bottom to Top, Right to Left. T
bottom right corner, continuing the read across the columns

Summary of experiment settings and relevant information for understanding each test



Visualization of results and data for a better understanding

CSAFE Steg Detection Tool

- Future Plans
  - Extend signature detection to additional applications (both for spatial and JPEG embedding)
  - Add additional statistical detection methods
  - Continue to refine design of GUI and the generated report
  - Collect signature patterns for all existing Android Stego Apps

csafe
Center for Statistics and Applications in Forensic Evidence

IOWA STATE UNIVERSITY

Thank You!

- 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.

csafe
Center for Statistics and Applications in Forensic Evidence