Improving Hidden Message Extraction Using LSB Steganalysis Techniques

Nikhil Mewalal and Wai Sze Leung

Abstract Increased awareness of the role of digital forensics in investigations has led to greater efforts being employed by users to conceal their data, possibly even using algorithms purposely designed to evade detection during steganalysis. A digital investigator seeking to ascertain whether some medium is indeed making use of steganography to hide pertinent evidence must therefore consider including other steganalysis techniques in their analysis in order to overcome the different steganographic strategies that may be used to evade detection. This paper investigates the design of a more comprehensive steganalysis tool that makes use of a series of statistical methods in conjunction with visual and forensic methods to detect messages hidden in images, specifically those hidden in PNG files using Least Significant Bit steganography. The study devises an appropriate combination of the techniques to generate a more effective and comprehensive steganalysis strategy for digital investigators attempting to detect hidden data.

Keywords Steganalysis · Steganography · Least significant bit

1 Introduction

A more comprehensive approach is required to conduct digital forensic investigations adequately when it comes to examining content for possible concealment through steganography.

Steganography is used as a means for communicating covertly in plain sight without arousing suspicion. This technique entails concealing a message inside an inconspicuous object in such a way that a casual observer is not able to differentiate between the original object (referred to as a cover object), and the object with the

N. Mewalal · W. S. Leung (✉)
University of Johannesburg, Johannesburg, South Africa
e-mail: wsleung@uj.ac.za

N. Mewalal
e-mail: 216086143@student.uj.ac.za

K. J. Kim and N. Baek (eds.), *Information Science and Applications 2018*,
Lecture Notes in Electrical Engineering 514,
https://doi.org/10.1007/978-981-13-1056-0_29

hidden message (also known as the stego image or steganogram). In the digital world, this cover object could be in the form of media, such as an image file, a video file, or even a music file [1].

Conversely, steganalysis refers to the complementary operation of detecting messages that have been hidden using steganography. During this process, the steganalysis algorithm is executed with the aim of interrogating the properties of an object which may be serving as the cover for hidden content with the aim of searching for any anomalies that could be deemed suspicious.

For digital forensics investigators, steganalysis is not without challenges. The existence of numerous steganography techniques (which can be dependent on the cover object file type), and the inability to extract the hidden message embedded in the first place can end up successfully frustrating steganalysis efforts.

In this paper, we propose the implementation of a more encompassing steganalysis tool that employs a greater variety of techniques to establish with greater certainty, whether a suspected file is a steganogram or simply a clean object. For the study, we will focus specifically on messages embedded into Portable Network Graphic (PNG) files. Our prototype will thus implement a series of Least Significant Bit (LSB) steganalysis techniques from varying domains to counter anti-detection attempts.

The rest of the paper is organized as follows: Sect. 2 briefly reviews some of the LSB steganalysis techniques to establish the different domains of LSB steganalysis techniques that exist. Section 3 then outlines a model of our more encompassing steganalysis solution. Section 4 presents the implementation details, along with the results of our prototype in Sect. 5, concluding the paper in Sect. 6.

2 Literature Review

2.1 Pairs of Values (Chi-Squared Attack)

This technique detects LSB embedding by using the histogram representation of the image. In a cover image, the gradient of the bars of the histogram can be noticeably smoother with bar heights varying throughout. In contrast, the bars on the histogram of a steganogram have neighbors that are roughly of equal height, producing a more rigid pattern [2]. Such an observation can be explained by how changes are applied within value pairs, resulting in an even distribution of 0 s and 1 s for each [2].

The success of histogram attacks on LSB steganography however relies on a fully-embedded image (where every single LSB is utilized to store a message).

2.2 Sample Pairs Analysis

When the image is only partially embedded along a pseudo-random path, examiners are no longer able to rely solely on a histogram of pixels while ignoring the dependency among neighboring pixels in natural images. For this reason, a more accurate and reliable method of detection that considers the spatial correlation within the image is used.

2.3 RS Analysis

RS Steganalysis relies on how LSB embedding operations work to determine whether an image contains a hidden message, as well as what the length of that image may be. This is achieved by identifying the presence of an imbalance in the cover file to establish the existence of hidden data [3, 4].

3 Model

Although the previous section has described several statistical techniques that could be employed for uncovering the presence of steganography, the use of just one domain area, such as statistical steganalysis, may not yield sufficiently thorough results. To address the shortcomings of a single steganalysis approach, we consider the application of several analysis models, which when used in conjunction with each other, provide a complementary set of techniques to test for most characteristics that reveal the presence of hidden messages.

3.1 Visual Models

LSB Amplification. This model aims to enhance the luminosity of the image in a manner that will end up removing all the parts of the image that is blocking the message. The human eye will then be able to distinguish whether there is a hidden message present in this message [5].

Difference and Neighborhood Histogram. Whilst this model may technically fall under a statistical method, it has been included as a visual one as it involves the production of a visual representation of the histogram which the user should ideally interpret. The neighboring bars in the histogram of a steganogram, for example, will exhibit similar heights [6].

3.2 Statistical Models

Chi-Square Attack. The approach to this form of steganalysis is to compare the expected frequency distribution in suspected stego images with a sample distribution observed in the possibly changed carrier image. Such an approach will however require an expected frequency distribution of the original cover image. Realistically, it would not be feasible to have a database of every possible image out there.

This shortcoming can however be addressed by estimating the theoretical expected frequency distribution [5].

Sample Pairs Analysis. This approach focuses on the analysis of transitions (such as slight color changes) in adjacent vertical or horizontal pixel pairs that are often imperceptible to the human eye [7]. An example is changing a pixel which is white (represented by FF FF FF) to FF FF FE.

3.3 Forensic Models

The model behind this attack is a custom one based on how LSB steganography works, reverse-engineering the process to extract the embedded message. The model aims to iterate through pixels in the domain search space and extract the least significant bit for that image. These values are then collected and concatenated in the end to produce a byte stream. This byte stream will be cast into a string value and then the result will be presented to the user.

4 Experimentation and Results

4.1 Preparation of Image Files

Images from the VOC 2005 Database: Dataset 1, as provided by the University of Oxford, were used for assessing our prototype implementation. The set contains 1578 images of categories motorbikes, bicycles, people, and cars in arbitrary poses [8]. From these, 26 images were selected and each processed to produce three different versions of the file. Details of the three versions are presented in Table 1.

Table 1 Preparation for each of the 26 images used for the experiment

Version	Embedded message (using LSB steganography)	Size (kb)
Clean image	None	N/A
Medium-length steganogram	US Constitution (pure text form)	26
Long-length steganogram	Lewis Carroll's Alice in Wonderland (pure text form)	110

4.2 Steganographic Process

To embed the images with the medium- and long-length text messages described in Table 1, a LSB steganographic program developed for a separate, previous project was used. This program was tested extensively and verified as functioning correctly.

For each of the 26 images processed by the LSB steganographic program, two additional files with embedded messages were created.

4.3 Testing of Statistics Methods

The implementation of the statistical algorithms incorporated in the model (Chi-Squared Attack, Sample Pairs Analysis, and RS Analysis) was assessed first. All 78 images prepared were run through the three statistical steganalysis techniques to obtain output in the form of percentages that suggested the possibility of steganography being embedded in the image. As seen in the results displayed in Figs. 1, 2 and 3, an additional threshold field was added to aggregate the results from the three statistical algorithms and reach a consensus-based outcome.

While the statistical algorithms were mostly accurate, it struggled to produce the correct result for several instances where the hidden message embedded was of medium-length.

4.4 Testing of Visual Methods

Since visual methods require the input of a visual confirmation from a human user, the setup of our tests centered on LSB Amplification, Neighborhood Histogram, (and later the Forensic Steganalysis) are modified to focus on a single image set instead. Table 2 below shows the file sizes of each of the images.

	A	B	C	D	E
1					
2	File name	Above stego threshold?	Chi Square	Sample Pairs	RS analysis
3	bike_002.png	false	0.035468595761012	0.013984777438386	0.016651815829314
4	bike_003.png	false	0.008229074303705	0.039003241986158	0.054287459259021
5	bike_005.png	false	0.316796754268329	0.005393382665105	0.016094220137041
6	bike_006.png	false	0.365469502271365	0.000747269945835	0.007313332622236
7	bike_008.png	false	0.273511517940003	0.002179440452387	0.007340031304305
8	bike_010.png	false	0.254215883605039	0.058812578276481	0.061335988259352
9	bike_013.png	false	0.008150305418937	0.026467929308288	0.023017141543606
10	bike_014.png	false	0.012463141931748	0.009746105548825	0.013941395320895
11	carsgraz_001.png	false	0.065019496494699	0.008527372185195	0.010297906016202
12	carsgraz_003.png	false	0.016444644307993	0.109340904223203	0.113528642194243
13	carsgraz_004.png	false	0.003993026564761	0.055286489364555	0.044514200367782
14	carsgraz_005.png	false	0.001112347052283	0.067272123943676	0.062696196803319
15	carsgraz_006.png	false	0.028089441026169	0.021706082389459	0.015657144258195
16	carsgraz_007.png	false	0.109090148297126	0.021435708157301	0.007759150253215
17	carsgraz_008.png	false	0.190302436862535	0.003389807895217	0.0074578526559
18	carsgraz_010.png	false	0.029931966386534	0.002874203846808	0.008157519721937
19	person_001.png	false	0.026873974349217	0.000342545462514	0.003165103037904
20	person_002.png	false	0.003646754371118	0.00997339836073	0.008207876882597
21	person_003.png	false	0.304680696666344	0.005719421372457	0.004465042495023
22	person_004.png	false	0.091825685225163	0.012043457037301	0.011324143014481
23	person_005.png	false	0.043814293651911	0.002185850745777	0.006482946128998
24	person_006.png	false	0.251164078266182	0.01196994231021	0.01277944301108
25	person_007.png	false	0.026236846116335	0.008063938131099	0.018209035719065
26	person_008.png	false	0.007036435561474	0.086274572859263	0.077706962679651
27	person_009.png	false	0.018503514149924	0.000330608118594	0.006362561028678

Fig. 1 Results of statistical algorithms against cover images

	A	B	C	D	E
1					
2	File name	Above stego threshold?	Chi Square	Sample Pairs	RS analysis
3	bike_002.png_constitution.png	true	0.398465363076042	0.247020555287117	0.242173425679415
4	bike_003.png_constitution.png	true	0.359716089539047	0.250466407539127	0.230298231637796
5	bike_005.png_constitution.png	true	0.659515384319639	0.116974348707154	0.127297868651865
6	bike_006.png_constitution.png	false	0.31578259880315	0.093442926699728	0.094168571373288
7	bike_008.png_constitution.png	true	0.304909943395779	0.154241090689532	0.163280489288853
8	bike_010.png_constitution.png	true	0.495464187961221	0.188754052056058	0.186868311912344
9	bike_013.png_constitution.png	true	0.267470056432877	0.190373132933006	0.191495979940256
10	bike_014.png_constitution.png	true	0.324888368972554	0.186667048493133	0.193272141192999
11	carsgraz_001.png_constitution.png	true	0.286848122424317	0.211045849503554	0.204957246752936
12	carsgraz_003.png_constitution.png	true	0.402657525067698	0.260008467087691	0.260848571129253
13	carsgraz_004.png_constitution.png	true	0.318059652770868	0.232170539940528	0.213838959521698
14	carsgraz_005.png_constitution.png	true	0.309902888930206	0.237936047320714	0.220351726291779
15	carsgraz_006.png_constitution.png	true	0.307932841680613	0.249422739731853	0.220667751215157
16	carsgraz_007.png_constitution.png	true	0.341120683089263	0.217427208850338	0.210973485279597
17	carsgraz_008.png_constitution.png	true	0.339453067604177	0.196331438614886	0.191429433959119
18	carsgraz_010.png_constitution.png	true	0.287563168871884	0.244492466853642	0.232940697210976
19	person_001.png_constitution.png	true	0.324724823005207	0.176835973295443	0.175970631177478
20	person_002.png_constitution.png	true	0.27751879809089	0.177564153153279	0.176442821366838
21	person_003.png_constitution.png	true	0.542086330682632	0.124081363641832	0.1436670052695
22	person_004.png_constitution.png	false	0.261625380894664	0.128066656985941	0.136199510522887
23	person_005.png_constitution.png	true	0.300491038378471	0.154479237261791	0.1579761368283
24	person_006.png_constitution.png	false	0.295464895694483	0.099833890440181	0.098510040099934
25	person_007.png_constitution.png	false	0.386905226774512	0.127396766694647	0.129522359729434
26	person_008.png_constitution.png	true	0.338977111885571	0.201794804824168	0.195858970219223
27	person_009.png_constitution.png	true	0.274152963424447	0.213083504165284	0.202429374813855

Fig. 2 Results of statistical algorithms against stego images (medium-length text)

4.5 Testing of Forensic Method

Because the clean images would have nothing to extract, this test focuses on recovering the hidden text from the stego images that were embedded with the medium-

	A	B	C	D	E
1					
2	File name	Above stego threshold?	Chi Square	Sample Pairs	RS analysis
3	bike_002.aic.png	true	0.999996013696524	0.560884270602339	0.538092400742346
4	bike_003.aic.png	true	0.99999265313637	0.548845319472144	0.553801495350278
5	bike_005.aic.png	true	0.969942008846784	0.54781722021032	0.544178605284058
6	bike_006.aic.png	true	0.997145164587792	0.553044587543496	0.550655530021393
7	bike_008.aic.png	true	0.999996834942754	0.560438779517371	0.556773588820101
8	bike_010.aic.png	true	0.99773107380999	0.540343838593908	0.52969428827519
9	bike_013.aic.png	true	0.999037344785862	0.557729371493558	0.551038540919139
10	bike_014.aic.png	true	0.999981929287196	0.537943087489016	0.541813069961786
11	carsgraz_001.aic.png	true	0.997532926593816	0.57094789291879	0.551890526011005
12	carsgraz_003.aic.png	true	0.999998713539164	0.559302951189692	0.556590424868653
13	carsgraz_004.aic.png	true	0.98812940994461	0.555203414125766	0.548643666360857
14	carsgraz_005.aic.png	true	0.999918076645771	0.550238134071812	0.54793159544631
15	carsgraz_006.aic.png	true	0.984131908322956	0.554924105564913	0.551510477058286
16	carsgraz_007.aic.png	true	0.993661089837016	0.568090110543817	0.552815363462716
17	carsgraz_008.aic.png	true	0.988848467241532	0.558933084358594	0.550412154913702
18	carsgraz_010.aic.png	true	0.994118425320778	0.56445114818576	0.543239052027151
19	person_001.aic.png	true	0.967460267932885	0.551407580151617	0.534918627306265
20	person_002.aic.png	true	0.999990090695096	0.56483655969909	0.55026267863385
21	person_003.aic.png	true	0.999330239589465	0.53492661921218	0.530234102622953
22	person_004.aic.png	true	0.999218373421416	0.560435033670094	0.548225554943698
23	person_005.aic.png	true	0.980419841159189	0.559741449440341	0.545829437755498
24	person_006.aic.png	true	0.999991068086851	0.566834452887568	0.547025582659521
25	person_007.aic.png	true	0.992964088787539	0.537320771021972	0.530426689510618
26	person_008.aic.png	true	0.998854889475253	0.530426683333352	0.526252305186295
27	person_009.aic.png	true	0.982149143880421	0.663218641610513	0.543741160384810

Fig. 3 Results of statistical algorithms against stego images (long-length text)

Table 2 File sizes of select image set used for experiment

Version	Size (kb)
Clean image	397
Stego image, embedded with the US Constitution (medium-length)	523
Stego image, embedded with Alice in Wonderland (long-length)	609

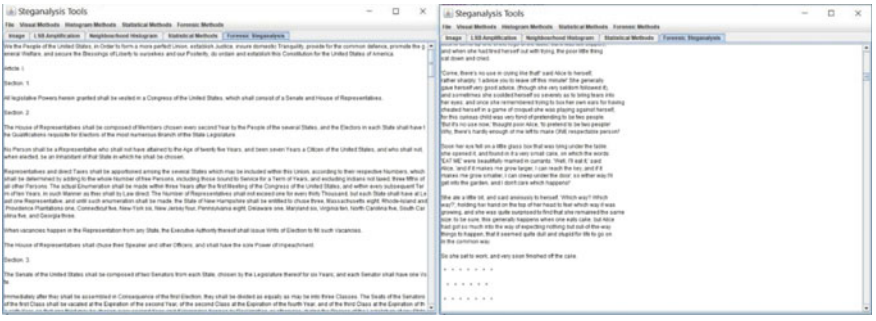

Fig. 4 Results of text recovered from the two stego images using forensic steganalysis

and long-length messages. By applying the algorithm described in Sect. 3.3, we were able to recover the original text, as seen in Fig. 4.

5 Discussion of Results

5.1 Statistical Techniques

Medium-length messages hidden in stego images could at times result in the incorrect consensus that it was clean. A threshold was chosen such that any steganalyses producing probabilities higher than 20% would lead to the assumption that the image quite likely hides a message.

Images Embedded with Long-Length Messages. When it comes to images embedded with long-length messages, Chi-Squared tests perform incredibly well with the average certainty probability of the image containing steganography sitting at 99%. In contrast, both Sample Pairs and RS Analysis averaged at a probability of 55% and 54% respectively. Since the threshold is set at 20%, both algorithms can be seen to still yield positive, accurate results.

Images Embedded with Medium-Length Messages. As in the case with long-length embedded messages, Sample Pairs and RS Analysis performed similarly, detecting at an average of 19% and 18.6% respectively.

Seeing as the threshold value was 20%, these algorithms would have incorrectly classified many of the images as being clean, suggesting that such techniques do not perform well. In comparison, Chi-Squared tests yielded an average of 34.6%. Although this probability is also relatively low, the Chi-Squared test would still correctly classify the images due to the 20% threshold.

Such results serve to validate the appropriateness of the threshold level.

Clean Images. Once again, Sample Pairs and RS Analysis perform similarly. The average for steganography being present in clean images was around 2% for both. This average value is even lower at 1% using the Chi-Squared test. Overall, all 3 algorithms performed well as they did not incorrectly classify an image as being a stego object.

5.2 LSB Amplification

Clean Image. When using LSB Amplification on a clean image, the result is an image that resembles an old television set which is not tuned to a channel due to the completely random distribution of information. If this was the only image to sample as an observer, there would be little reason to doubt that there is anything suspicious about this image.

Image Embedded with Medium-Length Message. Because the image has been manipulated to embed a message, a definite pattern can be seen starting from the top left of the image, noticeable to the human eye. In the case of our selected image and

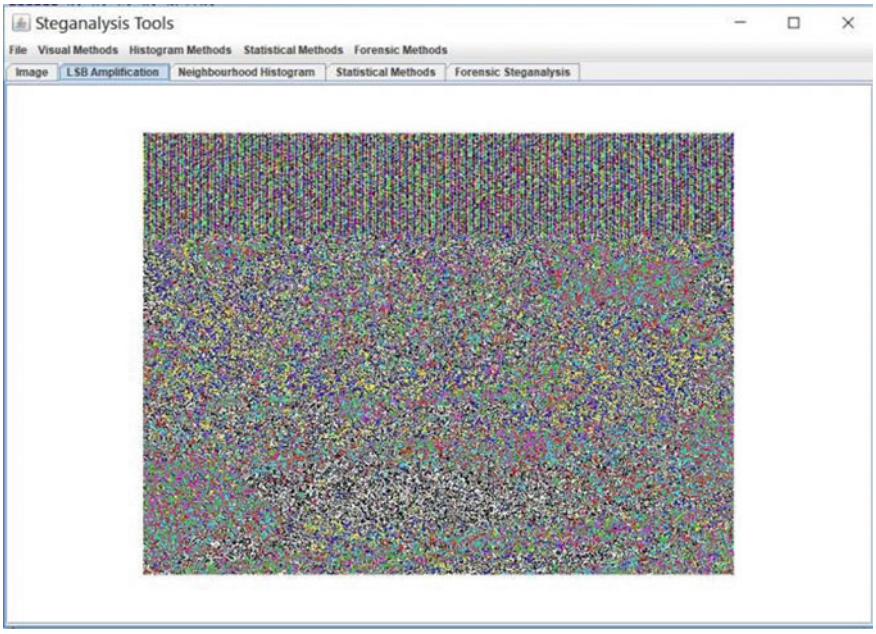

Fig. 5 LSB Amplification with medium-length message

embedded image, we noticed that this pattern persisted for roughly the first 25% of the image's LSB enhancement (as seen in Fig. 5).

This observation can be attributed to the fact that given 397/523 * 100 = 75.9% (where the original file size is 397 kb while the medium length stego image is 523 kb), we have established how approximately 25% of the stego file contains hidden data.

Image Embedded with Long-Length Message. As noticed in the image embedded with a medium-length message, the extent at which noise is present in LSB Amplification in an image embedded with a message is dependent on the size of the message being hidden.

The noise level of the same image embedded with the longer Alice in Wonderland text is therefore much more pronounced. In such a case, a person asked to assess whether the image is embedded with a hidden message will have little reason to doubt that the image is indeed suspicious.

5.3 Neighborhood Histogram

Clean Image. As indicated by Westfeld, neighborhood histograms of images devoid of steganography generally have between 8 and 10 neighborhood colors [4]. In our test image, the neighborhood histogram produced 10 neighborhood colors, with all the bars of varying length.

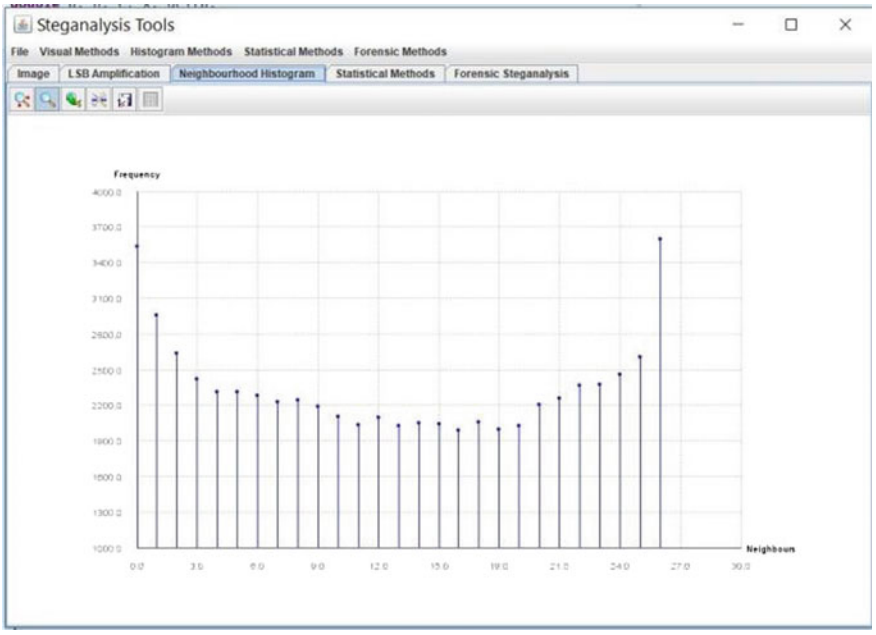

Fig. 6 Neighborhood histogram with long-length message

Image Embedded with Medium-Length Message. As established earlier in the LSB Amplification discussion, the embedded medium-length message takes up around 25% of the total file space. This observation accounts for the frequency of the neighborhood colors starting off very high and gradually lowering over time. The lower end of the histogram, which reflects typical behavior present in clean images, is the normal part of the image that does not contain any part of the concealed medium-length message.

Image Embedded with Long-Length Message. Due to the size of the message taking up almost the entire cover file space, the intensity of the frequency of neighborhood colors is consistently strong throughout the histogram. In this example (as seen in Fig. 6), most of the neighboring bars (as opposed to only some in the Medium-Length Message) are also of a similar height, making it easy for a human to visually discern that there is steganography embedded in the image.

6 Conclusion

Based on the experiments conducted, the following conclusions can be drawn:

- No one single statistical method can provide a solid and 100% detection rate—sometimes, the Chi-Square test will yield a better result than RS Analysis and sometimes, the opposite will be true.
- Combining results of the statistical methods leads to conclusions that are almost always accurate—this is especially true when a series of statistical techniques are combined, and a weighted average is used to draw the conclusion regarding the presence of steganography.
- Assessing each image for steganography using a combination of statistical methods is computationally taxing. On their own, each statistical test is already quite computationally expensive. This can be overcome by finding a mean of all the results to improve scanning time significantly. Specifically, the tool could start off with the tests known to be more accurate such as Chi-square and RS analysis. If both return good results, the steganalysis tool should not waste further resources by pursuing Primary Set and Sample Pairs Analysis.
- Employing visual techniques is a very strong way to identify suspicious images. However, this will need to be done on an image by image basis, which would ultimately prove non-feasible for investigators requiring results on a bulk set of images. For such purposes, investigators should revert to statistical steganalysis.
- The neighborhood histogram visual technique provided another very accurate approach to detecting steganography. The main concern here is that investigators employing this technique would need to have the knowledge to correctly interpret the result. It is however possible to programmatically develop the rules so that the interpretation of the histogram can be carried out by the computer instead.
- The initial results of the message extraction technique employed in the prototype proved to be positive, demonstrating how messages can be recovered from an image for forensic steganalysis purposes.

For further work, we anticipate testing our message recovery technique against other embedding techniques (other than LSB) to assess its validity.

Additional areas that will be focused on include the implementation of the programmatic interpretation of histograms and automating the decision-making concerning the optimal deployment of appropriate statistical methods for testing images for the presence of steganography.

References

1. Kessler GC, Hosmer C (2011) An overview of steganography. Adv Comput 83:51–107
2. Schaathun HG (2012) Machine learning in image steganalysis. Wiley, Norway
3. Bohme R (2010) Advanced statistical steganalysis. Springer

4. Manoharan S (2008) An empirical analysis of RS steganalysis. In: The third international conference on internet monitoring and protection internet monitoring and protection, pp 172–177
5. Westfeld A (2002) Detecting low embedding rates, Berlin
6. Zhang T, Ping X (2003) Reliable detection of LSB steganography based on the difference image histogram, Hong Kong
7. Shreelekshmi R, Wilsey M, Veni Madhavan C (2011) Improved LSB steganalysis based on analysis of adjacent pixel pairs. SIViP 7(5):811–816
8. Everingham M (2015) The PASCAL object recognition database collection. http://host.robots.ox.ac.uk/pascal/VOC/databases.html#VOC2005_1. Accessed 14 July 2017