Steganalysis for LSB inserts in low stego-payload artificial color images

D E Vilkhovskiy
Dostoevsky Omsk State University, pr. Mira, 55, Omsk, 644007, Russia
vilkhovskiy@gmail.com

Abstract. In this study a new method of steganalysis is presented for detecting and locating a hidden message embedded using LSB replacement as a steganography algorithm. The method is applied for analysing artificial color images of a gradient fill and shows high detection and locating accuracy in low stego-payload of 25 to 10 percentage. The method is based on analysing pixel combinations of an LSB map to classify unique and non-unique pixel combinations and finding the largest rectangle algorithm for, respectively, detecting and locating purposes. To exclude noisy data from further consideration, a pre-processing filter is developed and presented.

1. Introduction
LSB replacement is a quick, cost-effective, and easy-to-apply steganography method to hide a secret message in an image. Despite numerous papers on LSB steganalysis, the problem of detection still exists for two reasons, at least. First, attackers steadily decrease stego-payload to avoid detection – up to 40-10%. Currently, thanks to a huge number of images sent via email, social media, or other electronic channels, sending dozens or even hundreds of stego-images, each containing a small piece of hidden message, is not associated with great costs or effort. However, most well-known methods of steganalysis, such as RS-steganalysis [1], HCF-COM steganalysis [2], ALE-steganalysis [3], SRM-model [4], etc, do not offer a reliable solution for low stego-payload images.

Second, partially, this low stego-payload problem can be solved with algorithms based on machine learning [5, 6] and, especially, on convolutional neural networks [7,8]. However, CNN-based steganalysis is a cost-intensive solution while methods based on machine learning, being less cost-intensive, still, show poor detection accuracy when dealing with 25-% and, especially, 10-% payload.

Third, detection-only methods do not answer the question about where the insert is located. Nevertheless, an exact hidden message location is crucial for further steganalysis and discovering the exact message itself.

Besides, most of them are capable to analyze only grayscale images, leaving color images without proper coverage. Thus, it is important to develop a method of steganalysis for color images that will have high detection accuracy for low payloads and will be able to detect the exact location of the hidden message to create a solid ground for further message extraction.

In this study, we started with steganalysis of artificial color images with a gradient fill. To clarify, being artificial, such color images are still more complicated stego containers to deal with if compared with grayscale images as they are based on three components – red, green, blue – each of their can vary from 0 to 255. Thus, the choice of artificial color images as a focus of the study is reasonably justified.
2. General problem statement
For the purpose of this study, a message was hidden in a blue component and located within a left top quarter of an artificial color image with gradient fill. A monochrome bitmap for a zero layer for an artificial color image with LSB insertions used as a testing example is presented in figure 1.

![Image](image1.png)

Figure 1. A monochrome bitmap for a zero layer of the artificial image of gradient fill used as a testing example.

It is evident that the area with LSB replacement visually differs from the area that is free from any hidden messages. To clarify, LSB-insertion changes pixel sequence along with destroying its order. Therefore, the embedding area mostly contains unique pixel combinations, while the non-embedding area contains a large number of repeating pixel combinations that form black-and-white stripes, which are clearly defined in figure 1.

Further in the study, we present an algorithm that can detect an area with a high density of unique pixel combinations and, thus, detect an LSB-insert and its location.

3. Analysing pixel combinations of an LSB-map
Analysing pixel combinations of an LSB-map aims to detect LSB-insertions and build a basis for locating the embedded area.

The method is based on sequential analysis of each of the pixels of the least significant bit map where the analysed pixel is taken in a group of two pixels neighboured at left, right, up, down, and in all four diagonals. An example of a pixel combination group with the analyzed pixel centered is presented in figure 2.

![Image](image2.png)

Figure 2. An example of pixel combination group with the analyzed pixel centered.

The pixel group combination is recorded binarily in slots of a hash map, a special data structure with values and keys. The keys are used to navigate the user and computing means through data array, so that for each key there is only one value in the map.

For the purpose of steganalysis presented in this study, the key is an exact location of the analysed pixel in the analysed monochrome bitmap for the zero layer while the value is a binary recorded pixel
combination. For the example, provided in figure 2, a binary recorded pixel combination is presented in equation (1) as the following subsequence:

\[
\begin{pmatrix}
0 & 0 & 1 & 1 & 0 \\
1 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 1 & 1 \\
1 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 0
\end{pmatrix}
\]  \( (1) \)

After recording, all combinations are subsequently compared with each other to detect repeated combinations. The repetitions are recorded in a second hash map, where the key is still an exact location of the analysed pixel and a value is the number of repetitions detected for the analysed combination, recorded in the first hash map.

Then, a binary matrix \( M_0 \) is formed using a logical IF-function as follows:

- if a value (the number of combination repetitions) for the analyzed key is zero, then, the combination is recognized as unique and the analyzed pixel gets binary 0
- else – the combination is recognized as non-unique and the analyzed pixel gets binary 1

If the built matrix contains 0 values located in a part of the image area with high density while another part of the image area contains a great number of 1 values, then the steganalysis result is classified as positive and the image is classified as stego. If no high-density 0 value area is detected, the steganalysis result is classified as negative and the image is classified as non-stego.

4. Finding the largest rectangle to locate an LSB-insert
Finding the largest empty rectangle was first considered by A. Naamad, D. Lee and V. Shu [9] with some subsequent clarification and modifications in other studies [10].

4.1. Basics of the algorithm to find the largest empty rectangle
The algorithm analyzes a source matrix \( M_0 \) to build a resulting matrix \( M_1 \):

- assigns the ‘0’ value to all binary 1 of the matrix \( M_0 \)
- assigns the index number from 1 to \( \infty \) to binary 0 of the matrix \( M_0 \)
- recursively generates a rectangle area using a matrix \( M_1 \)

An example of a source matrix \( M_0 \) and a resulting matrix \( M_1 \), got after the finding largest empty rectangle algorithm is applied, is presented in table 1.

| Table 1. An example of a source matrix \( M_0 \) and a resulting matrix \( M_1 \) |
|-----------------|-----------------|
| **Source matrix \( M_0 \)** | **Resulting matrix \( M_1 \)** |
| 0 0 0 1 1 0 | 1 1 1 0 0 1 |
| 0 0 0 0 0 0 | 2 2 0 1 2 0 |
| 0 0 0 0 0 0 | 3 3 1 2 3 1 |
| 0 1 0 0 0 1 | 4 4 2 3 4 2 |
| 1 0 0 1 0 0 | 5 0 3 4 5 0 |

A rectangularized area in the example, provided in table 1, is presented in figure 3.
4.2. Noisy data problem

For purpose of this study, noisy data refer to a single 1-value or a group of 1-values in a source matrix $M_0$ that are located among 0-values with the density not exceeding 70%. To clarify, noisy data are pixels of combinations that repeat once or twice for the analyzed bit map but are located among a bulk of unique combinations.

Noisy data create certain limitations for using the largest empty rectangle algorithm, narrowing the area to find. The main risk of that area narrowing is that such area contains only part of the hidden message. Therefore, a found content of such a message can be unclear or even contradictory to its true content.

An example of a pixel map with noisy data in the embedded area is presented in figure 4. The detected area of an LSB insertion for the example, provided in figure 4, is presented in figure 5. White dots on figures 4 and 5 are occasional non-unique pixel combinations that are considered as noisy data.

4.3. Pre-processing filter for noisy data

To improve locating LSB-inserts, noisy data shall be excluded from further analysis. For this, a pre-processing filter is to be applied. Earlier, noisy data was described as a single 1-value or a small group of 1-values in a source matrix $M_0$ located among 0-values with the density not exceeding 70%. The preprocessing filter detects such random 1 values and converts them to 0-values.

Examples for pixel maps with noisy data in the embedded area, provided in figure 3, and the detected area of an LSB-insertion after applying a pre-processing filter, is presented, respectively, in figures 6 and 7.
5. Conclusion

For the example, provided in figure 1, a detected and successfully located LSB-insert is presented in figure 8 as a grey rectangle. As it can be seen, the area of this grey rectangle is of high accuracy and covers the embedding area almost in full.

To conclude, the presented method of steganalysis for LSB-inserts in low stego-payload artificial color images, based on finding the largest empty rectangle with filter pre-processing, provides high LSB-inserts detection accuracy. One of its values is its capability to locate LSB-inserts at high locating accuracy.

References

[1] Fridrich J, Goljan M and Soukal D 2003 Higher-order statistical steganalysis of palette images Proc. of SPIE vol. 5020 pp 178–190
[2] Harmsen J and Pearlman W 2003 Steganalysis of additive noise modelable information hiding Proc. of SPIE vol 5020 pp 131–142
[3] Cancelli G, Doerr G, Cox I J and Barni M 2008 Detection of 1 ± LSB Steganography based on the Amplitude of Histogram Local Extrema Proc. Int. Conf. Image Processing pp 1288–1291
[4] Goljan M, Fridrich J and Cogranne R 2014 Rich model for steganalysis of color images. In Information Forensics and Security (WIFS), IEEE International Workshop. pp. 185–190
[5] Kumar U P and Shankar D D 2019 Blind Steganalysis for JPEG Image using SVM and SVM-PSO Classifiers International Journal of Innovative Technology and Exploring Engineering (IJITEE) vol 8 pp 1239 – 1246
[6] Chaeikar A 2019 Ensemble SW image steganalysis: A low dimension method for LSBR detection. Signal Process Image Commun, vol 70 pp 233–245
[7] You W, Zhang H and Zhao X 2020 A Siamese CNN for Image Steganalysis. *IEEE Transactions on Information Forensics and Security* vol. 16 pp 291–306

[8] Kim J, Park H and Park J-I 2020 CNN-based image steganalysis using additional data embedding. *Multimed Tools Appl* vol 79(1–2) pp 1355–1372

[9] Naamad A, Lee D T and Hsu W-L 1984 On the Maximum Empty Rectangle Problem. *Discrete Applied Mathematics* pp 267–277

[10] Acharyya A, De M, Subhas C and Pandit S 2020 Variations of largest rectangle recognition amidst a bichromatic point set *Discrete Applied Mathematics* vol 286 pp 35–50