Steganalysis for DCT inserts with the Koch-Zhao steganographic method in low stego-payload images

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

Abstract. This study focuses on the problem of detecting and locating secret data embedded using the Koch-Zhao steganographic method with discrete embedding. The proposed method of steganalysis is based on discrete cosine transform and enables to control and verify JPEG and MPEG images of stego-payload not exceeding 25%. Mid-frequency components are considered as the components targeted by the Koch-Zhao steganographic method. The proposed method of steganalysis delivers strong detection and locating accuracy and performs in 10-% stego-payload cases with sufficient reliability. Both gray-scale and color images can be verified on being a carrier or not being when using the detecting method proposed in the study.

1. Introduction

Though there is a wide range of simple but highly effective steganographic techniques that enable to hide a secret message in digital images used as carriers, many of them have some limitations regarding their capability to deal with the compressed images. To clarify, the limitation comes into effect when the user (either the sender or the recipient) compresses an image that has secret data in it. For example, being effective for uncompressed images, steganographic techniques based on the least significant bit (hereinafter, LSB) replacement or matching [1, 2] are not suitable for embedding secret data in compressed images.

Besides, if a stego image with an LSB insert is compressed, it becomes impossible to extract an embedded message as compression transforms LSB sequences while both LSB replacement and LSB matching deal exactly with a spatial domain. Besides, LSB replacement or matching is not applicable for such image standards as the JPEG and MPEG standards.

To avoid compression-associated limitations, other steganographic techniques were developed. Such techniques are based on manipulations performed within an image frequency domain, the domain that has little to no transformation while compressing. One of such methods was developed by Koch E. and Zhao J. – known as the Koch-Zhao steganographic method [3]. The method applies frequency conversions based on discrete cosine transform (hereinafter, DCT) coefficients. It is robust against compression and cost-effective regarding its requirements, efforts, and computing facilities to perform embedding. Besides, the Koch-Zhao steganographic method is fully applicable for the JPEG and MPEG standards, which are already based on DCT processing.

Thus, to ensure the Information Security of a company, organization, or another entity and prevent sensitive data to be exported to any third party that is not among the authorized data stakeholder, a method of steganalysis against the Koch-Zhao steganographic method is developed and proposed in this paper.
2. General problem statement

As mid-frequency components, instead of high- and low-frequency components, are the components that the analyzed DCT-based steganographic method targets due to the low risk of getting any visually-detected image distortion the use of mid-frequency components enables to achieve, the study focuses on mid-frequency components as well.

In one of previous works [4], a proposed method of steganalysis against the Koch-Zhao steganographic method was based on the hypothesis that embedding is performed as continuous embedding.

In this study, we focus on non-continuous, discrete embedding and present a new method of detecting and locating a DCT-based hidden message for low stego-payload color images, where the hidden data area does not exceed 25% of the carrier capacity. Histograms for continuous embedding and discrete embedding are presented, respectively, in figure 1 and figure 2.

![Figure 1. Continuous embedding.](image1)

![Figure 2. Discrete embedding.](image2)

The long vertical lines in figure 5 represent areas embedded with a hidden message while empty spaces between them represent embedding-free areas.

Further in the study, we present an algorithm that can detect and locate the hidden message using the DCT subsequence changes between an embedding and embedding-free areas.

3. Analysing DCT subsequence and its signatures

In general, the algorithm for detecting and locating DCT inserts is based on two signatures – deviations of the current element values from the subsequence maximum and their next neighbored element.

The algorithm consists of the following steps:

Step 1. Generating new subsequence $C_{i}^{(j)'}$ so that it presents only modular values and finding its maximum modular value $M_{j}$.

Step 2. Calculating the deviation of element values $P_{i}$ and $R_{i}$ through the entire subsequence $C_{i}^{(j)}$ as presented below:

$$P_{i} = M_{j} - |C_{i}|,$$  \hspace{1cm} (1)

$$R_{i} = C_{i} - C_{i+1},$$  \hspace{1cm} (2)

where $C_{i}$ is the value of the analyzed subsequence element;

$C_{i+1}$ is the value of the subsequent element next to the analyzed element.

Step 3. Building an aggregated signature array for further classification and clustering. An example of an aggregated signature array is presented in figure 3, where $(x, y)$ coordinates are $(P_{i}, R_{i})$ deviations calculated for each of the elements in provided subsequence.

For clustering and finding cluster centroids, K-means clustering algorithm and machine learning are used.
Figure 3. An aggregated signature array.

Step 4. Analysis of aggregated signature array. Ideally, here the following pattern is to be applied:

- If $P_i \to 0$ – then, the element signifies carrying a hidden message inside
- If $P_i \to M_j$ – then, the element signifies not carrying a hidden message inside
- If $|R_i| \to M_j$ – then, the element signifies being a boundary of the hidden message
- If $R_i \to 0$ – then, the element signifies not being a boundary of the hidden message

For each given subsequence element, being classified as not being a boundary of the hidden message does not show any correlations with being a carrier or not-carrier.

Thus, the element is classified as a secret data carrier only if the following statement is true for this element:

$$P_i \to 0; R_i \to 0$$

(3)

Thus, for the example, provided in figure 3, a detected embedding area is grouped elements located within the gray rectangle as it is presented in figure 4.

Figure 4. An embedding area detected.

4. Applying machine learning for automatic clustering and classification
The statement described in formula (3) cannot be verified as sufficient for solving clustering and classification problems. To clarify, as it is presented in figures 3 and 4, both $P_i$ and $R_i$, while tending
to $0$ value rather than $M_j$ value, are not really equal to zero. Thus, for our example, the following statement is true:

\[ 0 \leq P_i < 14 \]  \quad (4)
\[ 0 \leq R_i < |12| \]  \quad (5)

In addition, further analysis shows that there is some centered value for each of the elements of the sample array. Thus, the clustering and classification problem could be narrowed to the task of finding the relevant cluster centroid. In other words, the element is classified as a secret data carrier only if the following condition is met for this element:

\[ P_i \rightarrow k; \ R_i \rightarrow m, \]  \quad (6)

where $k$ and $m$– respectively, $x$ and $y$ coordinates for the cluster centroid.

The number of clusters relevant for each exact case and the exact cluster centroids are initially unknown. Thus, to solve this task machine learning and some clustering algorithm should be applied.

For the purpose of our study, K-means algorithm designed for unsupervised learning and clustering is suitable to use. There are a lot of variations of K-means clustering regarding how to calculate cluster centroids and other aspects [5]. The main questions to find answers there are as follows:

- how many clusters should be taken for the given array?
- what are the centroids for each cluster to have correct clustering?
- what are $k$ and $m$ for the cluster that contains elements with embedding

Here, we use K-means algorithm main of which was presented by Arthur D and Vasilvitsky S in their study [6].

Based on our empirical research, the optimal number of clusters for the purpose of detecting and locating a hidden message is four clusters.

For the example provided in figure 3, cluster centroids are presented in figure 5 in form of large grey dots.

![Figure 5. Clusters and cluster centroids.](image-url)
The centroid coordinates for the cluster that contains elements with embedding are \((6.046658, -0.012688)\)

5. Conclusion

The proposed method of steganalysis is a low dimension method, which make it efficient but cost-effective in detecting and locating hidden messages embedded using the Koch-Zhao steganographic method. The method deals with just two signatures, deviations of the current element values from the subsequence maximum and their next neighbored element values, which are used for clustering all the elements with K-means algorithm of unsupervised learning, famous for its great performance for solving clustering tasks.

References

[1] Bhuiyan T, Sarower A H, Karim R and Hassan M 2019 An Image Steganography Algorithm using LSB Replacement through XOR Substitution International Conference on Information and Communications Technology (ICOIACT) pp 44–49

[2] Jadhav V V and Belagali P P 2016 An effective Image steganography using LSB Matching International Journal of Advanced Research in Computer and Communication Engineering vol 5, issue 3 pp 15–19

[3] Koch E and Zhao J 1995 Towards robust and hidden image copyright labeling IEEE Workshop on Nonlinear Signal and Image Processing pp 452–455

[4] Belim S V and Vilkovskiy D E 2019 J. Phys.: Conf. Ser. 1210 012012

[5] Geron A 2019 Hands-on machine learning with Scikit-Learn, Keras, and Tensorflow concepts, tools, and techniques to build intelligent systems 2nd Edition ISBN 978-1-492-03264-9

[6] Arthur D and Vasilvitsky S 2007 K-Means++: The Advantages of Careful Seeding Proceedings of the 18th Annual ACM-SIAM Symposium on Discrete Algorithms pp 1027–1035