ANALYSIS OF STEGANOGRAPHIC METHODS IN DCT DOMAIN

Vladimír HAJDUK*, Martin DZIAK*, Miroslav VOZŇÁK**, Dušan LEVICKÝ*
*Department of Electronics and Multimedia Communications, Faculty of Electrical Engineering and Informatics, Technical University of Košice, Letná 9, 042 00 Košice, Slovak Republic, Tel.: +421 55 602 2861, E-mail: vladimir.hajduk@tuke.sk, martin.dziak.4@student.tuke.sk, dusan.levicky@tuke.sk
**Department of Telecommunications, Faculty of Electrical Engineering and Computer Science, VSB-Technical University of Ostrava, 17. listopadu 15, 708 33 Ostrava, Czech Republic, tel. +420 603 565 965, E-mail: voznak@ieee.org

ABSTRACT

The main role of steganalysis is a successful detection of secret communication. This communication is exclusively created by steganography. Steganographic methods deals with hiding a secret information into any type of multimedia data, for example to static images. Among basic requirements to steganographic systems belongs the perceptual transparency. Inserted information is perceptually transparent if an average subject is unable to distinguish any difference between data before and after embedding process. Nevertheless, each steganographic method necessarily causes some change in some statistical parameter. It represents the basis for building a successful steganalyzer. In this article are tested the impact of four steganographic methods to the selected statistical parameters which are usually utilized in the image objective quality assessment. Specifically, peak signal-to-noise ratio, normalized cross correlation, a local histogram of DCT coefficients and sample variance. The contribution of the article consists in the usage of results in the theory of statistical vector creation in building the particular image steganalytic method.

Keywords: *histogram, statistical parameters, steganalysis, steganographic methods, steganography, variance*

1. INTRODUCTION

The aim of steganography is to establish a subliminal channel which does not arouse a suspicion [1].

Example: there are two participants (they can be denoted as A and B) who want to communicate each other securely by sending the data via an Internet. If A wants to send a message to B, utilizes encryption in order to make it potentially unreadable. The third participant C is able to monitor the channel, but they cannot read the message. Although an encryption ensures secure communication, it reveals that there is a concealed information transmitted. The steganographic methods solve this problem. For example, if sender embeds a secret message into a static image and transmits it to the receiver, it will seem like an ordinary communication to participant C.

Moreover, an important attribute of steganographic methods is a minimization of impact to image statistical parameters after an embedding process, since the greater impact a method has, the more vulnerable to detect by an attacker it is [2]. In other words, the goal is to make a method more resistant to steganalysis [3]. In general, steganalytic technique extracts statistical parameters from a testing image to evaluate them by the previously trained model. Result is the statement whether an image contains a secret message or not [4] [5].

The proposed article deals with an embedding of secret messages by diverse steganography algorithms in order to detect an impact to four statistical parameters. Results can be utilized to make a set of statistical parameters to build universal or targeted steganalytic system [6].

2. STATISTICAL PARAMETERS

In general, the basic image processing quality parameter is PSNR (Peak Signal-to-Noise Ratio). PSNR indicates the ratio between the maximum energy of signal and maximum energy of noise in an image. PSNR is obtained by equation (1) [7].

$$PSNR = 10 \cdot \log\left(\frac{\left(2^n - 1\right)^2}{MSE}\right)[dB] \tag{1}$$

In (1), n represents bit depth of an image and MSE mean square error [8]. MSE is calculated by (2).

$$MSE = \frac{1}{M \cdot N}\sum_{i=1}^{M}\sum_{j=1}^{N}\left[f(i,j) - g(i,j)\right]^2 \tag{2}$$

Component $f(i,j)$ denotes pixels of original image with spatial resolution $M \times N$ whereas $g(i,j)$ represents stego image pixels with the same resolution. When MSE equals zero, compared images are the same. Contrarily, the higher the value is, the more different images are.

Next statistical feature utilized in the work is Normalized Cross Correlation (NCC) (3) [9] [10]. It is not dependent on the image size and achieves high efficiency.

$$NCC = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N} X_{i,j} \cdot Y_{i,j}}{\sum_{i=1}^{M}\sum_{j=1}^{N}\left(X_{i,j}\right)^2} \tag{3}$$

Elements $X_{i,j}$ represent the pixel values of the original image and $Y_{i,j}$ are stego image pixel values. Image dimension is $M \times N$.

The third statistical parameter was obtained from a discrete cosine transformation domain (DCT domain). It was differential histogram of DCT coefficients between cover and stego images [11]. It was sufficient to use local histogram of 11 values occurring near the maximum (4).

$$h_b^{i,j} \subset h^{i,j}, \quad b = \{-5,\ldots,5\}, b \in Z \tag{4}$$

The last but not less important characteristic in statistics is the sample variance [12]. In general, sample

variance is the expectation of the squared deviation of a random variable from its mean, and it informally measures how far a set of (random) numbers are spread out from their mean. It is defined by equation (5), where (6) is a deviation from mean and n represents the number of samples. For matrices, the result is a row vector containing the variance of each column.

$$S^2 = \frac{\sum_{i=1}^{n}(x_i - \bar{x})^2}{n-1} \tag{5}$$

$$x_i - \bar{x} \tag{6}$$

3. TESTING PARAMETERS

The randomly generated secret messages were embedded into 200 cover images in JPEG format using steganographic methods MB1, MB2 [13], nsF5 [14] and PQ [15] (i.e. different secret message to each image). For the methods nsF5 and PQ there were messages with payloads 0.1, 0.5 and 1 bpnz (secret message size in bits per non-zero AC DCT coefficients). On the other hand, for the methods MB1 and MB2 was chosen payload with 0.1, 0.2 and 0.3 bpnz, since the methods MB1 and MB2 have smaller maximal capacity than the previous methods [16]. PQ method used a converted database of cover images into grayscale.

Statistical parameters of static images which have been observed were PSNR, local histogram, NCC and sample variance. The messages have been inserted into images with different resolutions and statistical characteristics thus the results in the tables were averaged to a single image. The objective statistical parameters were not correlated with any subjective evaluation.

4. EXPERIMENTAL RESULTS

As a first statistical parameter was chosen PSNR. In the following Table 1 are shown the values that represent the average impact of each steganographic method to the cover image database.

Table 1 The average PSNR values for the sample of 200 images

Payload [bpnz]	nsF5 PSNR [dB]	PQ PSNR [dB]	Payload [bpnz]	MB1 PSNR [dB]	MB2 PSNR [dB]
0.1	55.64	28.08	0.1	50.97	49.49
0.5	46.68	28.07	0.2	48.12	46.72
1	40.42	28.07	0.3	46.45	45.16

It is obvious that PSNR was decreasing with increasing the payload for all steganographic algorithms. However, the PQ method caused considerably lower values of PSNR than the other methods. The reason is that the PQ operates with grey images only, thus in the calculation, there are not included two other matrices as in a color image.

Results from the normalized cross-correlation point of view are shown in the Fig. 1. There are used three different payloads for all four steganographic methods. The payload represents percentage of each steganographic method´s maximal capacity (see the section 3).

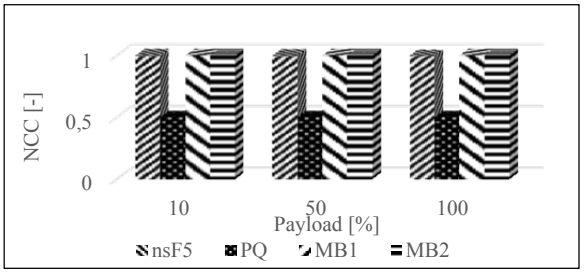

Fig. 1 Average NCC values of steganographic algorithms nsF5, PQ, MB1 and MB2

Methods nsF5, MB1 and MB2 obtained NCC higher than 0.99. It points to the fact that cover and stego images were almost the same. For the PQ method it was around 0.5.

The local histograms of DCT coefficients of the cover and stego images are illustrated in the Fig. 2 and Fig. 3.

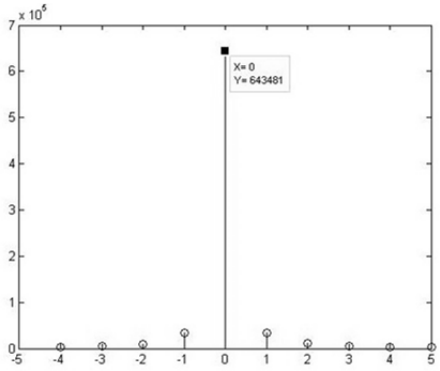

Fig. 2 Local histogram of cover image DCT coefficients

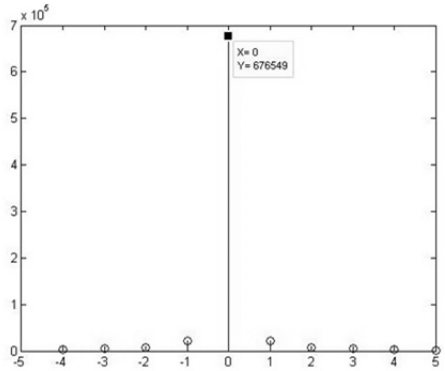

Fig. 3 Local histogram of stego image DCT coefficients

The local histogram of cover images was obtained by calculation of each cover image local histogram with the subsequent averaging. The same calculation was performed for stego images of all algorithms with the three different message sizes. The result was 14 local histograms where the first belonged to cover images, second to cover images of PQ method and 12 left to the stego images of the each steganographic method and secret message size.

An example of the calculation of differential local histogram between cover and stego images is shown in the

Table 2. In more details, it is differential local histogram between cover images and stego images of the method MB1 (payload = 0.3 bpnz) and method nsF5 (payload = 1 bpnz).

Table 2 Average frequency of 11 DCT coefficients of cover images and nsF5 and MB1 stego images

Coef.	Freq. (cover images)	Freq. (MB1/ 0.3)	Freq. (nsF5/1)	Dif. (MB1/ 0.3)	Dif. (nsF5/1)
-5	2296	2298	1994	-2	302
-4	3349	3342	2818	7	531
-3	5327	5335	4347	-7	980
-2	10259	10144	7789	116	2470
-1	30637	30753	20447	-116	10190
0	563250	563250	593951	0	-30701
1	30848	30982	20626	-134	10222
2	10393	10259	7900	134	2493
3	5406	5413	4405	-7	1001
4	3401	3394	2866	7	535
5	2328	2328	2013	0	315

The result difference between the frequencies of DCT coefficients from the Table 2 is shown in the Fig. 4 and Fig. 5 in the form of histogram.

The first histogram shows that the method MB1 have not affected frequency of zero DCT coefficients. The same results were obtained for the method MB2 too. On the other hand, methods MB1 and MB2 most affected frequency of values 1, -1, 2 and -2.

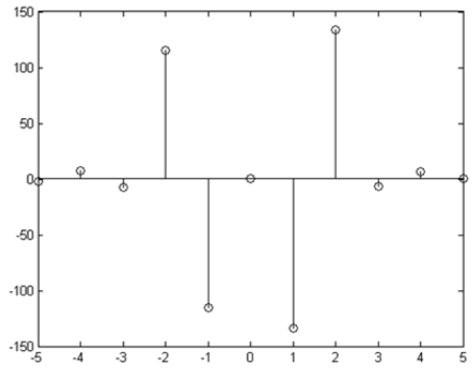

Fig. 4 Differential histogram between cover and stego images of method MB1 with 0.3 bpnz message size

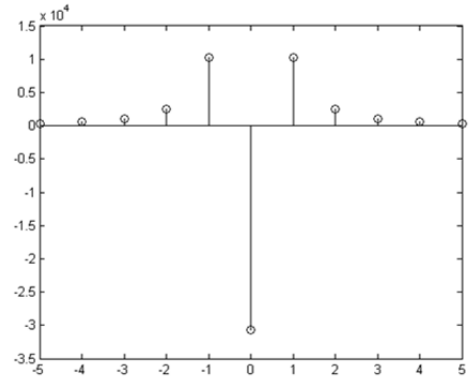

Fig. 5 Differential histogram between cover and stego images of method nsF5 with 1 bpnz message size

For the method nsF5, the frequencies of all stego DCT coefficients are smaller than in cover images except the zero value. Frequency of 0 is greater than in cover images.

The last statistical parameter utilized in the experiments was sample variance. Sizes of the secret messages were the same as in the previous simulations.

Table 3 Sample variance between cover and particular stego image databases

Payload [bpnz]	nsF5 Variance [-]	PQ Variance [-]	Payload [bpnz]	MB1 Variance [-]	MB2 Variance [-]
0.1	0.32	83.5	0.1	0.75	1.01
0.5	2.61	83.57	0.2	1.44	1.93
1	11.59	83.65	0.3	2.14	2.8

The Table 3 shows that by increasing size of secret message the sample variance was increasing as well. For the method nsF5 the variance ranged from 0.35 to 11.59. The smaller value belonged to 0.1 bpnz and the second one to max. size of message (1 bpnz). Methods MB1 and MB2 achieved similar results each other, whereas the method MB1 has less impact to the observed statistic. From all method the worst results achieved technique PQ. For all message sizes was observed variance higher than 83.

5. CONCLUSIONS

In the article, there was observed the impact of steganographic methods to the selected statistical parameters. Specifically, Peak Signal-to-Noise Ratio, Normalized Cross Correlation, local histogram of DCT coefficients and sample variance. Obtained results show that PSNR is generally increasing with increasing the size of a secret message for the all steganographic methods. We can say that all methods, except the PQ method, satisfy the PSNR limit between the cover and stego image. It has been assessed to 40 dB. Such a difference is imperceptible to the human eye. PSNR of PQ method was around 28 dB, what is already recognizable by an average human visual system. The calculation of NCC showed similar results. The methods nsF5, MB1 and MB2 achieved a value 0.99. It shows a nearly identical consistency of cover and stego images. The PQ method had achievements around 0.5. The difference in the local histogram between cover and stego images demonstrated that each of the tested methods affected it. The methods MB1 and MB2 maintained zero frequency coefficients, whereas the method nsF5 significantly increased the frequency of zero coefficients after the insertion process. From the sample variance point of view, the methods MB1 and MB2 achieved similar results. For the method nsF5 the variance ranged from 0.35 to 11.59. The biggest impact to the sample variance achieved PQ method.

ACKNOWLEDGMENTS

This publication arose thanks to the support of the Operational Programme Research and development for the project "(Development of the Centre of Information and Communication Technologies for Knowledge Systems) (ITMS code 26220120030), co-financed by the European Regional Development Fund".

REFERENCES

[1] AL-ANI, Z. K. – ZAIDAN, A. A. et al.: Overview: Main Fundamentals for Steganography, In: *Journal of Computing*, Vol. 2, No 3, pp. 158–165, 2010, ISSN 2151-9617.

[2] HOGAN, M. T. – BALADO, F. – SILVESTRE, G. C. M. – HURLEY, N. J.: Secure and robust steganography using side information at the encoder, In: *IEE Proceedings - Information Security*, Vol. 153, No. 3, pp. 87–95, Sept. 2006.

[3] BRODA, M. – HAJDUK, V. – LEVICKÝ, D.: The Comparison of Classifiers in Image Steganalysis, In: *Acta Electrotechnica et Informatica*, Košice, FEI-TU, Vol. 14, No. 4, pp. 1–4, 2014, ISSN 1335-8243.

[4] HAJDUK, V. – LEVICKÝ, D.: Cover selection steganography, *International Symposium ELMAR*, Zadar, pp. 205–208, 2016.

[5] BÖHME, R.: *Advanced Statistical Steganalysis*, Dresden: Springer 2010, ISBN 978-3-642-14312-0.

[6] COX, I. J. et al.: *Digital Watermarking and Steganography*, 2nd ed., USA: Burlington: Morgan Kaufmann Publishing, 2008, ISBN 978-0-12-372585-1.

[7] LEVICKÝ, D.: *Multimédiá a ochrana ich obsahu*, Košice, Elfa, 2012, ISBN 978-80-8086-199-5.

[8] TAN, H. L. – LI, Z. – TAN, Y. H. – RAHARDJA, S. – YEO, C.: A Perceptually Relevant MSE-Based Image Quality Metric, In: *IEEE Transactions on Image Processing*, Vol. 22, No. 11, pp. 4447–4459, Nov. 2013.

[9] HASNAT, A. – HAIDER, S. – BHATTACHARJEE, D. – NASIPURI, M.: Gray scale image colorization using normalized cross correlation, *International Conference on Inventive Computation Technologies (ICICT)*, Coimbatore, pp. 1–6, 2016.

[10] DUDÁŠ, M.: *Data hiding based on combination of DCT and SVD transformations,* Diploma thesis. Košice, TU FEI, 2015.

[11] PEVNÝ, T. – FRIDRICH, J.: Merging Markov and DCT Features for Multi-Class JPEG Steganalysis, In: *E. J. Delp and P. W. Wong, editors, Proceedings SPIE, Electronic Imaging, Security, Steganography, and Watermarking of Multimedia Contents IX*, San Jose, CA, Vol. 6505, pp 31–34, Jan. 29 – Feb. 1, 2007.

[12] HEINDEL, A. – KAUP, A.: Fast exclusion of angular intra prediction modes in HEVC using reference sample variance, *IEEE International Symposium on Circuits and Systems (ISCAS)*, Montreal, QC, pp. 2675–2678, 2016.

[13] SALLEE, P.: Model-based methods for steganography and steganalysis, In: *International Journal of Image Graphics*, pp. 167–190, 2005.

[14] FRIDRICH, J. – PEVNÝ, T. – KODOVSKÝ, J.: Statistically Undetectable JPEG Steganography: Dead Ends, Challenges, and Opportunities, In: *Proceedings of 9th workshop on Multimedia & security*, New York, 2007, ISBN 978-1-59593-857-2.

[15] FRIDRICH, J. – GOLJAN, M. – SOUKAL, D.: Perturbed quantization steganography, In: *ACM Multimedia System Journal*, pp. 98–107, 2005.

[16] MAJERČÁK, D. et al.: Performance evaluation of feature-based steganalysis in steganography, In: *Proceedings of the 23th International Conference Radioelektronika 2013,* Pardubice, Czech Republic: University of Pardubice, pp. 377–381, 2013, ISBN 978-1-4673-5518-6.

Received March 13, 2017, accepted August 25, 2017

BIOGRAPHIES

Vladimír Hajduk was born in Košice in 1990. He received his (M.Sc.) from Faculty of Electrical Engineering and Informatics, Technical University of Košice. Nowadays, he is a Ph.D. student at Department of Electronics and Multimedia Communications at Technical University of Košice. His research interests include image steganography, steganalysis, image processing and cryptography.

Martin Dziak was born in Stará Ľubovňa in 1994. He received his (B.Sc.) from Faculty of Electrical Engineering and Informatics, Technical University of Košice. His Bc. thesis was about modern methods of steganalysis under the supervision of Vladimír Hajduk. Nowadays, he is a M.Sc. student at Department of Electronics and Multimedia Communications at the same university.

Miroslav Vozňák was born in 1971 in Czech Republic, where he lives. He graduated from Faculty of Electrical Engineering and Computer Science VSB-Technical University of Ostrava and he holds a doctorate degree in Telecommunications from the same faculty (FEECS). He received his (Ph.D.) in 2002 and the thesis dealt with "Voice traffic optimization with regard to speech quality in network with VoIP technology". He is an IEEE Senior member and his research interests focus generally on information and communications technology, particularly on Voice over IP, quality of experience, network security and wireless networks.

Dušan Levický was born in 1948 in Slanec, Slovak Republic. He received the (M.Sc.) degree at the Faculty of Electrical Engineering at the Technical University of Košice in 1973. The (Ph.D.) degree received in 1985 in the field of electronics. In 1986 – 2012 he was the head of Department of Electronics and Multimedia Communications. In this time is full professor at the Faculty of Electrical Engineering and Informatics, Technical University of Košice. His research interests include multimedia communications, image coding, applied cryptography, digital image watermarking and steganography.