Use of the Normalized Gap of Maximum Singular Value of the Image Block to Evaluate the Capacity of the Steganographic Channel

Ivan Bobok[1], Alla Kobozieva[2] and Nataliya Kushnirenko[3]

[1,2, 3] *Odessa Polytechnic State University, Shevchenko av., 1, Odesa, 65044, Ukraine*

Abstract

The Least Significant Bit (LSB) method is one of the most widespread and demanded steganographic methods nowadays. Detection and decoding the hidden information, embedded in a container using the LSB, is a challenging task, in particular, in conditions of low capacity of the hidden communication channel. The existing steganalysis algorithms developed to detect the LSB, as a rule, solve the main problem of steganalysis - the detection of a hidden communication channel. However, the problem of the additional information recovery remains unfulfilled. The important step in solving this problem is the evaluation of the hidden (steganographic) channel capacity. In the current work, a digital image is used as container. All the results obtained can also be applied to digital video, which is considered as a sequence of frames. The aim of the work is to get estimates for the value of the capacity of the hidden communication channel, formed by the LSB method. To achieve the aim of the work the following studies carried out: performed additional in-depth investigation of properties of the normalized gap of the maximum singular value of non-intersecting image blocks, obtained by standard splitting; studied properties of a discrete function y(QF), that determines the number of image blocks in which the normalized gap of maximum singular value increases when the image is re-saved to lossy format with quality factor QF. As a result of the research, the estimates of the value of the capacity of the hidden communication channel, created using the LSB method and based on a container in a lossy format, were obtained.

Keywords

Steganalysis method, digital image, the capacity of the hidden communication channel, the LSB method, the normalized gap of singular value

1. Introduction

Steganography today is one of the most powerful and widely used areas of information security. One of the main questions here is who holds such a powerful means of protection, since the use of steganography, unfortunately, can lead to the setting up of hidden communication with anti-state, illegal, inhuman goals [1,2]. In such cases, early detection of hidden communication is critical. The main "weapon" for here is steganalysis [3]. Powerful efforts of scientists around the world today are aimed at solving the main task of steganalysis - to identify the presence of hidden (additional) information in information content [4]. However, in the condition of the information confrontation, that takes place in the modern world [2], these actions are not sufficient. Only the decoding of hidden information, its recovery will allow achieving the goal of steganalysis to the fullest. The extracting of hidden information and its decoding are the most

III International Scientific And Practical Conference "Information Security And Information Technologies", September 13–19, 2021, Odesa, Ukraine

EMAIL: onu_metal@ukr.net (A. 1); alla_kobozeva@ukr.net (A. 2); infsec2011@gmail.com (A. 3)
ORCID: 0000-0003-4548-0709 (A. 1); 0000-0001-7888-0499 (A. 2); 0000-0003-3722-0229 (A. 3)

complicated tasks. It can be facilitated by determining/evaluating the capacity of the organized steganographic channel [3,5], which is what this work is aimed at.

Today, one of the most widespread and demanded steganographic methods is the least significant bit modification method - *LSB* [3]. However, modern steganalysis methods, as a rule, do not evaluate the capacity of the hidden communication channel [6,7,8].

In [9], a steganalysis method was proposed, which aimed at detecting a hidden communication channel with low capacity. The method was based on properties of the normalized gap of the maximum singular value of image matrix block. In particular, it took into account the number of image blocks, obtained by standard matrix splitting, in which the normalized gap of the maximum singular value increased due to re-saving of image to a lossy format with different quality factors QF. This number was reflected by the discrete function $y(QF)$ that was built for the image under examination. Let us introduce the appropriate notation.

Let F be the matrix of the digital image, which is split in a standard way into non-intersecting *l*×*l*-blocks with singular values [10] $\sigma_1 \geq \sigma_2 \geq ... \geq \sigma_l \geq 0$, which form vector of singular values $\sigma = (\sigma_1, \sigma_2, ..., \sigma_l)^T$; the normalized vector of singular values $\bar{\sigma} = (\bar{\sigma}_1, \bar{\sigma}_2, ..., \bar{\sigma}_l)^T$ is determined by

$$\bar{\sigma} = \sigma / \|\sigma\|,$$

where $\|\sigma\|$ is a norm of vector σ. Then the normalized gap of the singular value $\sigma_i, i = \overline{1,l}$ is determined as follows [9]:

$$svdgap_n(i) = \min_{i \neq j} |\bar{\sigma}_j - \bar{\sigma}_i|,$$

whence it follows that the normalized gap of the maximum singular value is

$$svdgap_n(1) = \bar{\sigma}_1 - \bar{\sigma}_2$$

and

$$0 < svdgap_n(1) \leq 1$$

The efficiency of algorithmic implementation of the method proposed in [9] exceeds the modern analogues in terms of the detection of the hidden communication channel in conditions of a low capacity. It means, that the mathematical basis of the method provides sensitivity to small disturbances of the container in the process of steganographic transformation, and therefore can be considered promising for evaluating the steganographic channel capacity. To ensure the possibility of determining/evaluating the capacity of the hidden channel, additional studies of the properties of the function $y(QF)$ are required.

The aim of the work is to obtain estimates for the value of the capacity of the hidden communication channel, formed using the LSB method, by identifying the corresponding additional properties of $y(QF)$.

2. Main Body

Let the image were initially saved in a lossy format; F_1 is the matrix of the image, which is subject to examination. Formally, it is saved in a lossless format. If F_1 is a steganographic message, then we will assume that it is obtained on the basis of a Jpeg container with a matrix F . Let us apply to F_1 the steganographic transformation with the low capacity of the hidden communication channel (for example, 1%), which formally represented as [11]:

$$F_{1,1} = F_1 + \Delta F , \qquad (1)$$

where ΔF is the matrix representation of the additional information, $F_{1,1}$ is the matrix of the image-steganographic message. Let us define functions $y(QF)$ for F_1 and $F_{1,1}$ re-saving them with losses with all possible values of the quality factor *QF*. For a particular *QF*, as a rule, the value $y(QF)$ for $F_{1,1}$ will be greater than that for F_1. Geometrically it means that the $y(QF)$ graph for $F_{1,1}$ will be higher along the ordinate than the $y(QF)$ graph for F_1 whether the message or the container matches the matrix F_1. However, the difference between the values of the function $y(QF)$ (between the corresponding graphs) will be different depending on whether the matrix F_1 corresponds to the original image or steganographic message.

Let F_1 be the matrix of the container, then the steganographic message (1) for it will be the first and only one. If F_1 corresponds to the steganographic message, then for it (1) is a repeated steganographic transformation. Let us show that the primary transformation (1) with the help of the matrix ΔF will "lift" the $y(QF)$

graph higher along the ordinate compared to the graph constructed for F_1, than repeated transformation using the same matrix ΔF.

The steganographic transformation of the Jpeg container almost always leads to an increase in the smallest singular values and decrease in the normalized gap of the maximum singular value in the blocks involved in the steganographic transformation, thereby increasing the likelihood of the growth of the normalized gap of the maximum singular value when the image is re-saved into a lossy format. If the additional information is embedded in the image-steganographic message, then the normalized gap of the maximum singular value in blocks, involved in the primary steganographic transformation, is less than in the corresponding blocks of the original container. After the additional information is embedded in the steganographic message, the smallest singular values of the corresponding blocks involved in repeated steganographic transformation, which are no longer comparable to zero in those blocks that were involved in the primary transformation, can both decrease and increase. This fact can lead to both an increase and decrease in the normalized gap of the maximum singular value. Re-embedding the additional information in the steganographic message will generally increase the resulting capacity of the hidden communication channel, additionally disturbing the singular values, but the relative change in the smallest singular values of the container blocks be greater than in the smallest singular values of steganographic message with the same disturbance. Thus, the number of blocks in which the normalized gap of the maximum singular value will increase at re-saving with losses of the steganographic message, obtained as a result of consecutive double steganographic transformation will be greater, than when re-saving the primary steganographic message. However, the degree of this increase will be less than the degree of increase using the same (which is characterized by matrix ΔF), but the primary steganographic message on an empty container. Moreover, the degree of increase will be smaller the more the capacity of the hidden communication channel of the primary steganographic transformation. Indeed, the more the capacity of the hidden communication channel of the primary steganographic message, the more the number of container blocks, in which the normalized gap of the maximum singular value will decrease as a result of the steganographic transformation, the less the normalized gap of the maximum singular value in the blocks F_1 involved in the steganographic transformation, the “higher” will be the graph of the function $y\left(QF\right)$, obtained when re-saving F_1 with losses. When re-embedding additional information into a steganographic message formed with a relatively significant primary capacity of the hidden channel, there will be a significant number of blocks, where, after repeated steganographic transformation, the normalized gap of the maximum singular value will increase, rather than decrease, in comparison with the normalized gap of the maximum singular value in the block of the input steganographic message. This will lead to the fact that when re-saving a steganographic message obtained as a result of a double steganographic transformation, although the graph of the function $y\left(QF\right)$ will be higher than the graph of a similar function for the input steganographic message (obtained as a result of a single steganographic transformation), this difference will be the smaller, the larger was the capacity of the hidden channel of primary steganographic transformation. It was confirmed in practice by the results of a computational experiment, in which the following sets of digital images were involved:

- M_{Tif} – 500 images in lossless format (Tiff) (150 images from 4cam_auth base [12], 275 images from img_Nikon_D70s base [13], 75 images taken by non-professional camera);
- $M_{Jpeg,70}$, $M_{Jpeg,75}$, $M_{Jpeg,80}$ – each contained 500 images, obtained by re-saving of images from the set M_{Tif} to the Jpeg format with *QF*=70, 75, 80 respectively (the most frequently used quality factors in practice).

At the first stage, additional information was embedded into the original image (with or without loss) with the capacity of the hidden communication channel of 1, 5, 10%. The original image-container and the obtained steganographic messages were re-saved into lossy format (Jpeg) with all quality factors $QF \in \{1,2,...100\}$. As a result, discrete functions $y_0(QF)$ (for the container), $y_1(QF)$, $y_5(QF)$, $y_{10}(QF)$, $QF \in \{1,2,...100\}$ for the steganographic message were determined, respectively. A value characterizing the change in the function

$y_0(QF)$ was considered as a quantitative characteristic of the image change as a result of the primary steganographic transformation:

$$T_{0,i} = \left(\sum_{1}^{100} \left| y_0(QF) - y_i(QF) \right|^2 \right)^{\frac{1}{2}}, \qquad (2)$$

$i \in \{1,5,10\}$.

At the second stage, additional information was re-embedded with the channel capacity of 1% into the steganographic messages generated at the first stage (the matrix of additional information ΔF was randomly generated, the same matrix was used for steganographic messages with the channel capacity of 1, 5, 10%, formed on the basis of one container). Steganographic messages obtained after the repeated steganographic transformation were re-saved with losses (Jpeg format) with $QF \in \{1,2,...100\}$. As a result, discrete functions $y_{1,1}(QF)$, $y_{5,1}(QF)$, $y_{10,1}(QF)$, $QF \in \{1,2,...100\}$ were obtained for steganographic messages with the channel capacity of the primary steganographic transformation of 1, 5, 10%, respectively. By analogy with (2), the following value was considered as a quantitative characteristic of the change in the image-steganographic message after repeated transformation:

$$T_{i,1} = \left(\sum_{1}^{100} \left| y_i(QF) - y_{i,1}(QF) \right|^2 \right)^{\frac{1}{2}}, \qquad (3)$$

$i \in \{1,5,10\}$.

The experimental results for the original images in the lossy format for the case of the Jpeg format with the quality factor *QF*=75 are shown in Fig. 1 and in Table 1, where can be observed the general tendency of qualitative changes in the values of estimates (2), (3) with increasing the capacity of the hidden channel of the primary steganographic transformation: decreasing the mode of the histogram of values $T_{i,1}$ with a simultaneous increase in the value in the mode; decreasing the length of the interval of possible values $T_{i,1}$ by decreasing the maximum value. $T_{i,1}$. The quality results obtained are typical for lossy images, regardless of the specifics of the format (Jpeg) and the quality factor used (*QF*=75). Using a different lossy format (for example, Jpeg2000) or a different quality factor will only change the quantitative indicators of the histograms.

Analysis of the numerical values of (2), (3) using the obtained histograms (Fig. 1) allows us to make conclusions, that the following points are important for evaluation the value of the capacity of the hidden channel:

- If for image, which is under examination the value $T_{i,1} \geq 125$, then the steganographic transformation were not applied to it;
- If $61 < T_{i,1}$, then for analyzed image the capacity of the hidden channel is <5%, here the image can be a "clean" container;
- If $26 < T_{i,1}$, then for analyzed image the capacity of the hidden channel is <10%.

The results obtained at this stage of the research are not final, the quantitative estimates obtained for the capacity of the hidden channel are one-sided (upper estimates), such that they depend on the value of the capacity of the hidden channel of the primary stegano-transformation of the image in the Jpeg format (*QF*=75). By expanding the computational experiment, by increasing the variety of values of the capacity of the hidden channel for the primary stegano-transformation (for example, from 1 to K% with a step h%), the results obtained can be made more precise, what will be done in the development of the direct method for evaluating the capacity of the hidden communication channel. Using a different lossy format (for example, Jpeg2000) or a different quality factor *QF* will change the quantitative indicators of histograms, therefore, the development of a method requires quantitative characteristics for all possible (most used) values of the quality factor. Taking into account their possible variety, the preliminary step of determining *QF* for a container in a lossy format is required before using the method for estimating the capacity of the hidden communication channel. It can be done using, for example, the method proposed in [14,15].

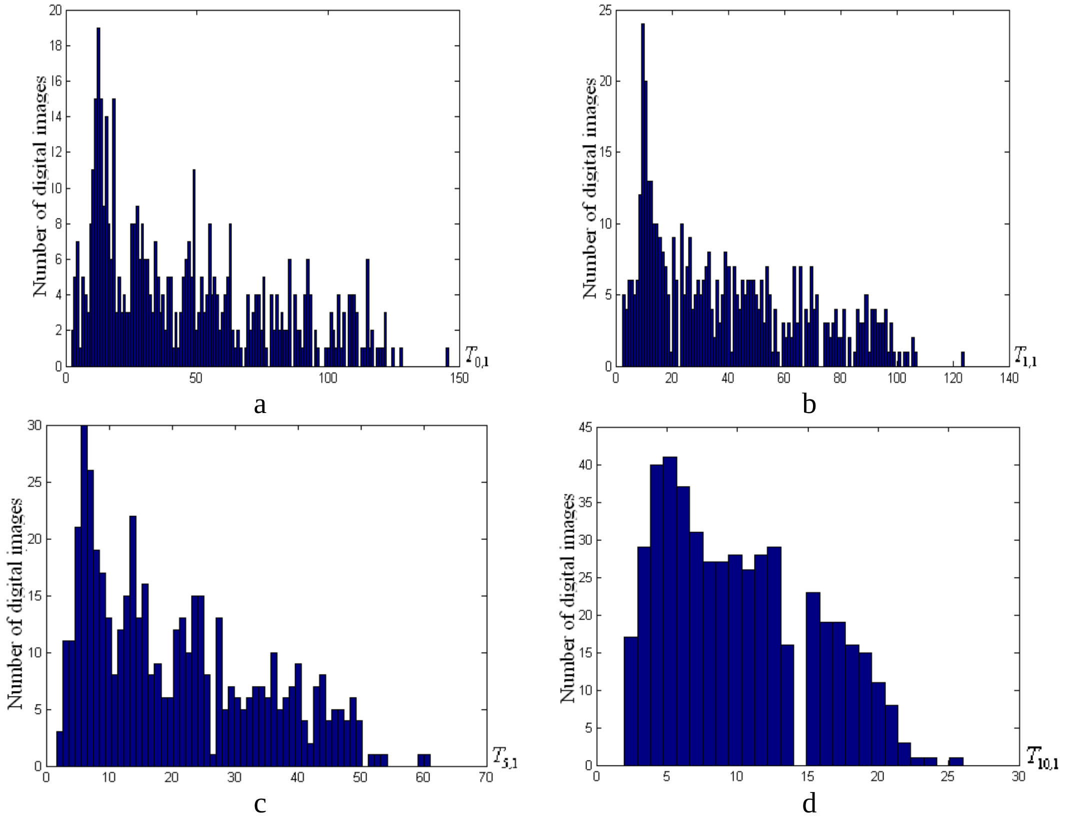

Figure 1: Histograms of values $T_{i,1}$, $i \in \{0,1,5,10\}$, for the original image-container, saved in Jpeg with QF=75: a – $T_{0,1}$ (the mode equals 13, the value in mode is 19); b – $T_{1,1}$ (the mode is 10, the value in mode is 24); c – $T_{5,1}$ (the mode is 6, the value in mode is 30); d – $T_{10,1}$ (the mode is 5, the value in mode is 41)

Table 1
Maximum and minimum values for the experiment $T_{i,1}$, $i \in \{0,1,5,10\}$ for image-containers, initially saved in Jpeg with *QF*=75

$T_{0,1}$		$T_{1,1}$		$T_{5,1}$		$T_{10,1}$	
Max	Min	Max	Min	Max	Min	Max	Min
146	2.1	124	2.4	61	1.7	26	2

3. Conclusions

The paper studied the properties of the normalized gap of the maximum singular value of the image matrix blocks, a discrete function $y(QF)$, that corresponds to the image in the conditions of its re-saving with losses with different quality factors and represents the number of blocks in which the normalized gap of the maximum singular value increases as a result of re-saving.

It is found that:

1. The number of image-steganographic message blocks, for which normalized gap of the maximum singular value increases when re-saving with losses, is greater, than in mage-container regardless of the container format (with/without losses);
2. The primary steganographic transformation of a digital image using a matrix ΔF changes («lifts» along the ordinate) the graph of the function $y\left(QF\right)$ higher, than a repeated steganographic transformation using the same matrix ΔF ;
3. The higher the capacity of the hidden communication channel of the primary steganographic transformation, the smaller the difference between corresponding

functions $y(QF)$ for steganographic messages, obtained by single and double steganographic transformations, while the same matrix ΔF is used to re-embed additional information regardless of the capacity of the hidden communication channel of the primary steganographic message.

As a result of the studies, one-sided estimates (from above) of the capacity of the hidden communication channel were obtained in the conditions of the image-container in the Jpeg format (*QF*=75). The conducted studies and the obtained results indicate that the chosen direction is promising for evaluating the capacity of the hidden communication channel of the primary steganographic transformation of a digital image and is currently being continued by the authors.

4. References

[1] W. Mazurczyk, S. Wendzel, S. Zander, A. Houmansadr, K. Szczypiorski (Eds.), Information Hiding in Communication Networks: Fundamentals, Mechanisms, Applications, and Countermeasures, Wiley, Hoboken, 2016. doi:10.1002/9781119081715

[2] L.G. Pirtskhalava, V.A. Khoroshko, Yu.E. Khokhlachova, M.E. Shelest, Information Confrontation in Modern Conditions, Comprint, Kyiv, 2019.

[3] A.V. Agranovsky, A.V. Balakin, V.G. Gribunin. Steganography, Digital Watermarking, and Steganalysis, Vyzovskaya kniga, Moscow, 2009.

[4] K. Karampidis, E. Kavallieratou, G. Papadourakis, A review of image steganalysis techniques for digital forensics, Journal of Information Security and Applications 40(2018). doi:10.1016/j.jisa.2018.04.005.

[5] V.S. Ponomarenko (Ed.), A method for estimating the value of the hidden bandwidth of a steganographic communication channel. Information systems in management, education, industry. Kharkiv, 2014.

[6] S.S. Chaeikar, A. Ahmadi, Ensemble SW image steganalysis: A low dimension method for LSBR detection, Signal Processing: Image Communication 70(2019). doi:10.1016/j.image.2018.10.004.

[7] S.S. Chaeikar, M. Zamani, A.A. Manaf, A.M. Zeki, PSW statistical LSB image steganalysis, Multimedia Tools and Applications volume 77 (2018). doi:10.1007/s11042-016-4273-6.

[8] S.T. Veena, S. Arivazhagan, Universal secret payload location identification in spatial LSB stegoimages, Annals of Telecommunications 74(2019). doi:10.1007/s12243-018-0676-x.

[9] I.I. Bobok, A.A. Kobozeva, Steganalysis method efficient for the hidden communication channel with low capacity, Radiotekhnika 198 (2019). doi:10.30837/rt.2019.3.198.02

[10] J.W. Demmel, Applied Numerical Linear Algebra, SIAM, 1997.

[11] A.A. Kobozeva, V.A. Khoroshko, Analysis of Information Security, DUT, Kyiv, 2009.

[12] Y. Hsu, S. Chang, Detecting image splicing using geometry invariants and camera characteristics consistency, 2006 IEEE International Conference on Multimedia and Expo, Toronto, 2006. doi:10.1109/ICME.2006.262447

[13] T. Gloe, R. Böhme, The "Dresden Image Database" for benchmarking digital image forensics, 2010 ACM Symposium on Applied Computing (SAC '10), New York, 2010. P. 1585–1591.

[14] A.A. Kobozeva, I.I. Bobok, L.E. Batiene, Steganoanalytical Method Based on the Analysis of Singular Values of Digital Image Matrix Blocks, *Problemele Energeticii Regionale* 3 (2018). URL: http://journal.ie.asm.md/ru/contents/electronni-jurnal-338-2018