UDC 004.056.5 **DOI:10.30837/rt.2019.3.198.02**

I.I. BOBOK, PhD, A.A. KOBOZEVA, Doctor of Sciences

STEGANALYSIS METHOD EFFICIENT FOR THE HIDDEN COMMUNICATION CHANNEL WITH LOW CAPACITY

Introduction

The rapid development of digital steganography, the publication of a large number of scientific works in this area in the open sources and restriction and even the ban of the use of cryptography on the legislative level in many countries have led to an increase in the use of steganographic methods for transmitting and storing confidential information [1,2]. The main advantage of steganography compared to cryptography is the concealment of the very fact that the confidential information is present in a particular information content, which makes the use of the steganographic system the common solution for the organization of a hidden communication channel [3]. However, the goals of organizing such a channel may be different: from the harmless, concerning specific individuals, to those that threaten the stability and vitality of a group of people united by specific goals, or the society as a whole. In this connection, the relevance of organizing an effective steganalysis of informational content increases. Its main task is to identify the presence or absence of additional information embedded in the non-attracting content, or container [4].

The most commonly used containers when organizing a hidden communication channel are digital images (DI), which is why DI is considered in this paper.

Currently, all steganalysis methods according to [1] can be classified into 6 main categories:

- visual steganalysis (visual detection of differences between container and steganographic message;
- signature or specific steganalysis (these techniques search for signature patterns to determine the presence of a hidden message);
- statistical steganalysis (those techniques developed by analyzing the embedding procedure and determining certain statistics that get modified as a result of the embedding process);
- spread spectrum steganalysis (aimed at the detection of embedded data introduced by steganographic methods, which perform the frequency spectrum spreading of the signal-container, i.e. by SS-methods (Spread-Spectrum));
- transform domain steganalysis (in the process of steganalysis the transform domain of DI investigated, e.g. discrete cosine transform domain, discrete wavelet transform domain, singular decomposition domain, etc.);
- universal or blind steganalysis (these techniques tries to detect the embedded messages regardless the steganographic technique applied to cover image).

The methods of the last group seem to be the most attractive since they are not related to the features of specific steganographic algorithms. However, the practice shows that they cannot provide equally high efficiency in detection of the results of various steganographic transform methods.

The most widely used steganographic method of DI transform is the modification of the least significant bit (the LSB-method) in its various implementations. The LSB-method detection remains an actual task. There are a large number of different steganalysis methods aimed at detecting the results of the LSB-method [4 - 8], belonging to different categories listed above. Most often, they are focused on statistical analysis [2], so the features of the current use of the LSB-method (with the low capacity of the hidden communication channel (HCC) (embedding rate)) make the vast majority of existing steganalysis methods ineffective (with 0.1<HCC<0.25 bpp), and practically unsuitable (with HCC <= 0.1 bpp) for detecting the hidden information presence. The testing of many modern methods under HCC <0.1 bpp is not performed at all [2, 9, 10]. Although the research in this area is being conducted and the development of new approaches is in progress [11-14], the task of providing the high efficiency of steganalysis method for LSB-embedding detection, which does not depend on DI type (color or grayscale) under the low HCC is still not solved.

For example, in [11], a steganographic algorithm is proposed, which is positioned as capable under the conditions of low embedding rate (0.01 bpp), however, the accuracy for these conditions is only 52.28 %. Similar efficiency results obtained under the embedding rate of 0.01 bpp for the steganalysis algorithms developed in [14].

In [12], a steganalysis algorithm for grayscale images was developed. The results of testing the algorithm given in the paper were carried out on more than 9000 DIs and obtained under the HCC rate from 0.1 to 0.5 bpp with the error rate of 21.0 % for the smallest HCC value. Such a result obviously cannot be considered a satisfactory value.

The steganalysis algorithm developed in [13] for color DI deserves great attention. The algorithm is based on analyzing the features of changing the number of color triads in a matrix of unique image colors while embedding additional information: containers stored in a lossy format have a small number of consecutive triads of triplets, while as a result of steganographic transform, even with small values of HCC, there is a significant increase in the number of such the triads. This makes it possible to detect the presence/absence of additional information in the digital content analyzed. The HCC of 0.05 bpp was the smallest value considered when testing the developed algorithm, while the detection accuracy coefficient was *ACC* = 0.9865. However, the algorithm is not efficient for grayscale images, which is a significant drawback.

Due to the large amounts of information, which is stored, sent or processed nowadays and usually stored in lossy formats, it is reasonable to consider the DI in a lossy format (LF) as a container in this paper.

The *aim* of the work is to increase the efficiency of steganalysis by developing a new steganalysis method for detecting the presence of additional information embedded by the LSB-method into the DI-container under conditions of the low communication channel capacity.

The HCC <= 0.1 bpp is considered as low HCC values. The effectiveness of the steganalysis algorithm estimated by Type I and Type II errors, as well as by the detection accuracy coefficient, formally defined below.

Main Body

For distinctness and taking into account the widest spreading of the Jpeg it is considered as a lossy format for DI (with various quality factors $QF \in \{0,1,2,\ldots,99,100\}$) further in the paper, Tif is used as a lossless format (LLF), a single rectangular $m \times n$ – matrix is considered as a formal representation of an arbitrary DI.

Let the matrix of the original DI in the LLF be F_T, and the matrix of the corresponding DI, which was obtained from LF by means of its repeated saving is F_J. Denote an arbitrary 4×4 – block of F_T / F_J as B_T / B_J respectively. Let $\sigma_T = \left(\sigma_1\left(B_T\right), \sigma_2\left(B_T\right), \sigma_3\left(B_T\right), \sigma_4\left(B_T\right)\right)^T$, $\sigma_J = \left(\sigma_1\left(B_J\right), \sigma_2\left(B_J\right), \sigma_3\left(B_J\right), \sigma_4\left(B_J\right)\right)^T$ be the vectors, those elements are the singular numbers (SN) of B_T, B_J blocks and wherein:

$$\sigma_i\left(B_T\right) \geq \sigma_{i+1}\left(B_T\right),\ \ \sigma_i\left(B_J\right) \geq \sigma_{i+1}\left(B_J\right),\ i = 1,2,3,\ \sigma_4\left(B_T\right) \geq 0,\ \sigma_4\left(B_J\right) \geq 0. \qquad (1)$$

Let us normalize vectors σ_T and σ_J, the obtained result given below:

$$\bar{\sigma}_T = \frac{\sigma_T}{\|\sigma_T\|} = \left(\bar{\sigma}_1\left(B_T\right), \bar{\sigma}_2\left(B_T\right), \bar{\sigma}_3\left(B_T\right), \bar{\sigma}_4\left(B_T\right)\right)^T,\ \bar{\sigma}_J = \frac{\sigma_J}{\|\sigma_J\|} = \left(\bar{\sigma}_1\left(B_J\right), \bar{\sigma}_2\left(B_J\right), \bar{\sigma}_3\left(B_J\right), \bar{\sigma}_4\left(B_J\right)\right)^T, \quad (2)$$

where $\|\sigma_T\|$ and $\|\sigma_J\|$ are norms of σ_T and σ_J. The condition (1) obviously also holds for elements of vectors $\bar{\sigma}_T$ and $\bar{\sigma}_J$, which further will be called the normalized SN.

In [15], a general approach to solve the problem of identifying violations of the DI integrity was proposed. It is based on the perturbation theory and matrix analysis and underlies further

reasoning. The development of the approach was reflected in [16], where it was shown that for the majority of the corresponding blocks B_T and B_J and matrices F_T and F_J, obtained as a result of their standard splitting, the following equation takes place:

$$\angle\left[e_1,\bar{\sigma}_T\right] > \angle\left[e_1,\bar{\sigma}_J\right], \tag{3}$$

where $e_1 = (1,0,0,0)^T$ is a standard space basis vector R^4, $\angle\left[e_1,\bar{\sigma}_T\right]$, $\angle\left[e_1,\bar{\sigma}_J\right]$ are the magnitudes of the angles between the vectors $\bar{\sigma}_T$ and e_1, $\bar{\sigma}_J$ and e_1 respectively, and the lower the quality factor QF used to obtain F_J, the smaller will be the angle between the normalized SN vector in the block B_J and the vector e_1.

Consider the relation (3) in more detail. Taking into account that

$$\left(e_1,\bar{\sigma}_T\right) = \|e_1\|\left\|\bar{\sigma}_T\right\| cos\left(\angle\left[e_1,\bar{\sigma}_T\right]\right) = cos\left(\angle\left[e_1,\bar{\sigma}_T\right]\right),\ \left(e_1,\bar{\sigma}_J\right) = \|e_1\|\left\|\bar{\sigma}_J\right\| cos\left(\angle\left[e_1,\bar{\sigma}_J\right]\right) = cos\left(\angle\left[e_1,\bar{\sigma}_J\right]\right),$$

where $\left(e_1,\bar{\sigma}_T\right), \left(e_1,\bar{\sigma}_J\right)$ are the scalar products of corresponding vectors, the relation (3) is rewritten as follows:

$$\left(e_1,\bar{\sigma}_T\right) < \left(e_1,\bar{\sigma}_J\right),$$

where for the majority of the corresponding blocks of F_T and F_J matrices we obtain:

$$\bar{\sigma}_1\left(B_T\right) < \bar{\sigma}_1\left(B_J\right). \tag{4}$$

Consider the case, when the singular numbers of block B_T has been perturbed because of lossy compression of image with the matrix F_T, that led to perturbation of elements of vector $\bar{\sigma}_T$. Denote these perturbations as $\Delta\sigma_1, \ldots, \Delta\sigma_4$. Then for the corresponding block B_J we have:

$$\bar{\sigma}_i\left(B_J\right) = \bar{\sigma}_i\left(B_T\right) + \Delta\sigma_i, \quad i = \overline{1,4}. \tag{5}$$

Then, taking into account (4) for most blocks:

$$\Delta\sigma_1 > 0. \tag{6}$$

If we consider the Euclidean norm as a vector norm in (2), then taking into account the normalization of vectors $\bar{\sigma}_T$ and $\bar{\sigma}_J$ and relation (5), we have:

$$\sum_{i=1}^{4}\left(\bar{\sigma}_i\left(B_T\right)\right)^2 = \sum_{i=1}^{4}\left(\bar{\sigma}_i\left(B_J\right)\right)^2 = \sum_{i=1}^{4}\left(\bar{\sigma}_i\left(B_T\right) + \Delta\sigma_i\right)^2,$$

from where

$$\sum_{i=1}^{4}\left(2\Delta\sigma_i\bar{\sigma}_i\left(B_T\right) + \left(\Delta\sigma_i\right)^2\right) = 0. \tag{7}$$

Let us rewrite (7) in more detail:

$$2\Delta\sigma_1\bar{\sigma}_1\left(B_T\right) + \left(\Delta\sigma_1\right)^2 + \left(\Delta\sigma_2\right)^2 + \left(\Delta\sigma_3\right)^2 + \left(\Delta\sigma_4\right)^2 + 2\Delta\sigma_2\bar{\sigma}_2\left(B_T\right) + 2\Delta\sigma_3\bar{\sigma}_3\left(B_T\right) + 2\Delta\sigma_4\bar{\sigma}_4\left(B_T\right) = 0 \tag{8}$$

It is $\bar{\sigma}_1\left(B_T\right) > 0$ for almost all blocks of the original DI in the LLF. Then

$$2\Delta\sigma_1\bar{\sigma}_1\left(B_T\right) + \left(\Delta\sigma_1\right)^2 + \left(\Delta\sigma_2\right)^2 + \left(\Delta\sigma_3\right)^2 + \left(\Delta\sigma_4\right)^2 > 0,$$

and the equality to zero of the expression value on the left-hand side of (8) is possible only due to the fact that there are negative values among $\Delta\sigma_2$, $\Delta\sigma_3$, $\Delta\sigma_4$.

Let us demonstrate that it is $\Delta\sigma_2 \le 0$ for most DI blocks using proof by contradiction. Let us suppose that $\Delta\sigma_2 > 0$. Then consider the principal possibility that (8) equals zero due to $\Delta\sigma_3$, $\Delta\sigma_4$, i.e. is it possible, in principle, to provide the equality to zero of the expression in (8) only at the expense of $\Delta\sigma_3$, $\Delta\sigma_4$ negativity. To do this, assume that both of these values are negative: $\Delta\sigma_3 < 0$ and $\Delta\sigma_4 < 0$. Moreover, given the fact that singular numbers are always non-negative, the maximum possible modulo values of $\Delta\sigma_3$, $\Delta\sigma_4$ are as follows:

$$\Delta\sigma_3 = -\bar{\sigma}_3(B_T),\ \Delta\sigma_4 = -\bar{\sigma}_4(B_T). \tag{9}$$

Then

$$\bar{\sigma}_3(B_J) = \bar{\sigma}_4(B_J) = 0,$$

that means that the vector $\bar{\sigma}_J = (\bar{\sigma}_1(B_J), \bar{\sigma}_2(B_J), 0, 0)^T$ lies in a plane defined by two vectors of the standard space basis R^4: $e_1 = (1,0,0,0)^T$ and $e_2 = (0,1,0,0)^T$. The end of the vector $(\bar{\sigma}_1(B_J), \bar{\sigma}_2(B_J), 0, 0)^T$ due to its normalization lies on the unit circle, which is the intersection of the unit sphere of space R^4 and the mentioned plane, whose center coincides with the origin. This position of the vector $\bar{\sigma}_J$ is the result of a perturbation of the normalized vector $\bar{\sigma}_T$, i.e. the result of its rotation at a certain angle within the first coordinate orthant of space R^4. First two coordinates $\bar{\sigma}_1(B_T), \bar{\sigma}_2(B_T)$ of vector $\bar{\sigma}_T$ are the direction cosines of its projection onto the coordinate plane of space R^4, defined by the vectors of the standard basis e_1 and e_2. In this case, taking into account the conditions (1), a simultaneous increase in the two first coordinates of the vector could not occur as a result of the DI compression, and if the first coordinate exactly increased (see (6)), then the second one should decrease. Thus, with $\Delta\sigma_2 > 0$ it is impossible to provide (8) even under the condition (9), i.e. with the largest modulus of possible negative perturbations $\Delta\sigma_3$, $\Delta\sigma_4$. Thus:

$$\Delta\sigma_2 \le 0. \tag{10}$$

In [17] the concept of gap $svdgap(i,A)$ of the singular numbers $\sigma_i(A)$ of matrix A introduced:

$$svdgap(i,A) = \min_{i \ne j} |\sigma_j(A) - \sigma_i(A)|.$$

Let us introduce the similar concept for the normalized singular numbers $\bar{\sigma}_i(A)$ of matrix A. Let us define $svdgap_n(i,A)$ as normalized gap of singular number $\sigma_i(A)$ of matrix A, which can be determined as follows:

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

Taking into account the conditions (1) for any block B of any DI obtain:

$$svdgap(1,B) = \sigma_1(B) - \sigma_2(B),$$

$$svdgap_n(1,B) = \bar{\sigma}_1(B) - \bar{\sigma}_2(B). \tag{11}$$

Taking into account (11), (4), (10):

$$svdgap_n(1,B_J) = \bar{\sigma}_1(B_J) - \bar{\sigma}_2(B_J) > \bar{\sigma}_1(B_T) - \bar{\sigma}_2(B_T) = svdgap_n(1,B_T).$$

Thus, when storing DI in lossy formats in most DI blocks (for which (3) holds) the normalized gap $\bar{\sigma}_1(B_J)$ is greater than the normalized gap $\bar{\sigma}_1(B_T)$, where B_T, B_J are the corresponding blocks F_T, F_J.

Since, with a decrease in the quality factor *QF* used to save DI in the Jpeg format, the number of blocks for which (3) takes place will increase [16], the increase will be observed in the number of DI blocks in which the normalized gap of the maximum SN will grow compared to its normalized gap in the corresponding blocks of the corresponding DI in a lossless format. Indeed, the lossy compression in a certain way reflects on the SN values of DI blocks: it reduces the contribution of the signal high-frequency component, blurs DI and leads to a decrease in the minimum singular number values of blocks [18]. However, in case of a compression with a high quality factor (relatively small values of the elements of the quantization matrix) the changes in the SN will be insignificant, i.e. the number of DI blocks, for which the relation (3) will not hold in the case of high *QF* will be greater than in the case of small *QF*. The number of such blocks does not increase monotonously with the quality factor decreasing (increasing elements of the quantization matrix), since with decreasing of quality factor the value $\angle[e_1, \bar{\sigma}_J]$ will decrease [16], differing more and more from the value $\angle[e_1, \bar{\sigma}_T]$ in accordance with (3). The obtained theoretical conclusion is illustrated in 2 DIs in lossless formats (Tif), where a monotonous decrease took place in the number of DI blocks obtained as a result of standard splitting, in which an increase in the normalized gap of the maximum singular number was observed, with an increase in *QF* (Fig. 1). This conclusion found the practical confirmation in the results of the computational experiment, described in detail below (see Fig. 3 (curve 1)).

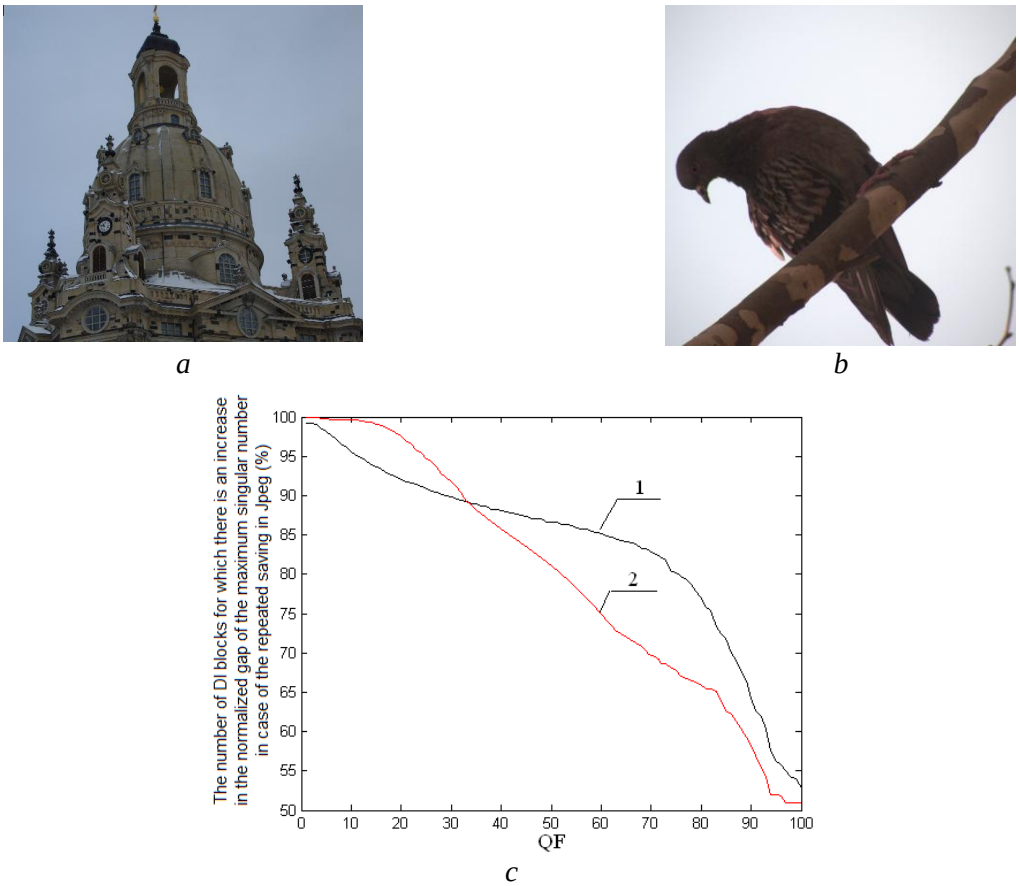


Fig.1. The results of the analysis of the maximum singular number normalized gap in the DI blocks with repeated saving in the Jpeg format with various quality factors *QF*: *a* – the original DI (Tif) from the img_Nikon_D70s base [19]; *b* – the original DI (Tif), obtained by a non-professional video camera; *c* – diagram that illustrates how the number of 4×4-blocks in DI, where the normalized gap of the maximum SN increased depends on *QF*: 1 – for DI from Fig.1, *a*, 2 – for DI from Fig.1, *b*

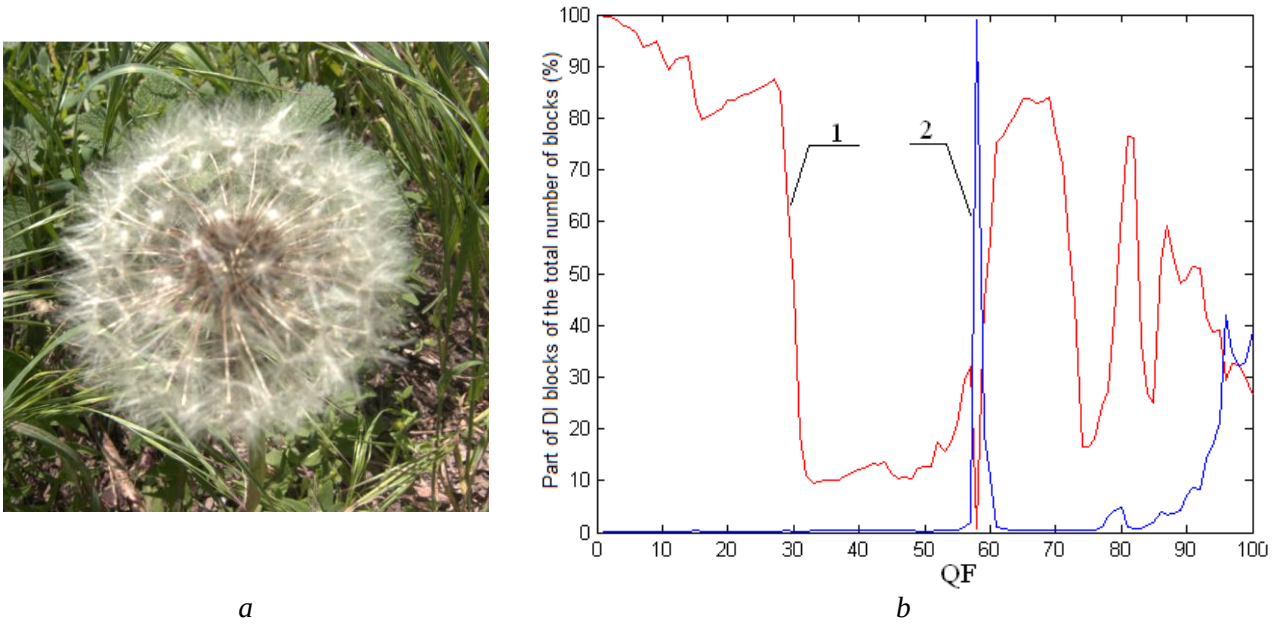
The monotonous increase in the number of blocks in the corresponding DI, for which the normalized gap of the maximum SN of block grows, will be violated with a decrease in the quality factor *QF* used to compress the original DI, if the image in lossy format (Jpeg) used as source. Indeed, if the original DI was stored with a quality factor QF_1, then its repeated saving with the same quality factor cannot significantly change the quantitative characteristics of the blocks, in particular, the singular number values (Table 1) (re-quantizing of the discrete cosine transform (DCT) coefficients in DI performed with the same quantization matrix as the primary one). Changes (if any) of the singular numbers will occur due to the presence of rounding in the process of compression [20], as well as rounding which causes the computational error when working in a floating point system. Therefore the number of blocks for which the normalized gap of the maximum SN will increase will be very small compared to the original DI (close to 0) (which is no longer typical for compression of image in the LLF with any quality factor), while the number of blocks, where the normalized gap of the maximum SN does not change, will be significant (the computational experiment shows, that the number of such blocks can exceed 90 % of the total number of blocks). However, the re-compression of the original DI with a quality factor different from QF_1 obviously breaks the above-mentioned monotony of changing the $4\times4-$blocks number, for which the normalized gap of the maximum SN increased, since the DI blocks have already been compressed (primary) with losses and the high-frequency component has already been reset to zero (taking into account the rounding that occur in the process of DI recovery after compression – it is close to zero). During the initial quantization, DCT coefficients corresponding to high (possibly medium) frequencies will be zeroed, resulting in a significant relative decrease in the lowest (possibly average) singular number values. Re-quantization will not significantly change the values of the DCT coefficients that became small after the initial quantization (and the smallest and possibly medium SN). For the maximum SN, the situation is different: as a result of quantization and subsequent rounding during the DI compression, the maximum singular number of block recovered after image quantization can both decrease and increase (depending on the rounding result after quantization), while three other singular numbers in block, as mentioned above, remain practically unchanged (this situation will occur for the same DI block when this image is saved for the second time with losses with different *QF*s (the results given in Table 1 for one randomly selected DI block stored in Jpeg format (QF = 85)) illustrate the above). This will lead to the fact that when DI is compressed with a quality factor $QF \neq QF_1$, the number of DI blocks for which the normalized gap of the maximum SN increases will be significantly different from zero, as the computational experiment shows, but the number of blocks where the normalized gap of the maximum SN will not change will decrease dramatically. These facts will lead to a loss of monotony for the number of blocks in which the growth of the normalized gap of the maximum SN occurred, with an increase in *QF*, which is an indication that the original DI was saved with losses.

Table 1

Result of repeated saving of original DI to Jpeg format with different quality factors QF, which was originally stored in Jpeg format (*QF*=85), for one $4\times4-$block

QF	Singular spectrum of the block				The normalized gap of the maximum SN
Original DI	**214.1468**	**4.8940**	**3.6310**	**0.1440**	**0.9768**
55	214.9262	3.0877	0.4180	0.1442	0.9855
60	210.4311	2.7594	0.9511	0.4780	0.9868
65	215.8175	2.8976	0.5545	0.3172	0.9865
70	210.2940	5.3903	1.7155	0.2854	0.9593
75	211.4048	5.6764	4.8425	0.0834	0.9677
80	213.0100	5.8375	3.5443	0.3043	0.9721
85	**214.1468**	**4.8940**	**3.6310**	**0.1440**	**0.9768**
90	214.0043	5.2478	4.1863	0.3131	0.9750
95	213.8960	4.8732	3.3984	0.4325	0.9768

The situation described above, in principle, can be obtained for DI, originally stored in Jpeg with any QF_1. Indeed, the original DI in the process of its analysis can be saved to the Jpeg format with each quality factor $QF \in \{0,1,2,\ldots,99,100\}$ (with step 1), which will give an opportunity to get a global minimum of the corresponding curve reflecting how the number of DI blocks in which the normalized gap of maximum SN increased as a result of repeated saving with losses depends on *QF*. The global minimum will be reached at $QF = QF_1$, and its value will be close to 0. The results of the analysis of a specific DI are shown in Fig. 2 to illustrate the truth of the above. Curves 1 and 2 (Fig. 2) have a global minimum and a maximum, respectively, with $QF = QF_1 = 58$, while the dependence of the number of DI blocks, in which there was an increase in the gap of the maximum SN, from *QF*, is not monotonic, which is in full compliance with the foregoing.



a *b*

Fig.2. The results of the analysis of the DI singular number blocks: *a* – the original DI (Jpeg format (QF = 58)); *b* – graphs which show relationship between the number of DI 4×4-blocks, given as a percentage of the total number of blocks, and the quality factor *QF* used in the repeated compression of DI: 1 – the number of blocks in which the normalized gap of the maximum SN increased; 2 – the number of blocks in which the normalized gap of the maximum SN did not change during the repeated saving

For practical confirmation of the findings, a computational experiment was carried out, which involved:

• 450 original DIs in a lossless format (Tif): 150 DIs from the 4cam_auth base [21] (size is 500×500 pixels) – set T_1; 200 DIs received by non-professional video cameras (size is 600×600 pixels) – set T_2, 100 DIs from the database img_Nikon_D70s [19] – set T_3 (size is 2000×2000 pixels);

• 4950 original DIs in Jpeg format, obtained by storing DIs from T_1, T_2, T_3 to Jpeg format with quality factors $QF \in M_1 = \{55,60,65,70,72,75,80,85,90,93,95\}$ (corresponding sets are denoted by $T_1^{(i)}$, $T_2^{(i)}$, $T_3^{(i)}$, $i \in M_1$).

In the experiment, each DI from the sets T_1, T_2, T_3, $T_1^{(i)}$, $T_2^{(i)}$, $T_3^{(i)}$, $i \in M_1$ was stored in the Jpeg format with values $QF \in M_2 = \{55,60,65,70,75,80,85,90,95\}$. Note that the elements of the sets M_1, M_2 were chosen as the most frequently used in practice, but at the same time M_1 contained values which were absent in M_2 by design, in order to consider such options when the quality factors of the secondary compression of DI do not coincide with the quality factor of the primary

one. In each of the 12 image groups $G_0, G_i, i \in M_1$ ($G_0 = T_1 \bigcup T_2 \bigcup T_3$, $G_i = T_1^{(i)} \bigcup T_2^{(i)} \bigcup T_3^{(i)}$, $i \in M_1$) for each quality factor $QF \in M_2$ used in repeated saving of the image, the average value of the number of DI 4×4-blocks obtained as a result of its standard splitting were calculated (as a percentage of the total block number) in which the normalized gap of the maximum SN increased. The results of the experiment, some of which are shown in Fig.3, fully confirm the theoretical conclusions obtained above.

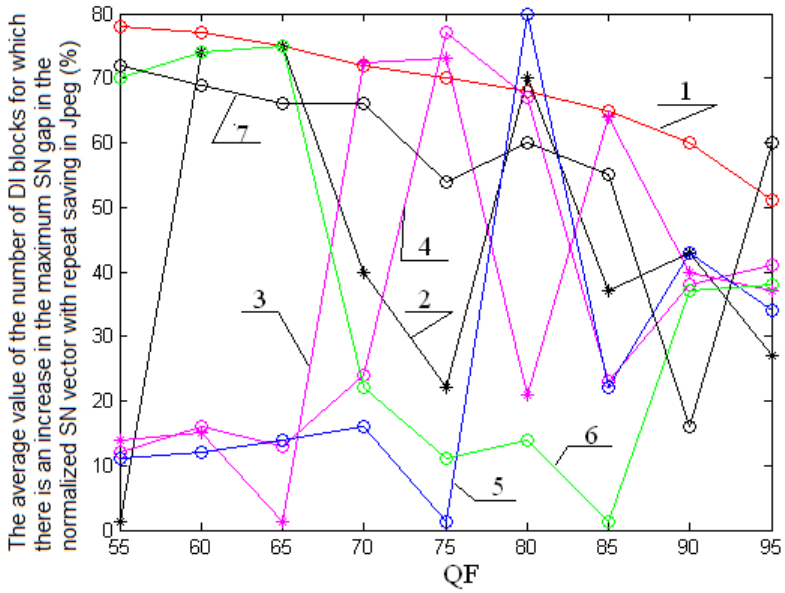


Fig. 3. Relationship between the average value of the DI block number, for which the normalized gap of the maximum SN increases as a result of DI repeated saving in Jpeg format, and the quality factor *QF* used for image repeated saving, when the original DIs were in the following formats: 1 – Tif; 2 – Jpeg with QF=55; 3 – Jpeg with QF=65; 4 – Jpeg with QF=72; 5 – Jpeg with QF=75; 6 – Jpeg with QF=85; 7 – Jpeg with QF=93

In the course of the experiment, it was revealed 6% of DIs from G_0, where a slight violation of the monotonous decrease in the block number occurred with an increased normalized gap of the maximum SN along with an increase in *QF* (a typical example is presented in Table 2). Obviously, this is a consequence of the features of machine arithmetic: calculations of SN blocks are performed in a set of floating-point numbers with an accumulation of computational error, which occurs here due to rounding. The possibility of such a situation is taken into account when developing the steganalysis method.

Table 2

Relationship between the relative number of blocks (% of the total number of DI 4×4-blocks obtained as a result of its standard splitting) with an increased normalized gap of the maximum SN and *QF* used for repeated saving, for a particular DI

QF								
55	60	65	70	75	80	85	90	95
67.66	67.06	66.45	**65.37**	**65.38**	65.00	63.29	58.40	42.76

The steganalysis method developed by the authors for detection of the steganographic transform results of any implementation of the LSB-method uses a DI in lossy format as a container, the expediency of which is justified above. After the embedding of an additional information, taking into account the well-known instability of the algorithmic implementations of the LSB method to attacks against the embedded message, the steganographic message is stored in a lossless format.

The main requirement for developed steganalysis method is the high efficiency in conditions of the low capacity of the hidden communication channel. The idea of this method is as follows. Due to the fact that in the conditions considered, the steganographic transform has little effect on the container, after the additional information embedding the properties of the DI steganographic message will not differ fundamentally from the properties of the used container. It means that for the matrix of the steganographic message, the dependence of the number of blocks, for which the normalized gap of the maximum singular number will increase, from the *QF* will not be monotonic.

In view of the above, the main steps of the proposed steganalysis method are as follows.

Let the DI with the matrix F_T be analyzed.

Step 1. Save the original DI in the lossy format – Jpeg with different quality factors $QF_i \in \{1,2,3,\ldots,100\}, i=\overline{1,t}$, $QF_i < QF_{i+1}, i=\overline{1,(t-1)}$. The result is the DI with matrices $F_i, i=\overline{1,t}$.

Step 2. For each pair of matrices F_T, $F_i, i=\overline{1,t}$, after the preliminary standard splitting them into non-intersecting $4\times 4-$blocks, determine the values $s_i, i=\overline{1,t}$, – is a number of blocks (a percentage of the total number of DI blocks) in $F_i, i=\overline{1,t}$, for which the normalized gap of maximum singular number increased compared to the corresponding blocks in F_T.

Step 3. *If*

$$\left((s_1 > s_2)\vee\left(0\le s_2 - s_1 \le P\right)\right)\wedge\ldots\wedge\left((s_{k-1} > s_k)\vee\left(0\le s_k - s_{k-1} \le P\right)\right)\wedge\ldots\wedge\left((s_{t-1} > s_t)\vee\left(0\le s_t - s_{t-1} \le P\right)\right),$$

(where P is the threshold value, which makes it possible to take into account the occurring monotony violations for the values $s_i, i=\overline{1,t}$, due to the peculiarities of machine arithmetic in the floating point system),

then

F_T – is an empty container

else

F_T – is steganographic message.

In the algorithmic implementation of the method, the following parameter values were used: $t=9$; $QF_i = 55+5(i-1), i=\overline{1,t}$; $P=1$.

To analyze the efficiency of the algorithmic implementation, a computational experiment conducted. During this experiment, the additional information was embedded by the LSB-method into DI-containers stored in Jpeg format. A randomly generated binary sequence was used as an additional information. The following values of the hidden communication channel capacity were used: 1, 0.1, 0.05, 0.01 bpp. As containers were used: 4950 images from the sets $T_1^{(i)}$, $T_2^{(i)}$, $T_3^{(i)}$, $i\in M_1$, and 350 DIs (size of 1000×1000 pixels) taken from the NRCS database [22] – the set T_J. In the course of the experiment, both the obtained steganographic messages and the original DIs from the sets T_1, T_2, T_3 were analyzed. The results of the computational experiment are given in Table 3 and Table 4 (the experiment-average value of Type II error is 2.7%). These results are illustrated on a specific example in Fig. 4, where 5 DI are presented in a lossless format, one of which is an original image, and the rest are the steganographic messages obtained by the LSB-method with different HCC values. The diagrams reflect how $s_i, i=\overline{1,9}$ depends on *QF*, used for repeated saving of the analyzed DI to Jpeg format, show that the monotony is present for the original DI (Fig. 4(f) curve 1), but there are monotony violations for DI steganographic messages (Fig. 4(f) curves 2-5).

For the convenience of comparing the efficiency of the method developed in the work with modern analogues, the obtained data were used to calculate the detection accuracy [13] (accuracy (ACC)) (Table 5):

$$ACC = (TP + TN)/(TP + FN + TN + FP), \quad (12)$$

where *TP* (*True Positive*) is the number of correctly identified steganographic messages (true positive result); *TN* (*True Negative*) is the number of correctly identified containers (true negative result); *FP* (*False Positive*) is the number of empty containers which were mistakenly qualified as steganographic messages (false positive (false alarm) or a Type II error); *FN* (*False Negative*) is the number of steganographic messages that are mistakenly identified as containers (false negative result Type I error).

Table 3

Type I errors of developed steganographic algorithm (%)

Container	**The capacity of a hidden communication channel (bpp)**			
	1	**0.1**	**0.05**	**0.01**
$T_1^{(95)}$	1.3	1.3	1.3	1.3
$T_1^{(93)}$	2	1.3	2	2
$T_1^{(90)}$	0.7	0	1.3	0.7
$T_1^{(85)}$	0.7	0.7	0.7	0.7
$T_1^{(80)}$	0.7	1.3	0.7	0
$T_1^{(75)}$	8	2	2	0.7
$T_1^{(72)}$	8	4	2	0.7
$T_1^{(70)}$	8	4	2	1.3
$T_1^{(65)}$	12	8	8.7	2
$T_1^{(60)}$	18.7	12	8.0	2
$T_1^{(55)}$	20	18.7	8.7	4
Image set average value ($T_1^{(i)}$, $i \in M_1$)	**7.3**	**4.8**	**3.4**	**1.4**
$T_2^{(95)}$	1.5	2	1	0.5
$T_2^{(93)}$	1.5	0	0.5	0
$T_2^{(90)}$	0	0	0	0
$T_2^{(85)}$	1	0	0.5	0.5
$T_2^{(80)}$	0	1	0.5	0
$T_2^{(75)}$	0	0	0	0
$T_2^{(72)}$	1	0	0	0
$T_2^{(70)}$	1.5	1	1	0
$T_2^{(65)}$	3.5	1	0.5	0.5
$T_2^{(60)}$	7	2	2	0.5
$T_2^{(55)}$	11.5	2.5	1	1
Image set average value ($T_2^{(i)}$, $i \in M_1$)	**2.6**	**0.9**	**0.6**	**0.3**
$T_3^{(95)}$	4	0	0	0
$T_3^{(93)}$	7	0	1	0
$T_3^{(90)}$	0	0	0	0
$T_3^{(85)}$	0	0	0	0

$T_3^{(80)}$	1	0	1	1
$T_3^{(75)}$	9	0	0	0
$T_3^{(72)}$	8	1	2	2
$T_3^{(70)}$	9	1	1	1
$T_3^{(65)}$	10	4	2	3
$T_3^{(60)}$	12	5	3	1
$T_3^{(55)}$	15	4	2	2
Image set average value ($T_3^{(i)}$, $i \in M_1$)	**6.8**	**1.4**	**1.1**	**0.9**
T_J	**0.9**	**0.6**	**0.6**	**0.9**
Experiment-average value	**4.8**	**2.2**	**1.5**	**0.8**

Table 4

Type II errors of developed steganographic algorithm (%)

Sets of original DIs		
T_1	T_2	T_3
0.7	0	11

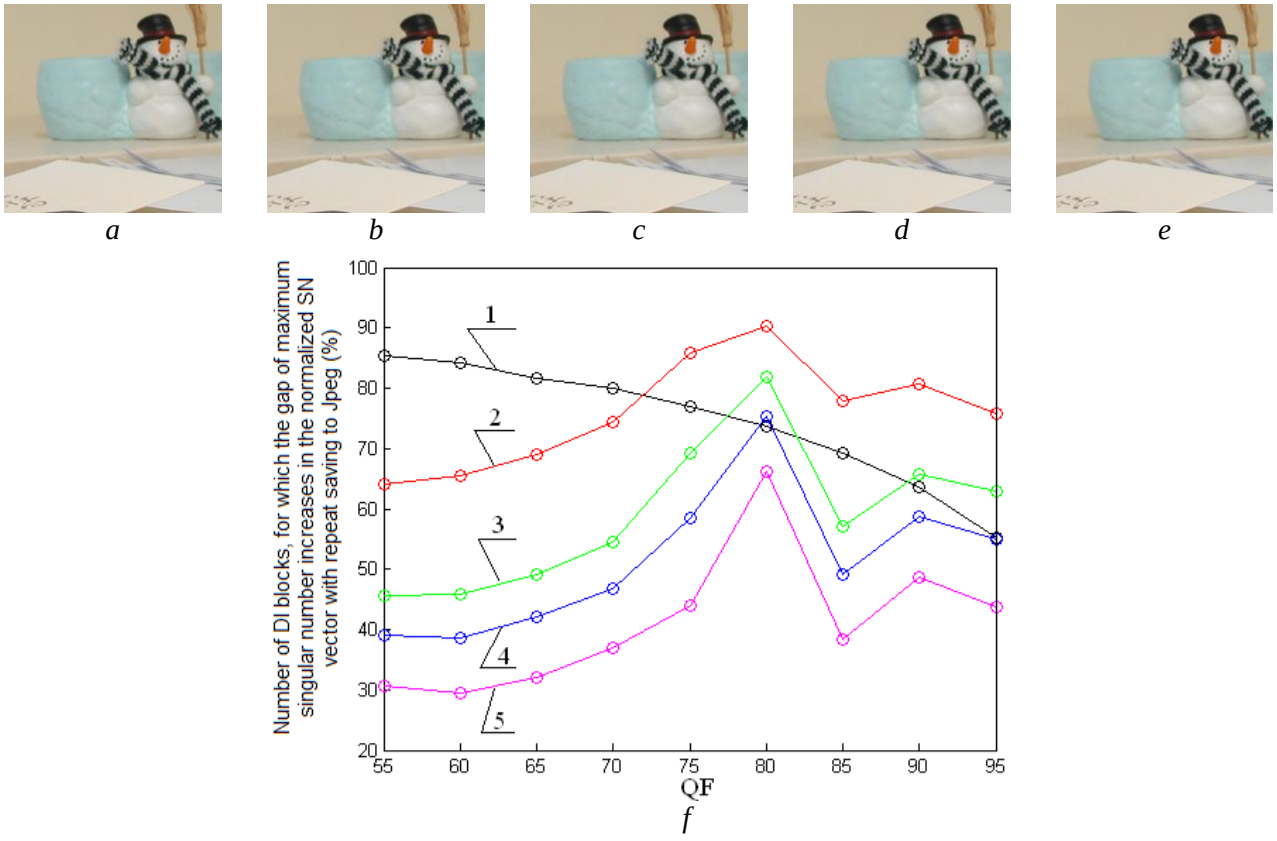


Fig. 4. Illustration of the steganalysis results obtained with developed algorithm for specific DIs: *a* – is an original DI; *b, c, d, e* – are steganographic messages, created by LSB-method with HCC 1, 0.1, 0.05, 0.01 bpp, respectively; *f* – diagrams that show how number of image blocks with an increased gap of maximum SN depends on *QF*, given that the image is converted for the second time to Jpeg format: 1 – for the original DI, 2,3,4,5 – for the steganographic messages, created by LSB-method with HCC 1, 0.1, 0.05, 0.01 bpp respectively

Table 5

The experiment-average (5750 DI) values of the detection accuracy coefficient for the developed algorithm, depending on the value of the HCC

The capacity of a hidden communication channel (bpp)			
1	0.1	0.05	0.01
0.954	0.978	0.987	0.991

The results of the computational experiment indicate a high efficiency of the algorithmic implementation of the developed method. The efficiency of the algorithm, as could be assumed on the strength of the theoretical basis of the developed method, increases with decreasing of HCC. Indeed, the smaller the HCC, the less perturbation is introduced into the DI-container by steganographic transform, the less DI steganographic message differs from the original container stored in the lossy format, the more effectively such steganographic message will be detected.

For a comparative analysis of the suggested algorithm efficiency, estimated by the ACC coefficient (12), modern analogous algorithms were chosen. These analogues are most efficient under the low HCC conditions and information about them is available from open sources: S1 (2006) [14], S2 (2006) [11], S3 (2008) [23], S4 (2009) [24], S5 (2010) [25], S6 (2015) [26], S7 (2015) [27], S8 (2016) [13], S9 (2016) [28]. The results are given in Table 6.

Table 6

Comparison of the developed algorithm efficiency, estimated using ACC, with modern analogues under the conditions of a low HCC

HCC, bpp	S1 (2006)	S2 (2006)	S3 (2008)	S4 (2009)	S5 (2010)	S6 (2015)	S7 (2015)	S8 (2016)	S9 (2016)	Our (2018)
0.1	0.9846	0.7727	0.9943	0.9937	0.9924	0.9971	0.988	0.9968	0.970	**0.978**
0.05	0.9769	0.6432	0.9283	0.9319	0.9404	0.9770	0.968	0.9865	0.941	**0.987**
0.01	0.5692	0.5094	-	-	-	-	-	-	-	**0.991**

Conclusions

As a result of the development of approach for detection of digital images integrity violations proposed by the authors earlier, the new steganalysis method has been created, as well as algorithm implementing it, which is effective in case of low hidden channel capacity, using LSB-method of embedding.

The computational complexity of the algorithm is determined by the number of non-intersecting 4×4-blocks into which the matrix of the analyzed DI is split, and in the case of its sizes of $n\times n$ pixels it is $\underline{O}\left(n^2\right)$ operations.

The developed algorithm significantly exceeds the existing analogues for HCC <0.1 bpp. With HCC = 0.01 bpp, this superiority over the best of its analogues (S1) is 74.1 %. In addition, it is workable for both color and grayscale DI, which often is not the case for analogues algorithms. In the case of an examination of color DI, 1, 2 or all color matrices (RGB scheme), brightness matrix (YUV scheme) will be analyzed.

References:

1. Karampidis K. A review of image steganalysis techniques for digital forensics / K. Karampidis, E. Kavallieratou, G. Papadourakis // Journal of Information Security and Applications. 2018. № 40. Pp. 217–235.
2. Saman Shojae Chaeikar. PSW statistical LSB image steganalysis / Saman Shojae Chaeikar, Mazdak Zamani, Azizah Bt Abdul Manaf, Akram M. Zeki // Multimedia Tools and Applications. 2018. Vol. 77, Iss. 1. Pp. 805–835.
3. Altaay A.A.J. An introduction to image steganography techniques / A.A.J. Altaay, S.B. Sahib, M.B. Zamani // Proceedings 2012 International Conference on Advanced Computer Science Applications and Technologies, ACSAT.
4. Li B. A survey on image steganography and steganalysis / B. Li, J. He, J. Huang, Y.Q. Shi // J. Inf. Hiding Multimedia Signal Process. 2011. No 2. Pp. 142–172.
5. Park T.H. Performance improvement of LSB-based steganalysis using bit-plane decomposition of images / T.H. Park, J.G. Han, Y.H. Moon, I.K. Eom // The Imaging Science Journal. 2016. No 64(5). Pp. 262–266.

6. Lerch-Hostalot D. LSB matching steganalysis based on patterns of pixel differences and random embedding / D.Lerch-Hostalot, D. Megias // Computers & Security. 2013. No 32. Pp.192–206.

7. Verma S. Relevance of steganalysis using DIH on LSB steganography / S. Verma, S. Sood, S.K. Ranade // International Journal of Advanced Research in Computer Science and Software Engineering. 2014. No 4(2). Pp. 835–838.

8. Xia Z. Steganalysis of LSB matching using differences between nonadjacent pixels / Z. Xia, X. Wang, X. Sun, Q.Liu, N.Xiong // Multimed Tools and Applications. 2016. No 75(4). Pp. 1947–62.

9. Lerch-Hostalot D. Unsupervised steganalysis based on artificial training sets / D. Lerch-Hostalot, D.Megías // Engineering Applications of Artifficial Intelligence. 2016. No 50. Pp. 45–59.

10. Juarez-Sandoval O. Compact image steganalysis for LSB-matching steganography / O. Juarez-Sandoval, M. Cedillo-Hernandez, G. Sanchez-Perez, K.Toscano-Medina, H. Perez-Meana, M.Nakano-Miyatake // In: Proceedings 2017 5th international workshop on biometrics and forensics (IWBF 2017). 2017. Pp. 1–6.

11. Zou D. Steganalysis based on Markov model of thresh-olded prediction-error image / D. Zou, Y.Q. Shi, W. Su, G.Xuan // 2006 IEEE international conference on multimedia and expo, ICME 2006 Proceedings, 2006. 2006. Pp. 1365–8.

12. Fridrich J. Steganalysis of content-adaptive steganography in spatial domain / J. Fridrich, J. Kodovský, V.Holub, M.Goljan // Lecture notes in computer science (including subseries on lecture notes in artificial intelligence lecture notes in bioinformatics (LNCS)). 2011. Vol. 6958. Pp. 102–17.

13. Ахмаметьева А.В. Стеганоанализ цифровых изображений, хранящихся в формате с потерями / А.В. Ахмаметьева // Захист інформації. 2016. Вип. 23. С.135-145.

14. Xiang-dong Chen. Detect LSB Steganography with Bit Plane Randomness Tests / Xiang-dong Chen, Feng Sun, Wei Sun // 6th World Congress on Intelligent Control and Automation, Dalian. 2006. Pp. 10306-10309.

15. Kobozeva A.A. General Principles of Integrity Checking of Digital Images and Application for Steganalysis / A.A. Kobozeva, I.I. Bobok, A.I. Garbuz // Transport and Telecommunication. 2016. Vol. 17, Iss. 2. Pp. 128-137.

16. Бобок И.И. Метод выявления изображений, пересохраненных в формат без потерь из формата с потерями // Математичне та комп'ютерне моделювання. 2017. Вип.16. С.5-14.

17. Деммель Д. Вычислительная линейная алгебра : теория и приложения / Пер. с англ. Х.Д. Икрамова. Москва : Мир, 2001. 430 с.

18. Кобозева А.А. Анализ информационной безопасности / А.А. Кобозева, В.А. Хорошко. Киев : ГУИКТ, 2009. 251 с.

19. Gloe T., Böhme R. The 'Dresden Image Database' for benchmarking digital image forensics. Proceedings of the 25th Symposium on Applied Computing (ACM SAC 2010). Sierre, 2010. Vol. 2, pp. 1585–1591.

20. Гонсалес Р. Цифровая обработка изображений / Р. Гонсалес, Р. Вудс ; пер. с англ. П.А. Чочиа. Москва : Техносфера, 2006. 1070 с

21. Hsu Y.-F. Detecting image splicing using geometry invariants and camera characteristics consistency / Y.-F. Hsu , S.-F. Chang // Proceedings of the IEEE International Conference on Multimedia and Expo (ICME'06). Toronto, 2006, pp. 549-552.

22. NRCS Photo Gallery: [Електронний ресурс] // United States Department of Agriculture. Washington, USA. Electronic resource. Access mode: http://photogallery.nrcs.usda.gov (Дата обращения: 26.07.2012).

23. Chen C. JPEG Image Steganalysis Utilizing both Intrablock and Interblock Correlations / C. Chen, Y.Q. Shi // IEEE International Symposium on Circuits and Systems. Seattle, Washington, USA, 2008. Pp. 3029-3032.

24. Huang F. Calibration based universal JPEG steganalysis / F. Huang, J. Huang // Science in china series F: Information sciences. 2009. Vol. 52. No. 2. Pp. 260-268.

25. Pevny T. Steganalysis by subtractive pixel adjacency matrix / T. Pevny, P. Bas, J. Fridrich // IEEE Transactions on Information Forensics and Security. 2010. No. 2. Pp. 215-224.

26. Jinyang Su. Steganalysis using regional correlation and second-order Markov features / Su Jinyang, Zeng Xianting, Wang Lei // International Journal of Security and Its Applications. 2015. Vol. 9. № 1. Pp. 69-76.

27. B. Xue, X. Li, B. Li and Z. Guo. Steganalysis of LSB replacement for multivariate Gaussian covers // 2015 IEEE China Summit and International Conference on Signal and Information Processing (ChinaSIP), Chengdu, 2015, pp. 836-840. doi: 10.1109/ChinaSIP.2015.7230522.

28. Q. Lin, J. Liu and Z. Guo. Local ternary pattern based on path integral for steganalysis // 2016 IEEE International Conference on Image Processing (ICIP), Phoenix, AZ, 2016, pp. 2737-2741.

Odesa National Polytechnic University *Received 21.04.2019*