UDC 004.056.5 **DOI:10.30837/rt.2019.4.199.16**

A.A. KOBOZEVA, Doctor of Engineering, Professor,
I.I. BOBOK, PhD, Associated Professor

METHOD FOR DETECTING OF DIGITAL IMAGE INTEGRITY VIOLATIONS DUE TO ITS BLOCK PROCESSING

Introduction

The detection of data integrity violations nowadays is one of the most significant issues for specialists in the field of information security [1-3]. In particular, this problem is highly relevant to digital images (DI), which this paper is dedicated to. Mentioned violations can be applied in different ways, have different goals and lead to various consequences. Using graphics editors, the digital image can be easily altered. For instance, "unwanted character" can be removed or replaced, new characters can be added, that can radically change the content of the depicted scene [2]. Impossibility to establish the fact of integrity violations for such images can lead to significant negative consequences for individuals and society as a whole, in case these images are used as material evidence in court, or as Black PR, etc.

Integrity violations of digital images occur when they are used as containers in modern steganographic systems. The frequency of such systems use is growing every day [3-5]. The organization of a hidden communication channel can lead to material damage to individual enterprises, firms, banks, etc. Moreover, it can cause the catastrophic consequences of a national scale as unauthorized users can utilize the information for anti-state activities.

In connection with those mentioned above, providing effective integrity verification for information contents has become the issue of current interest. In particular, for digital images, which used for non-entertaining purposes, the detection of integrity violations is essential.

Great attention is paid to the solution of this problem in the digital image examination [3,6]. However, the final solution has not been introduced yet, and the task of developing new methods for the detection of image integrity violations is still urgent.

Existing methods are usually aimed at identifying the results of specific perturbations: blurring the DI [7], sharpening [8], changing of brightness [9], etc. The steganalysis methods are also designed for specific steganographic methods [4]. However, when it comes to verification of digital image integrity, the list of possible perturbations is not always known. In this regard, it is difficult to overestimate the relevance of methods that allow to detect the presence of changes in the digital images and do not depend on special type of perturbations, which caused the changes, or methods, that are workable for a wide range of such actions (including, for example, applying different types of noise (which is a very common approach, often used for masking of other actions, such as cloning, steganographic transformation), various filtering, steganographic transformation based on various steganographic techniques). However, the lack of effective developments is currently observed, as open sources indicate.

The block processing of digital images is widespread today. It is typical for various modern steganographic algorithms, especially those that are positioned as resistant to compression with losses [10 – 12], it is also any processing that includes saving the resulting image in lossy formats (JPEG, JPEG2000), as well as local image processing, that takes place during photo editing, etc.

Block processing of digital images, regardless of the specifics, has its peculiarities [13]: its natural result most often leads to a decrease in the correlation of brightness values for nearby pixels, which are located at the boundaries of blocks used in processing, especially for those pixels that, being closest neighbours, will be on the borders of different blocks. With this in mind, there is a fundamental possibility of developing a method for detecting the block processing of the digital image, which is not focused only on a specific narrow set of options for such processing. However, the author did not find any related developments in open sources. Most often the object of studies, the results of which are available from the open sources, is the process of lossy image compression, and the aim is to find the block processing artefacts, which occurs at the same time [14, 15].

Aim and Tasks of the Research. The *aim* of the work is to ensure the effective detection of DI integrity violations due to its block processing, regardless of its specific type, by developing an appropriate method based on the results of the formal parameters studies of the digital image matrix blocks obtained by the author in [13].

To achieve the aim, the following tasks must be solved:

1. Based on the results of the studies obtained in [13], develop a method for detection of digital images block processing and perform its algorithmic implementation;
2. Considering the necessity to ensure the possibility of using the developed method for the integrity check of video sequences, provide the low computational complexity of the method algorithmic implementation;
3. Evaluate the effectiveness of the algorithmic implementation under various perturbing actions.

Main Body. Let **F** be the *n*×*m*-matrix of the digital image that is being examined. Split **F** in the standard way [16] into small square *l*×*l*-blocks. For a formal description of the block's properties, which denoted as **B**, one of the complete sets of its formal parameters is used [17]: the set of singular numbers and singular vectors of the block matrix, obtained using its normal singular decomposition [17]:

$$\mathbf{B} = \mathbf{U}\,\mathbf{\Sigma}\,\mathbf{V}^{\mathrm{T}}, \tag{1}$$

where **U**, **V** are orthogonal *l*×*l*-matrices of left and right singular vectors respectively, the columns **U** are lexicographically positive, **Σ** – diagonal *l*×*l*-matrix of singular numbers. It was found in [18] that for the original image in most of the *l*×*l*-blocks, the following relation holds:

$$\angle\left(\mathrm{u}_1,\overline{\overline{\sigma}}\right) \approx \angle\left(\mathrm{v}_1,\overline{\overline{\sigma}}\right) \approx \angle\left(\mathrm{n}^{\mathrm{O}},\mathrm{e}_1\right), \tag{2}$$

where $\angle(\mathrm{a},\mathrm{b})$ – an angle between vectors **a**, **b**; $\mathbf{u}_1$ and $\mathbf{v}_1$ – left and right singular vector of *l*×*l*-block respectively, that correspond to the maximum singular number σ_1 of this block, $\sigma_1 \geq \ldots \geq \sigma_l \geq 0$ is the singular number of the block,

$$\overline{\overline{\sigma}} = \left(\sigma_1^2,\sigma_2^2,\ldots,\sigma_l^{\,2}\right)^T \Big/ \left\|\left(\sigma_1^2,\sigma_2^2,\ldots,\sigma_l^{\,2}\right)^T\right\| \in R^l, \tag{3}$$

$\mathrm{n}^{\mathrm{O}} = \left(1/\sqrt{l},1/\sqrt{l},\ldots,1/\sqrt{l}\right)^T \in R^l$ is the *n*-optimal vector of space R^l, $\mathrm{e}_1 = (1,0,\ldots,0) \in R^l$ is the first vector of standard basis R^l.

As follows from (2), for the chosen approach, the vectors $\mathbf{u}_1$ and $\mathbf{v}_1$ behave identically, therefore, only $\mathbf{u}_1$ will be considered further in detail.

Regardless of the specifics and particular type, the block processing, as a rule, leads to specific consequences [13]: differences in changes in the number of small-sized blocks for which (2) holds, the matrix of the original digital image and one whose integrity was violated due to the block processing by shifting the grid of the matrix splitting. Based on the results of studies obtained in [13], a method for detection of the DI block processing proposed the main steps of which are as follows.

Step 1. Split in the standard way the digital image with matrix F, that is being analyzed, into small-sized blocks of $l \times l$ pixels. Let $B^{(l)}$ be an arbitrary block.

Step 2. For each block $B^{(l)}$ the following should be done:

2.1. Perform a normal singular decomposition (1): $B^{(l)} = U\Sigma V^T$;

2.2. Build a vector (3):

$$\overline{\overline{\sigma}} = \left(\sigma_1^2,\ldots,\sigma_l^2\right)^T \Big/ \left\|\left(\sigma_1^2,\ldots,\sigma_l^2\right)^T\right\|;$$

2.3. Find $\angle\left(u_1,\overline{\overline{\sigma}}\right)$.

Step 3. For the DI to be analyzed, the parameter $mod\, a_l$ of angle $\angle\left(u_1,\overline{\overline{\sigma}}\right)$, which corresponds to the largest number of image blocks and number of such blocks $MBlok_l$ must be determined (i.e., blocks, for which $\angle\left(u_1,\overline{\overline{\sigma}}\right) = mod\, a_l$).

If

$$mod\, a_l = \angle\left(n^O, e_1\right),$$

where $n^O \in R^l, e_1 \in R^l$,

then

if

$$MBlok_l \geq P_1,$$

where P_1 is an experimental threshold,

then

3.1. Split the DI under analysis into blocks of $2l \times 2l$ pixels. Let $B^{(2l)}$ be an arbitrary block.

3.2. For each of the obtained blocks $B^{(2l)}$:

3.2.1. Perform a normal singular decomposition (1): $B^{(2l)} = U\Sigma V^T$;

3.2.2. Build a vector (3):

$$\overline{\overline{\sigma}} = \left(\sigma_1^2,...,\sigma_{2l}^2\right)^T \Big/ \left\|\left(\sigma_1^2,...,\sigma_{2l}^2\right)^T\right\|;$$

3.2.3. Find $\angle\left(u_1,\overline{\overline{\sigma}}\right)$.

3.3. For image under analysis determine a parameter $mod\, a_{2l}$ of angle $\angle\left(u_1,\overline{\overline{\sigma}}\right)$, which corresponds to the largest number of image blocks, the number of such blocks is $MBlok_{2l}$ (blocks, for which $\angle\left(u_1,\overline{\overline{\sigma}}\right) = mod\, a_{2l}$), $MBlok = \left|MBlok_{2l} - MBlok_l\right|$

If

$$mod\, a_{2l} = \angle\left(n^O, e_1\right),$$

where $n^O \in R^{2l}, e_1 \in R^{2l}$,

then

if

$$\left(MBlok_{2l} \geq P_1\right) \& \left(MBlok \leq P_2\right),$$

where P_2 is an experimental threshold,

then

3.3.1. The image analyzed is being split into nonintersecting blocks of $l \times l$ pixels, while the splitting grid is shifted relative to the standard grid by P_3 pixels along the axis OX and by P_4 pixels along the axis OУ. Let $\overline{B}^{(l)}$ be an arbitrary block.

3.3.2. For each block $\overline{B}^{(l)}$:

3.3.2.1. Perform a normal singular decomposition (1): $\overline{B}^{(l)} = U\Sigma V^T$;

3.3.2.2. Build a vector (3):

$$\overline{\overline{\sigma}} = \left(\sigma_1^2,..,\sigma_l^2\right)^T \Big/ \left\|\left(\sigma_1^2,...,\sigma_l^2\right)^T\right\|;$$

3.3.2.3. Find $\angle\left(u_1,\overline{\overline{\sigma}}\right)$.

3.3.3. For the DI under analysis determine the parameter $\overline{mod\, a_l}$ of angle $\angle\left(u_1,\overline{\overline{\sigma}}\right)$, which corresponds to the largest number of image blocks, the number of such blocks is $\overline{MBlok}_l$.

If

$$\overline{mod\, a}_l = \angle\left(n^O, e_1\right),$$

where $n^O \in R^l, e_1 \in R^l$,

then

if

$$\overline{MBlok}_l \geq P_1,$$

then

3.3.3.1. The image analyzed is split into nonintersecting blocks of $2l \times 2l$ pixels, while the splitting grid is shifted relative to standard grid by P_3 pixels along the axis OX and P_4 pixels by the axis OУ. Let $\overline{B}^{(2l)}$ be an arbitrary block.

3.3.3.2. For each block $\overline{B}^{(2l)}$ obtained by splitting the following must be done:

3.3.3.2.1. Perform a normal singular decomposition: $\overline{B}^{(2l)} = U\Sigma V^T$;

3.3.3.2.2. Build a vector:

$$\overline{\overline{\sigma}} = \left(\sigma_1^2,...,\sigma_{2l}^2\right)^T \Big/ \left\|\left(\sigma_1^2,...,\sigma_{2l}^2\right)^T\right\|;$$

3.3.3.2.3. Find $\angle\left(u_1,\overline{\overline{\sigma}}\right)$.

3.3.3.3. For image under analysis determine the parameter $\overline{mod\, a}_{2l}$ of an angle $\angle\left(u_1,\overline{\overline{\sigma}}\right)$, which corresponds to the largest number of image blocks, the number of such blocks is $\overline{MBlok}_{2l}$, $\overline{MBlok} = \left|\overline{MBlok}_{2l} - \overline{MBlok}_l\right|$

If

$$\overline{mod\, a}_{2l} = \angle\left(n^O, e_1\right),$$

where $n^O \in R^{2l}, e_1 \in R^{2l}$,

then

if

$$\left(\overline{MBlok}_{2l} \geq P_1\right) \& \left(\overline{MBlok} \leq P_2\right),$$

then

$$S_l = \left|MBlok_l - \overline{MBlok}_l\right|;\ S_{2l} = \left|MBlok_{2l} - \overline{MBlok}_{2l}\right|,$$

if

$$\left(S_l \geq V_1\right) \& \left(S_{2l} \geq V_2\right),$$

(4)

where V_1, V_2 are experimental thresholds,

then

The integrity of the image has been violated;

if

$$\left(S_l < V_1\right) \& \left(S_{2l} < V_2\right),$$

then

The integrity of the image has not been violated;

if

$$\left(S_l \geq V_1\right) \& \left(S_{2l} < V_2\right),$$

(5)

then

The integrity of the image has been violated;

if

$$\left(S_l < V_1\right) \& \left(S_{2l} \geq V_2\right),$$

then

The integrity of the image has not been violated;

otherwise

The integrity of the image has been violated

otherwise

The integrity of the image has been violated

otherwise

The integrity of the image has been violated

otherwise

The integrity of the image has been violated

otherwise

The integrity of the image has been violated

otherwise

The integrity of the image has been violated

otherwise

The integrity of the image has been violated

otherwise

The integrity of the image has been violated

Comment. In the absence of information about the location of the splitting grid during the initial block processing of the digital image, the grid shift repeatedly performed with a small step (for example, one pixel) with a calculation of S_l and S_{2l} for each grid location. The number of shifts in each direction is limited by the block size *l*. If at some step the situation (4) or (5) takes place, then the integrity is violated. The algorithmic implementation of the method is based on the practical results obtained in [13], which was focused on the analysis of 2×2 and 4×4 blocks of digital image, which is the subject to the integrity examination.

It was found in [13] that the changes in the relative quantities of 2×2- and 4×4-blocks of the image matrix, obtained as a result of its standard splitting, for which the condition held:

$$\angle\left(u_1, \overline{\overline{\sigma}}\right) = \angle\left(n^O, e_1\right), \tag{6}$$

after shift of the standard splitting grid of image matrix for original images will differ from those, whose integrity was violated due to the block processing. In addition, quantitative estimates of these differences were found. Thus, for the vast majority of original images, these changes do not exceed 1%, while for the vast majority of images that were affected by block processing, the change in the number of 2×2- and/or 4×4-blocks exceeds (most often, significantly) 1%. Considering this, as well as the results of studies concerning the minimum and maximum values of the relative 2×2-, 4×4-blocks number, for which condition (6) holds while the various perturbations performed under the studied images, the following threshold values and parameter values are proposed for the algorithmic implementation of the developed method: $l = 2$, $P_1 = 6$, $P_2 = 20$, $V_1 = V_2 = 1$, $P_3 = P_4 = 1$.

The implementation of steps 3, 3.3, 3.3.3 and 3.3.3.3 in the algorithm of the developed method is performed by constructing a histogram of values $\angle(u_1, \overline{\overline{\sigma}})$, while the mode of the histogram de-

termines the angle $\angle(u_1, \overline{\overline{\sigma}})$. Its value corresponds to the largest number of blocks of the considered digital image, and the mode of the histogram represents the number of such blocks in this image.

At the first stage of the computational experiment, testing of the algorithmic implementation of the developed method was carried out, taking into account the following.

All changes in the digital image can be formally represented as a collection of perturbations of a complete formal parameters set: singular numbers and singular vectors obtained as a result of normal singular decomposition of the image matrix (matrix blocks), while the important point is that the singular numbers are those formal parameters that do not change upon transition from the spatial domain of the digital image to the frequency domain [17]. Therefore, to ensure the universality of block processing modelling the experiment is carried out in the form of perturbations of the singular numbers and/or singular vectors in blocks.

Block disturbances are often the result of steganographic transform [10 – 12]. Modern steganographic transforms must be resistant to attacks against the embedded message (at least until lossy compression takes place so that the steganographic messages can be stored in the most widely used lossy formats). It can be achieved taking into account the following conditions [19]: the smallest singular numbers are not affected by steganographic transform, which is resilient to perturbations; for the principal possibility of decoding the additional information being transmitted, the total result of the perturbations produced by its embedding must exceed the perturbations, that can affect the block of steganographic message (SM) during the compression process. With the formal representation of steganographic transforms through perturbations of a complete formal parameters set, the latter requirement can lead to a violation of the reliability of the steganographic message perception, as well as to a violation of the initial order of the singular numbers, which, can not only complicate the process of decoding the additional information, but make it impossible [19]. To avoid this, it is sufficient to carry out the steganographic transform in such a way that only the maximum singular numbers of blocks σ_1 (and possibly σ_2) and singular vectors, which correspond them, should be affected by perturbations, required to cover the perturbation of steganographic message [19] (in the latter case, this causes the perturbation of all block singular numbers, since the perturbation of at least one singular vector leads to disturbance of all the others in the process of bringing them into a state of pairwise orthogonality with the perturbed one).

Taking the above into account, in the first stage of the computational experiment, the block image processing during the testing of the developed algorithm was modelled with the help of different perturbations of the two maximal singular numbers (σ_1 and σ_2) and the first left singular vectors ($\mathbf{u}_1$) of 8×8-blocks. The block size was chosen based on the frequency of its use in various transformations of the digital image [7, 12, 17]. The distortion of the image with the n×n-matrix F was estimated using the difference indicator PSNR (peak signal-to-noise ratio):

$$PSNR = 10 lg\left(\frac{255^2}{MSE}\right),$$

where $MSE = \frac{\|\Delta F\|_F^2}{n^2}$, $\|\Delta F\|_F$ is the Frobenius norm of the digital image perturbation matrix ΔF.

The perturbations of the singular numbers and singular vectors were chosen so that the PSNR value was around 37 dB, which in practice is considered acceptable from the point of view of reliability of the perturbed image perception [12]. The perturbations of the vector $\mathbf{u}_1$ were carried out by its multiplying by the rotation matrix for a small angle (2±1)° (the mean value of PSNR = 44 dB), and also by adjusting the vector $\mathbf{u}_1$ with the n-optimal vector of space R^8, used in modern steganographic algorithms, which are resistant to lossy compression [10]. The perturbations of the singular numbers σ_1 and σ_2 in blocks reach the maximum value ±50 (with the maximum perturbation of the singular number PSNR = 35 dB) and were selected for each experiment so that the required value of the PSNR remains practically unchanged (for example, part of a computational ex-

periment in which the block processing of the DI was modelled as perturbations of singular numbers in blocks, led to PSNR = 38 dB, σ_1 and σ_2 were varied within ±25 with step of 3).

In computational experiments conducted in the current work, the following original digital images were used:

- M_1 set: 400 images, size 800×800 pixels, TIF format [20];
- M_2 set: 300 images, size 400×400 pixels, TIF format [6];
- M_3 set: 160 images, size 800×800 pixels, TIF format, taken by non-professional cameras.

For the original digital images with $M_1 \bigcup M_2 \bigcup M_3$ the set of 8600 images was created. These images were affected by the block processing implemented by perturbations of the blocks' singular numbers and/or singular vectors, defined above. After the perturbation, the DI was stored in lossless (TIF) and lossy (JPEG) format.

The algorithm efficiency was estimated by Type I (failure to detect the violation of digital image integrity) and Type II errors (integrity violation detected in the original image). The experimental results for Type I errors are given in table 1. Type II errors are shown in Table 2.

Table 1

Type I errors (%)

Mean PSNR of image violation by block processing (dB) / Format for saving of violated digital image	Due to σ_1 and σ_2			Due to $\mathbf{u}_1$	
	35	38	40	44	38
TIF	1.8	3.2	5.6	1.2	6.6
JPEG (*QF*=75)	2.4	2.4	5.0	2.8	5.5

Table 2

Type II errors (%)

The set of digital images, examined by the developed algorithm		
M_1	M_2	M_3
6.0	8.7	10
The average value for the experiment ($M_1 \bigcup M_2 \bigcup M_3$) – 7.6		

The results of the experiment indicate the high efficiency of the developed algorithm in detecting of the digital image integrity violations, caused by its block processing and the number of Type I errors practically does not depend on format in which the processed digital image stored (with/without losses).

The algorithm developed in the paper is effective for the detection of the DI lossy compression. It is confirmed by the results of the second stage of the computational experiment. The experiment was carried out for digital images with $M_1 \bigcup M_2 \bigcup M_3$. These images were re-stored in JPEG format with various quality factors and then examined using the developed algorithm. The results that reflect the Type I errors are presented in Table 3.

Table 3

Type I errors when detecting the fact of lossy compression of the DI using the developed algorithm (%)

Set of original digital images	Quality factors *QF*, used for the repeated saving an image to Jpeg format			
	85	75	65	50
M_1	4.7	4.7	4.7	5.3
M_2	14	14	11	14
M_3	9	5	3	4
The average value for the experiment	8.2	7.2	6	7.2

For the convenience of comparing the efficiency of the algorithm developed in the work with modern analogues, the values of the detection accuracy of integrity violation [21] (accuracy (ACC)) were calculated according to the obtained data (Fig. 1):

$$ACC = (TP + TN)/(TP + FN + TN + FP), \quad (7)$$

where *TP* (*True Positive*) represents the number of digital images, for which the integrity violation was correctly detected; *TN* (*True Negative*) is the number of correctly detected original images; *FP* (*False Positive*) the number of original images, which were incorrectly detected as images with integrity violation (Type II error); *FN* (*False Negative*) the number of digital images with integrity violations, which were mistakenly recognized as the original ones (Type I error).

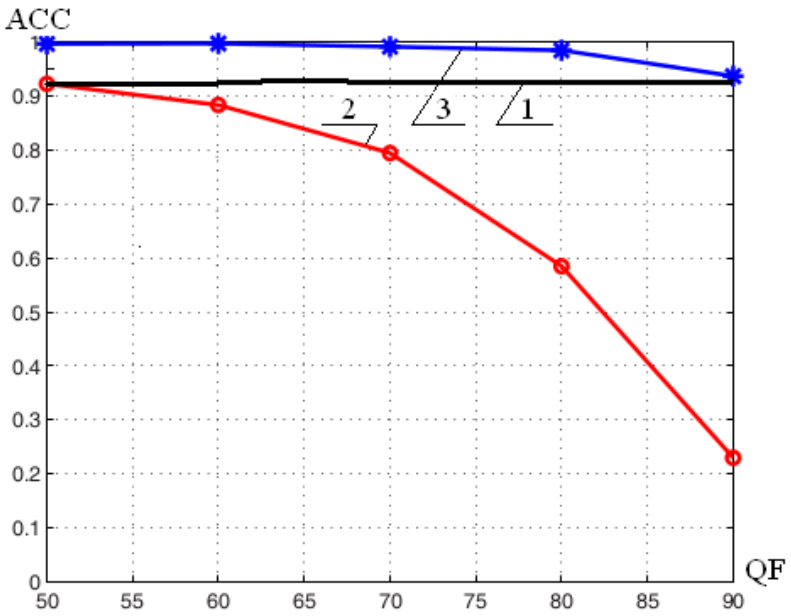

Fig. 1. Results of lossy compression detection in Jpeg image:
1 – developed algorithm; 2 – the algorithm proposed in [14]; 3 – the algorithm proposed in [15]

As can be seen from the obtained results, the developed algorithm provides slightly worse detection accuracy of digital image integrity violation caused by its lossy compression than the best analogues in conditions of $QF = 90$, while the accuracy of detection in the conditions of compression with lower quality coefficients remains high and practically independent from *QF*.

The third stage of the computational experiment shows, that the developed algorithm is effective for detecting the integrity violations of the original digital images in a lossless formats under complex perturbations, if some block processing is present as its part, for example, saving a perturbed image in a lossy format (JPEG), while the other components of the complex perturbations do not necessarily process the digital image by blocks. The following were considered as such complexes in the experiment: the imposition of various noises, different image filtering (in this case, the filtering and noise parameters were chosen so that the PSNR for the perturbation of the image was around 37 dB) and then saved to JPEG with various quality factors. Information about Type I errors obtained from the results of the experiment is given in Table 4. Here, during the experiment, the digital images with $M_1 \bigcup M_2 \bigcup M_3$ were used. Each filter option used masks of size 3×3.

Testing of the developed algorithm as a steganalysis algorithm for detecting the presence of additional information in the digital image was carried out at the fourth stage of the computational experiment for steganographic algorithms which perform block steganographic transforms: S1 (2005) [22], S2 (2006) – Koch and Zhao method, the algorithmic implementation of which uses the coefficients of discrete cosine transform (4,5) and (5,4), with chosen threshold value $P = 25$, as pro-

posed in [12], S3 (2012) [10], S4 (2013) [23], S5 (2013) [24], S6 (2016) [25]. Steganographic algorithms were intentionally chosen so that these transformations were carried out in various domains of the image container: frequency (S2), domains of singular and spectral matrices decompositions of container blocks (S1, S3, S4), spatial domain (S5, S6). During the computational experiment, the steganographic messages were formed by each of the listed steganographic algorithms on the basis of 860 image containers from the set $M_1 \bigcup M_2 \bigcup M_3$, while steganographic messages were saved in two formats, which are lossless (TIF), lossy (JPEG). The experimental results are shown in Table 5.

It should be noted that although the embedding of an additional information in the S4 method the alignment of the vector $\mathbf{u}_1$ with the *n*-optimal vector takes place, the number of Type I errors for the developed algorithm when working with steganographic messages generated by S4, significantly less (Table 5) than when working with the digital images, the integrity of which were violated by the similar perturbation $\mathbf{u}_1$ (PSNR = 38 dB) (Table 1).

This happens due to the fact, that when the additional information is embedded in S4 method, all the singular vectors of the current block are perturbed (in the process of bringing them to a pairwise orthogonal state).

Table 4

Type I errors of developed algorithm under various attack complexes, which involve the block processing (%)

QF for saving the digital image to JPEG after the perturbation	Type of perturbation			
	Noise applying		Filtering	
	Gaussian (*D*=0.0001)	Multiplicative (*D*=0.001)	Increases sharpening (*k*=0.3)	Median
	PSNR=40 *dB*	*PSNR*=36 *dB*	*PSNR*=36 *dB*	*PSNR*=44 *dB*
65	0.9	0.2	9	13.2
70	3.7	0.5	10	12
75	6.9	2	14	14
80	8.9	2	15	14

Table 5

Type I errors of detecting the additional information embedding in the digital image by the developed algorithm (%)

Steganographic algorithm / Format of SM saving	S1 (2005)	S2 (2006)	S3 (2012)	S4 (2013)	S5 (2013)	S6 (2016)
TIF	4.1	1.1	1.6	3.3	1.7	1.6
JPEG (*QF*=75)	3.3	1.3	2.2	2.7	2.4	2.5

Since, as noted above, the developed algorithm is effective in detecting integrity violations as a result of complex attacks, if block processing is present in the complex, it is natural to expect that the proposed algorithm will be effective in detecting the additional information embedded into the container image in a lossy format by one of the most common and often used steganographic methods – the least significant bit modification method (LSB method). The fifth stage of the computational experiment was devoted to evaluating the effectiveness of the developed algorithm under these conditions, during which the digital images with $M_1 \bigcup M_2 \bigcup M_3$ were initially re-saved to JPEG with the most widely used quality factors $QF \in \{65, 75, 85\}$, and then they were used as containers for embedding the additional information by LSB-based methods with different values of the hidden (steganographic) communication channel capacity (HCC). The results of steganalysis using the developed algorithm are presented in Table 6.

The results of comparison the developed algorithm effectiveness with modern steganalysis algorithms, aimed at detecting of LSB embeddings, using ACC parameter (7), are presented in Table

7, where the following notation is used: SS1 (2006) [26], SS2 (2006) [27], SS3 (2008) [28], SS4 (2009) [29], SS5 (2015) [30], SS6 (2016) [31], SA – the developed algorithm.

The obtained results show, that the effectiveness of the developed algorithm does not practically depend on the hidden channel capacity. In addition, it remains effective under conditions for which most analogues are not designed: with a capacity of a hidden communication channel less than 0.05 bit/pixel. As follows from the above results, the SA made it possible to increase the efficiency of the additional information detection, which was embedded by LSB-method with the hidden channel capacity value of 0.01 bit/pixel by 65% compared to the best analogue (S1 (2006)). For other values of the hidden channel capacity, the ACC value for the developed algorithm is compared with the ACC values of the considered analogues (Table 7).

Table 6

Type I errors of developed algorithm in case of steganalysis of messages, generated by LSB-method (%)

Set of digital images (TIF)	QF, used for saving of image in JPEG	Capacity of the hidden communication channel, created with LSB-method (bit/pixel)			
		1	0.5	0.1	0.01
M_1	65	2	4	4.7	4.7
	75	3	6.3	4.7	4.7
	85	2	4	4.7	4.7
M_2	65	3.2	4.3	5.2	5.7
	75	4.3	5.2	4.7	5.7
	85	5.2	6.3	5.7	6.3
M_3	65	3.1	3.1	3.1	3.7
	75	6.2	5.6	5.6	5.6
	85	6.8	6.2	6.2	6.2
Average value (2580 digital images for each value of the hidden communication channel capacity)		4.1	5	5	5.1

Table 7

Comparison of the effectiveness of the developed algorithm and modern steganalysis algorithms for LSB embeddings detection, which evaluated by the ACC

HCC, (bit/pixel)	SS1 (2006)	SS2 (2006)	SS3 (2008)	SS4 (2009)	SS5 (2015)	SS6 (2016)	**SA (2019)**
0.1	0.9846	0.7727	0.9943	0.9937	0,988	0.970	**0.94**
0.05	0.9769	0.6432	0.9283	0.9319	0,968	0.941	**0.94**
0.01	0.5692	0.5094	-	-	-	-	**0.94**

Comment. Since the developed method for the detection of image integrity violations caused by the perturbation, which involved the block processing, performs the expertise of the digital image per block, the computational complexity of its algorithmic implementation will be determined by the number of image matrix blocks, i.e., it for the digital image with $n \times n$-matrix it will be $\underline{O}\left(n^2\right)$ operations.

Conclusions

In this work, the method developed and its algorithmic implementation performed. It provides effective detection of the image integrity violations, which occur due to the block processing regardless of its specific type.

In the course of a computational experiment carried out to evaluate the effectiveness of the proposed algorithm, the following were considered as block processing: perturbations of the singular numbers and/or singular vectors of blocks; lossy image compression; steganographic transformation which perform the embedding of an additional information block-by-block (in spatial, frequency, spectral, singular decomposition domains); set of complex actions, which include lossy image compression; steganographic transformation of a container image saved in a lossy format using

the LSB-method. Under the conditions of each of the listed actions on the digital image, the developed algorithm demonstrated the high efficiency, which was estimated using Type I and Type II errors, as well as using the ACC parameter – accuracy of the integrity violation detection.

Comparison of the SA effectiveness with its analogues was carried out under the conditions of specific perturbations for various algorithms since the information about direct analogues for the developed method has not been found in open sources. In all cases considered, the efficiency of the developed algorithm is comparable to the best of the modern analogues. In addition, if the SA used as steganalysis algorithm for detecting the LSB-embeddings in the container image, saved with losses, it remains effective in conditions of small HCC when most of the analogue algorithms are inapplicable. Under the conditions of HCC = 0.01 bit/pixel, the developed algorithm made it possible to increase the efficiency of steganalysis by 65 % (compared to the best of the considered analogues).

The proposed algorithmic implementation of the developed method has polynomial complexity of degree 2, which makes it possible to use it for examining the integrity of video sequences.

Список літератури:

1. Ленков С.В., Перегудов Д.А., Хорошко В.А. Методы и средства защиты информации : в 2 т. Киев : Арий, 2008. 344 с.
2. Uliyan D.M., Jalab H.A., Abdul Wahab A.W., Sadeghi S. Image region duplication forgery detection based on angular radial partitioning and Harris key-points // Symmetry. 2016. Vol. 8, Issue 7. 62 p.
3. Kobozeva A.A., Bobok I.I., Garbuz A.I. General principles of integrity checking of digital images and application for steganalysis // Transport and Telecommunication. 2016. Vol. 17, Issue 2. P. 128-137.
4. Karampidis K., Kavallieratou E., Papadourakis G. A review of image steganalysis techniques for digital forensics // Journal of Information Security and Applications. 2018. No. 40. P. 217 – 235.
5. Lerch-Hostalot D., Megias D. Unsupervised steganalysis based on artificial training sets // Engineering Applications of Artificial Intelligence. 2016. Vol. 50, Issue C. P. 45 – 59.
6. Hsu Y., Chang S. Detecting image splicing using geometry invariants and camera characteristics consistency // Proceedings of 2006 IEEE International Conference on Multimedia and Expo (ICME'06), Toronto, Canada. 2006. P. 549 – 552.
7. Зорило В.В., Кобозева А.А. Метод выявления результатов размытия цифрового изображения // Сучасна спеціальна техніка. 2010. № 3(22). С. 52 – 63.
8. Зоріло В.В., Кіосєва О.І., Зоріло І.В. Модифікація алгоритму виявлення штучного підвищення різкості цифрового зображення // Інформатика та математичні методи в моделюванні. 2018. Т. 8, № 2. С. 156 – 163.
9. Лебедева Е.Ю., Кобозева А.А. Основы метода выявления клонированных участков изображения, подвергнутых коррекции яр кости // Сучасна спеціальна техніка. 2013. № 3. С. 13 – 20.
10. Мельник М.А. Стеганоалгоритм, устойчивый к сжатию // Інформаційна безпека. 2012. № 2(8). С. 99 – 106.
11. Кобозева А.А., Костырка О.В., Лебедева Е.Ю. Стеганопреобразование пространственной области изображения-контейнера, устойчивое к атакам против встроенного сообщения // Problemele Energeticii Regionale. 2014. № 1(24). С. 1 – 12.
12. Конахович Г.Ф., Пузыренко А.Ю. Компьютерная стеганография: теория и практика. Киев : МК-Пресс, 2006. 288 с.
13. Бобок І.І. Дослідження змін властивостей параметрів блоків цифрового зображення при блоковій обробці як основа методу виявлення порушення його цілісності // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. 2018. № 2(36). С. 56 – 67.
14. Tjoa S., Lin W., Zhao H., Liu K. Block size forensic analysis in digital images // Proceedings of 2007 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP'07), Honolulu, USA. 2007. P. I-633-I-636.
15. Luo W., Huang J., Qiu G. (2009) A Novel Method for Block Size Forensics Based on Morphological Operations // Kim HJ., Katzenbeisser S., Ho A.T.S. (eds) Digital Watermarking. IWDW 2008. Lecture Notes in Computer Science, vol 5450. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-04438-0_20
16. Гонсалес Р., Вудс Р. Цифровая обработка изображений. Москва : Техносфера, 2006. 1070 с.
17. Кобозева А.А., Хорошко В.А. Анализ информационной безопасности. Киев : ГУИКТ, 2009. 251 с.
18. Бобок И.И. Теоретическое развитие общего подхода к проблеме выявления нарушений целостности цифровых контентов, основанного на анализе полного набора формальных параметров // Інформатика та математичні методи в моделюванні. 2017. Т. 7, № 3. С. 170 – 177.
19. Кобозева А.А., Мельник М.А. Формальные условия обеспечения устойчивости стеганометода к сжатию // Сучасна спеціальна техніка. 2012. № 4(31). С. 60–69.

20. 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, Switzerland. 2010. Vol. 2. P. 1585 – 1591.

21. Geetha S., Sindhu S., Kamaraj N. Close color pair signature ensemble adaptive threshold based steganalysis for LSB embedding in digital images // Transactions on Data Privacy. 2008. Vol. 1, Issue 3. P. 140–161.

22. Bergman C., Davidson J. Unitary embedding for data hiding with the SVD // Proc. SPIE 5681, Security, Steganography, and Watermarking of Multimedia Contents VII, (21 March 2005); https://doi.org/10.1117/12.587796

23. Кобозева А.А., Мельник М.А. Стеганографический алгоритм, основанный на sign-нечувствительности сингулярных векторов матрицы изображения // Системи обробки інформації. 2013. Вип. 3(110), Т. 2. С. 90 – 94.

24. Рудницький В.М., Костирка О.В. Стійке стеганоперетворення в просторовій області зображення-контейнера // Інформатика та математичні методи в моделюванні. 2013. Т. 3, № 4. С. 353 – 360.

25. Костирка О.В. Модифікація стійкого до збурних дій стеганоперетворення просторової області зображення-контейнера // Інформатика та математичні методи в моделюванні. 2016. Т. 6, № 1. С. 85 – 93.

26. Chen X., Sun F., Sun W. Detect LSB Steganography with Bit Plane Randomness Tests // Proceedings of 2006 6th World Congress on Intelligent Control and Automation, Dalian, China. 2006. P. 10306 – 10309.

27. Zou D., Shi Y.Q., Su W., Xuan G. Steganalysis based on Markov model of thresholded prediction-error image // Proceedings of 2006 IEEE International Conference on Multimedia and Expo, Toronto, Canada. 2006. P. 1365 – 1368.

28. Chen C., Shi Y.Q. JPEG image steganalysis utilizing both intrablock and interblock correlations // Proceedings of 2008 IEEE International Symposium on Circuits and Systems. Seattle, USA. 2008. P. 3029 – 3032.

29. Huang F., Huang J. Calibration based universal JPEG steganalysis // Science in China Series F: Information Sciences. 2009. Vol. 52, Issue 2. P. 260 – 268.

30. Xue B., Li X., Li B., Guo Z. Steganalysis of LSB replacement for multivariate Gaussian covers // Proceedings of 2015 IEEE China Summit and International Conference on Signal and Information Processing (ChinaSIP), Chengdu, China. 2015. P. 836 – 840.

31. Lin Q., Liu J., Guo Z. Local ternary pattern based on path integral for steganalysis // Proceedings of 2016 IEEE International Conference on Image Processing (ICIP), Phoenix, USA. 2016. P. 2737 – 2741.

Odesa National Polytechnic University *Received 20.11.2019*