Transport and Telecommunication, 2016, volume 17, no. 2, 128–137
Transport and Telecommunication Institute, Lomonosova 1, Riga, LV-1019, Latvia
DOI 10.1515/ttj-2016-0012

GENERAL PRINCIPLES OF INTEGRITY CHECKING OF DIGITAL IMAGES AND APPLICATION FOR STEGANALYSIS

Alla A. Kobozeva, Ivan I. Bobok, Artem I. Garbuz

Odessa National Polytechnic University
Odessa, Ukraine, 1 Shevchenko Avenue,
Ph.: +380953901846, onu_metal@ukr.net

The new common approach for integrity checking of digital images is developed. The new features of formal parameters defining image are revealed, theoretically grounded and practically tested. The characteristics of the mutual arrangement of left and right singular vectors corresponding to the largest singular value of the image's matrix (block of matrix) and the vector composed of singular numbers is obtained. Formal parameters are obtained using normal singular decomposition of matrix (block of matrix) which is uniquely determined. It is shown that for most blocks of original image (no matter lossy or lossless) the angle between the left (right) mentioned singular vector and vector composed of singular numbers is defined by the angle between the n-optimal vector and the vector of standard basis of the range corresponding dimension. It is shown that the determined feature brakes for the mentioned formal parameters in a non-original image. This shows the integrity violation of the image, i.e. the existence of the additional information embedded using steganography algorithms. So this can be used as a basis for development of new universal steganography methods and algorithms, and one example of the realization is proposed. The efficiency of the proposed algorithm won't depend on the details of steganography method used for embedding. All the obtained results can be easily adapted for the digital video and audio analysis.

Keywords: singular number, singular vector, n-optimal vector, normal singular decomposition, steganography analysis, steganalytical method

1. Introduction

The integrity of information is one of the main criteria of safety. Today data objects are usually presented in a digital format (images, audio and video). If you use such objects in the media, medicine, science, judicial investigations, etc. you must be sure in the absence of the unauthorized changes. This makes the task of checking their integrity extremely important.

The modern level of IT has led to wide circulation of different types of digital content falsification including digital images. The existing methods for detection of images integrity violation are not satisfactory (Rey and Dugelay, 2002; Amerini, et al., 2013; Farid, 2009; Gul and Kurugollu, 2010).

A special case of the digital content integrity violation is embedding the additional information using steganography algorithms for future sending or storage. Recently there was intensification of scientific and research activities in the steganography area. The reason is that in many countries of the world there is the restriction or even denial of use of cryptographic tools for information protection. Publication of the obtained results in the field of steganography in press with open access provided increasing possibilities of using results of researches by various anti-state and terrorist structures. So it is extremely important to improve the steganalysis efficiency to detect the presence of hidden information at the present moment. However the existing steganalytical methods, which are positioned as universal, focused on a limited set of steganography algorithms (Bobok and Kobozeva, 2011; Natarajan and Anitha, 2012). Such methods essentially can't guarantee the detection of the new steganography algorithms. In addition the effectiveness of many existing steganalytical methods critically depends on the format of digital image container as well as the format in which the image is stored after the embedding of hidden information. An important and unresolved task of steganalysis is the detection of hidden information with low embedding rate (Bobok and Kobozeva, 2011). All this indicates inconsistency of the existing approaches used in the development of universal steganalytical methods. The integrity violation of the digital image container is a prerequisite of steganography transformation and the detection of these violations can be used as the steganalysis basis. Such approach to steganalysis makes it universal and independent of the specific type of steganography algorithms and digital image container format.

2. Materials and Methods

The new approach for solving problems of the detection of various violations of the integrity of digital content is presented. At this moment the effectiveness of proposed approach is confirmed by series

of numerical experiments (Kobozeva and Khoroshko, 2009). Here every information system is represented as a finite set of two-dimensional matrixes. The change of the system's state is formally described as a set of the perturbation of matrix parameters full set. Set of singular values and singular vectors of the matrix (matrixes) used as a set of the parameters. The formal parameters satisfy the certain requirements (Kobozeva and Khoroshko, 2009). The universality of the proposed approach makes it perspective for further use in the detection of various integrity violations of digital images, i.e. for the steganalysis organization.

The basic idea of the proposed approach (Kobozeva and Khoroshko, 2009) is as follows. All images are stored in digital formats – lossy or lossless. The quantity of such formats is finite. The saving process and formal presentation of digital images occurs according to certain algorithms, results in specific characteristic features of the formal parameters (singular values and vectors of matrixes). Detection of these patterns gives possibility to state the originality of digital image; but their violations is the result of the integrity violations.

The aim of this research is theoretical basis development of the new common approach for organizing the detection process of integrity violation of digital images. The efficiency of the developed approach should not depend on the specific type and method of implementation of these forgeries and image format.

3. Results and Discussion

We will consider one matrix $\mathbf{F}$ as formal representation of digital image (Kobozeva and Khoroshko, 2009). We will split matrix $\mathbf{F}$ into non-crossing $l \times l$ -blocks $\mathbf{B}$.

Let's

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

– singular value decomposition of a matrix B, which is uniquely determined in accordance with (Kobozeva and Khoroshko, 2009). Here $\mathbf{U},\mathbf{V}$ – orthogonal $l \times l$ -matrixes, where $\mathbf{u}_1,\ldots,\mathbf{u}_l$ (columns of $\mathbf{U}$), $\mathbf{v}_1,\ldots,\mathbf{v}_l$ (columns of $\mathbf{V}$) – left-singular vectors and right-singular vectors of $\mathbf{B}$ correspondingly; $\boldsymbol{\Sigma} = \mathrm{diag}(\sigma_1,\ldots,\sigma_l)$, where $\sigma_1 \geq \ldots \geq \sigma_l \geq 0$ – singular values of $\mathbf{B}$.

Matrixes $\mathbf{B}\mathbf{B}^{\mathbf{T}}$ and $\mathbf{B}^{\mathbf{T}}\mathbf{B}$ are indecomposable for vast majority of original image's blocks (Kobozeva, 2014). The results of computational experiments involved one thousand 1000×1000 digital images (with different container format, brightness, contrast, content generated by professional and non-professional video cameras). It was defined that only 0.07% of the total number of image's blocks may be decomposable for 8×8-blocks in principle (Kobozeva, 2014). And this number is slightly increasing for 4×4-blocks.

For symmetric nonnegative matrix $\mathbf{B}\mathbf{B}^{\mathbf{T}}$ in accordance with (1):

$$\mathbf{B}\mathbf{B}^{\mathrm{T}} = \left(\mathbf{U}\boldsymbol{\Sigma}V^{\mathrm{T}}\right)\left(\mathbf{U}\boldsymbol{\Sigma}V^{\mathrm{T}}\right)^{\mathrm{T}} = \mathbf{U}\boldsymbol{\Sigma}^2\mathbf{U}^{\mathrm{T}},$$

that is normal spectral decomposition of matrix $\mathbf{B}\mathbf{B}^{\mathbf{T}}$ (Kobozeva and Khoroshko, 2009) which is uniquely determined. Here, Eigen values of matrix $\mathbf{B}\mathbf{B}^{\mathbf{T}}$ are equal to the square of the singular values of $\mathbf{B}$, and left-singular vectors of $\mathbf{B}$ are orthonormal lexicographically positive eigenvectors vectors of $\mathbf{B}\mathbf{B}^{\mathbf{T}}$. Similarly is for right-singular vectors of $\mathbf{B}$ and matrix $\mathbf{B}^{\mathbf{T}}\mathbf{B}$. Using Frobenius theorem in the presence of non-decomposition of $l \times l$ -matrixes $\mathbf{B}\mathbf{B}^{\mathbf{T}}$ and $\mathbf{B}^{\mathbf{T}}\mathbf{B}$ shown that singular vectors $\mathbf{u}_1$ and $\mathbf{v}_1$ of original image, and vector $\boldsymbol{\sigma} = \sigma / \|\sigma\|$ ($\boldsymbol{\sigma} = (\sigma_1,\ldots,\sigma_l)^{\mathrm{T}} \in \mathbf{R}^l$) are stable, sign-stable (Kobozeva and Khoroshko, 2009), non-negative, and geometrical located in first coordinate orthant of the $\mathbf{R}^l$. These properties exist regardless of the digital image format. This suggests the existence of the certain dependence between $\mathbf{u}_1$, $\mathbf{v}_1$ and $\boldsymbol{\sigma}$ in blocks of original image.

The angle between vectors $\mathbf{u}_1$ and $\boldsymbol{\sigma}$ (identify as $\angle(\mathbf{u}_1,\boldsymbol{\sigma})$), $\mathbf{v}_1$ and $\boldsymbol{\sigma}$ (identify as $\angle(\mathbf{v}_1,\boldsymbol{\sigma})$) of majority of original image's blocks equal to angle between n-optimal vector $\mathbf{n}^{\mathbf{O}}$ (where

$\mathbf{n}^{\mathbf{O}} = \left(1/\sqrt{l}, 1/\sqrt{l}, \ldots, 1/\sqrt{l}\right)^{\mathrm{T}} \in \mathbf{R}^{l}$) and vector of standard basis $\mathbf{e}_1 = (1,0,0,\ldots,0) \in \mathbf{R}^{l}$ (identify as $\angle\left(\mathbf{n}^{\mathbf{O}}, \mathbf{e}_1\right)$):

$$\angle(\mathbf{u}_1, \boldsymbol{\sigma}) \approx \angle(\mathbf{v}_1, \boldsymbol{\sigma}) \approx \angle\left(\mathbf{n}^{\mathbf{O}}, \mathbf{e}_1\right). \quad (2)$$

Computational experiments (which involved 500 digital images in various formats – lossy and lossless) were conducted to confirm (2).

The results of experiments are presented in histograms Γ_U (Γ_V) (*bin* = 1°) of angle values between vectors $\mathbf{u}_1$ and $\boldsymbol{\sigma}$ ($\mathbf{v}_1$ and $\boldsymbol{\sigma}$) of $l \times l$-blocks obtained as result of standard matrix decomposition for various l values.

The experimental results are in full accordance with the theoretical conclusions: global maximum of Γ_U-, Γ_V-histograms for most blocks is achieved for $\angle\left(\mathbf{n}^{\mathbf{O}}, \mathbf{e}_1\right)$. The most appropriate in terms of satisfying (2) is to use 4×4-blocks of image's matrix for analysis of digital images (Fig. 1, a). Here, histograms global maximum is achieved for $\angle\left(\mathbf{n}^{\mathbf{O}}, \mathbf{e}_1\right) = 60^{\circ}$.

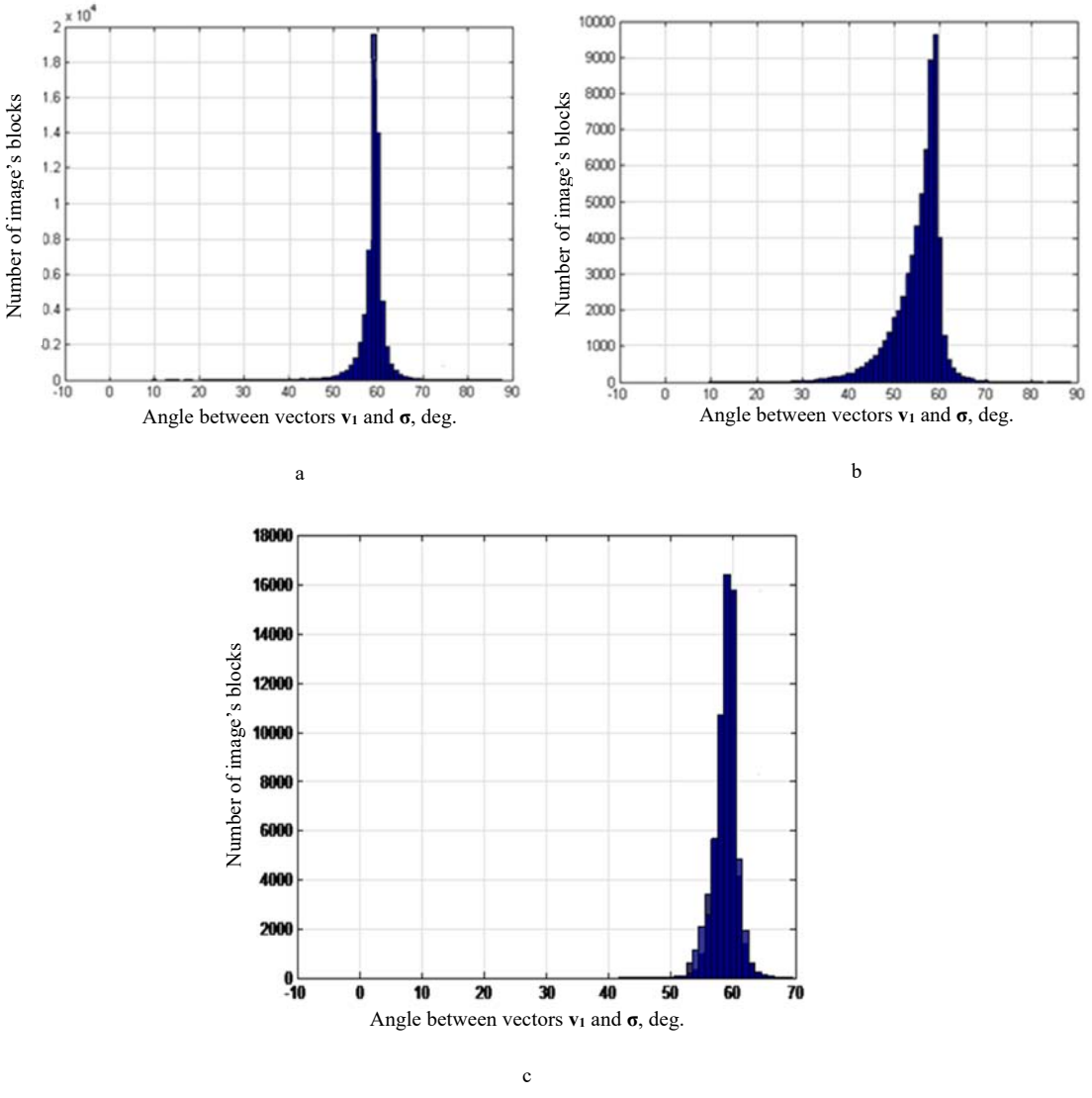


Figure 1. Γ_V–histograms: a — original image; b — noisy image (Gaussian noise, Expected value = 0, D = 0.001); c — stegano image generated by LSB (Bobok and Kobozeva, 2011) (embedding rate 0.75 bpp)

The established ratio (2) is specific for original digital images. For majority of blocks the ratio (2) will be violated in the conditions of the perturbation actions on images. This was confirmed by the results of computational experiments with such perturbation actions: the Gaussian additive, Multiplicative with different characteristics, "Salt-Pepper", Poisson noise.

However, taking into account only one parameter – argument of a global maximum of Γ_U-, Γ_V-histograms for the digital image it is possible situation when to separate the original image from non-original will be impossible because analyzed parameters can be the same (Fig. 2). It is necessary to use additional characteristics of digital images for analysis. Taking into account all aforesaid it is clear that ratio (2) violation after changing the original image will reduce the number of blocks in which (2) will take place. Formally this will be expressed in reducing of the global maximum of Γ_U-, Γ_V-histograms for perturbed digital image as compared with original one. The horizontal "enlargement" of the histogram will be as consequence (Fig. 1, b and 1, c).

The Γ_U-, Γ_V-histograms of original and perturbed digital images were directly considered and compared for practical confirmation of the received results. Γ_U (Γ_V) global maximum value of original image often about 1.5-2 times higher than the corresponding perturbed image. Also the histogram of perturbed image is "wider" than the original one (Fig. 1).

Thus, the relation of the size of a global maximum of Γ_U (Γ_V) to the size of dispersion of values can act as the padding quantitative parameter for separation of the original digital image from the non-original one.

The proposed approach will make it possible to distinguish between the original and non-original image and in addition in some cases will allow making conclusions about the nature of perturbation action. Already now the different nature of value distribution of sizes of the analyzed angles for the original digital image and the noisy one is apparent (Fig. 3). The curve constructed in Fig. 3 is the curve of Gaussian distribution corresponding to parameters of the corresponding histograms. It was obtained using Matlab function `histfit`. The effect of Multiplicative noise imposing makes the distribution of angles closer to Gaussian distribution unlike the original digital image or image with Gaussian noise added.

The obtained characteristics allow distinguishing the original digital image from and perturbed one even if global maximum of Γ_U-, Γ_V-histograms are equal.

All aforesaid can be used for development of identification methods of digital images integrity violation. As the main steps of one of such methods first presented in this paper – method Kobozeva-Bobok-Garbuz (KBG) – may be the following ones.

Step 1. To build the Γ_U, Γ_V for the analyzed digital image.

Step 2. To define for the Γ_U, Γ_V the arguments of the global maximums A_U, A_V and the global maximums M_U, M_V accordingly.

Step 3. To calculate the quantities of the S_U, S_V blocks for analyzed digital image using Γ_U, Γ_V having $\angle(\mathbf{u_1}, \boldsymbol{\sigma}) \in [60^\circ - T, 60^\circ + T]$, $\angle(\mathbf{v_1}, \boldsymbol{\sigma}) \in [60^\circ - T, 60^\circ + T]$, where T – parameter of the method.

Step 4. Checking.

If A_U, $A_V \notin \{59, 60, 61\}$, then the integrity of analyzed digital image is violated.

If A_U, $A_V \in \{59, 60, 61\}$ and $(S_U/M_U > P_U) \vee (S_V/M_V > P_V)$, where P_U, P_V – the threshold values, that are defined experimentally, then the integrity of analyzed digital image is violated.

If A_U, $A_V \in \{59, 60, 61\}$ and $(S_U/M_U \le P_U) \vee (S_V/M_V \le P_V)$, then the integrity of analyzed digital image is not violated.

The further results are given for the method implementation with such parameters values: $T = 15°$, $P_U = P_V = 3.2$. Let assume for convenience: $k_U = S_U/M_U$, $k_V = S_V/M_V$.

Let us illustrate the work of the proposed method for two digital images, that are stored in different formats (in terms of loses): Lena (lossless) (Fig. 4, a), Owlet (lossy) (Fig. 4, b). These images are taken from the digital images databases, that are traditional for various algorithms testing – The USC-SIPI Image Database, and The NRCS Photo Gallery.

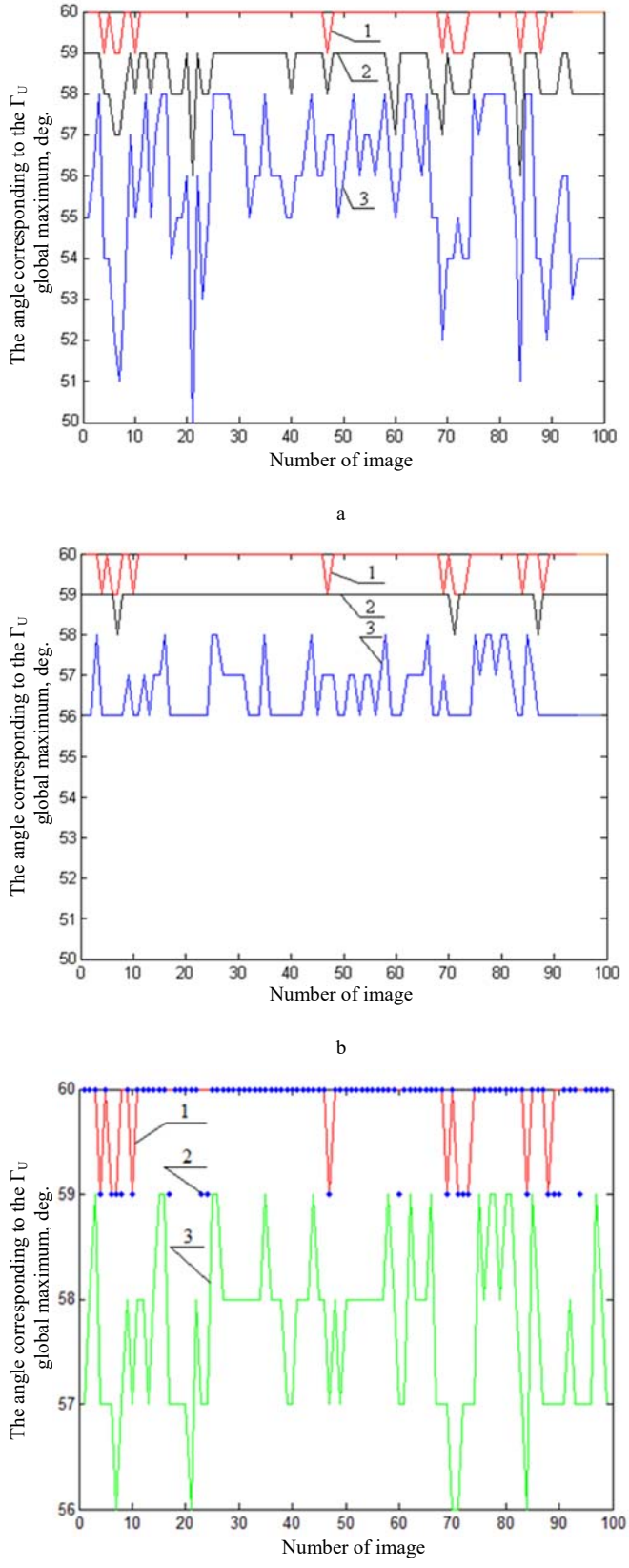
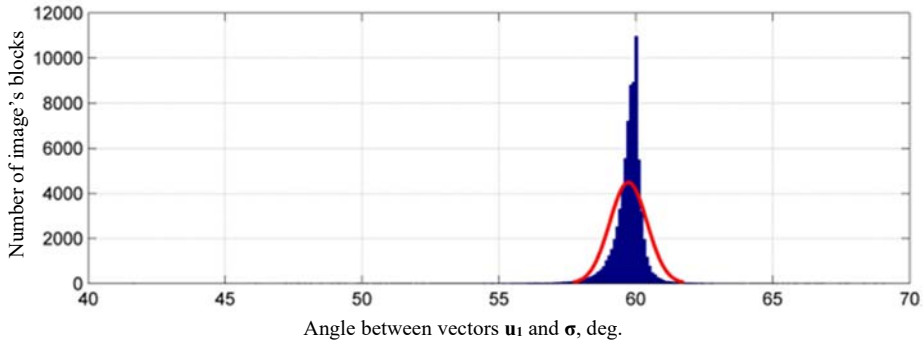
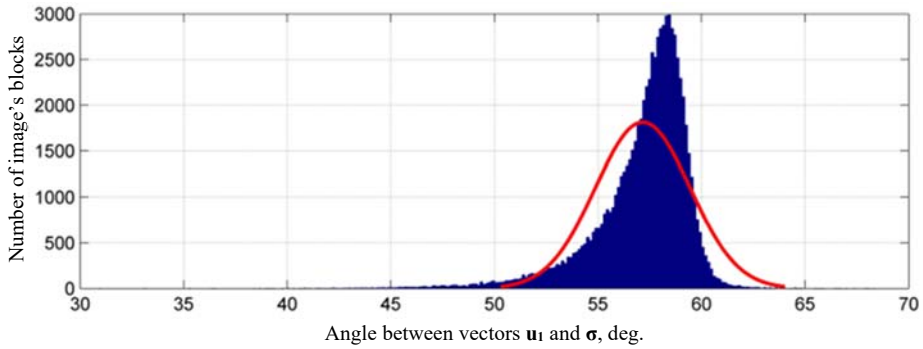


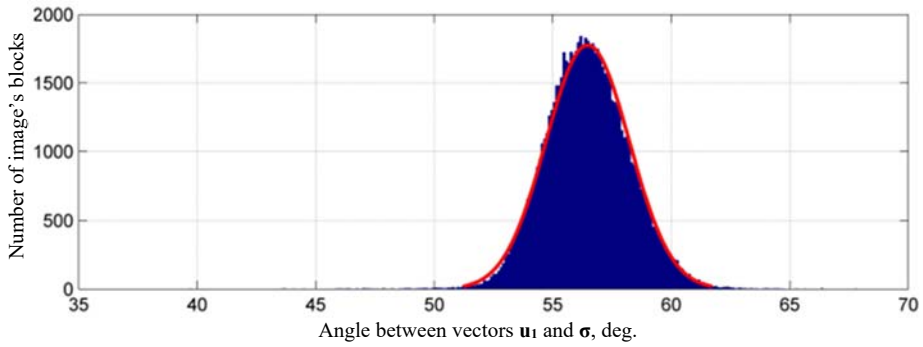
Figure 2. The angle corresponding to the Γ_U global maximum versus number of digital image: a — 1 – original image; 2 – noisy image (Gaussian noise, Expected value = 0, D = 0.001); 3 – noisy image (Gaussian noise, Expected value = 0, D = 0.01); b — 1 – original image; 2 – noisy image (Multiplicative noise, D = 0.001); 3 – noisy image (Multiplicative noise, D = 0.01); c — 1 – original image; 2 – noisy image ("Salt-Pepper", D = 0.05); 3 – noisy image (Poisson noise)



a



b



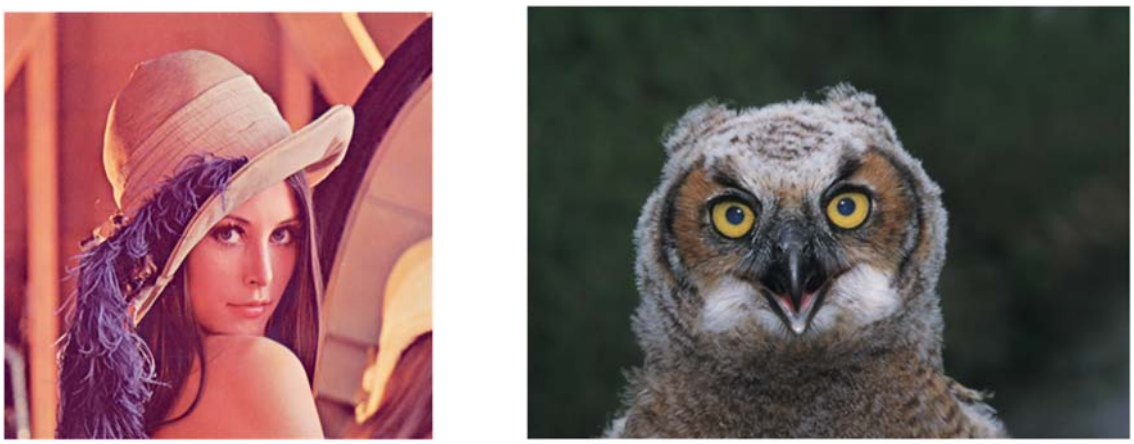
c

Figure 3. Γ_U–histograms (bin = 0.5°): a — original image; b — noisy image (Gaussian noise, Expected value = 0, D = 0.001); c — noisy image (Multiplicative noise, D = 0.001)

As it is seen from the results shown in Table 1 and 2, the considering of proposed quantitative variables allows separating the original digital image from the one with integrity violated because of disturbances, that are differ from steganography transformation. Also it is achieved by means of imbedding the suppressed information using various steganography algorithms (in Table 2 the various modifications of the LSB-method under various hidden communication channel throughput (HT) are shown). Even where $A_U = A_V = 60°$ (for example, the case of superimposition of the "Salt-Pepper" noise on tested digital images) the directed qualitative comparison of histograms Γ_U, Γ_V for original and perturbed digital image taking into account the written above allows their classification (Fig. 5), that are confirmed by additional qualitative parameters k_U and k_V for which: $k_U \geq P_U$, $k_V \geq P_V$.

As it seen of results shown in Table 1 and 2, the effectiveness of KBG for separation of original digital image from the image with violated integrity does not depends on source image format

(lossy/lossless), specificity of used steganography algorithms, specialties and parameters of superimposed noises: all images instances with violated integrity were detected by KBG method, the original images are also classified correctly.



a b

Figure 4. Test digital images: a – Lenna; b – Owlet

Table 1. The results of test digital images analysis in integrity violation conditions using perturbation actions, that differ from steganography transformation (the results are presented as: A_U/k_U (A_V/k_V))

Images	Γ_U									Γ_V							
	Original image	Perturbation action								Original image	Perturbation action						
		Gaussian		Speckle		Salt & Pepper		Poisson			Gaussian		Speckle		Salt & Pepper		Poisson
		$D=10^{-3}$	$D=10^{-4}$	$D=10^{-2}$	$D=10^{-3}$	d=0.02	d=0.05				$D=10^{-3}$	$D=10^{-4}$	$D=10^{-2}$	$D=10^{-3}$	d=0.02	d=0.05	
Lenna	60 / 3.13	58 / 5.91	59 / 4.20	57 / 6.16	59 / 5.05	60 / 4.67	59 / 6.30	57 / 6.39		60 / 3.07	58 / 5.65	59 / 4.32	57 / 5.98	59 / 5.08	60 / 4.58	60 / 6.17	57 / 6.45
Owlet	60 / 3.01	55 / 10.6	59 / 4.46	57 / 5.56	59 / 3.24	60 / 3.71	60 / 5.02	57 / 7.97		60 / 3.04	56 / 9.94	59 / 4.34	57 / 5.67	60 / 3.29	60 / 3.79	60 / 5.11	57 / 7.89

One of the most widely used steganography methods for now is the LSB, but the problem of embedding detection using LSB-method is not completely solved till present time. Accounting this, to get comparative evaluation of KBG work in the context of steganography analysis, the modern steganalytical methods were chosen: Ker's, Liu's, HGE, NDH COM, RLH COM, Fused feature, Joint feature set (Xia, et al., 2011; Li, et al., 2011). These methods can detect the LSB-method and they are reviewed in modern public media as the most effective ones. The results of computational experiment, where 500 digital images of various formats (lossy/lossless) were used, are presented in Table 3. There is the integral parameter ρ (Fridrich, 2004) were used as the qualitative one, that characterizes the efficiency of steganalytical methods. As it seen of the Table 3, the KBG method is comparable to the best of reviewed analogues in efficiency in the context of detection of additional information embedding. At that, the proposed method has wider application area by detection of digital image integrity violation, that are different from steganography transformation results.

Table 2. The results of test digital images analysis in integrity violation conditions by means of steganography transformation using various steganography algorithms (the results are presented as: A_U/k_U (A_V/k_V))

Images	Γ_U										Γ_V									
	Steganography algorithms and its parameters										Steganography algorithms and its parameters									
	LSB-matching			LSB-replacement			Kutter, et al., 1998		Koch and Zhao, 1995		LSB-matching			LSB-replacement			Kutter, et al., 1998		Koch and Zhao, 1995	
	Embedding rate, bpp			Embedding rate, bpp							Embedding rate, bpp			Embedding rate, bpp						
	0.5	0.75	1	0.5	0.75	1	v=0.01	v=0.05	p=40	p=35	0.5	0.75	1	0.5	0.75	1	v=0.01	v=0.05	p=40	p=35
Lenna	60 / 3.77	60 / 3.79	60 / 3.84	60 / 3.68	59 / 3.69	59 / 3.74	58 / 4.91	57 / 5.90	58 / 5.10	58 / 5.01	60 / 3.81	59 / 3.84	59 / 3.90	60 / 3.57	59 / 3.56	59 / 3.61	58 / 4.94	57 / 5.41	58 / 4.98	58 / 4.88
Owlet	60 / 3.94	60 / 3.95	59 / 3.98	59 / 3.91	59 / 3.92	59 / 3.93	57 / 4.87	57 / 5.38	58 / 4.77	58 / 4.65	59 / 3.90	60 / 3.92	59 / 3.94	60 / 3.89	59 / 3.91	59 / 3.94	58 / 4.74	57 / 5.47	58 / 4.76	58 / 4.31

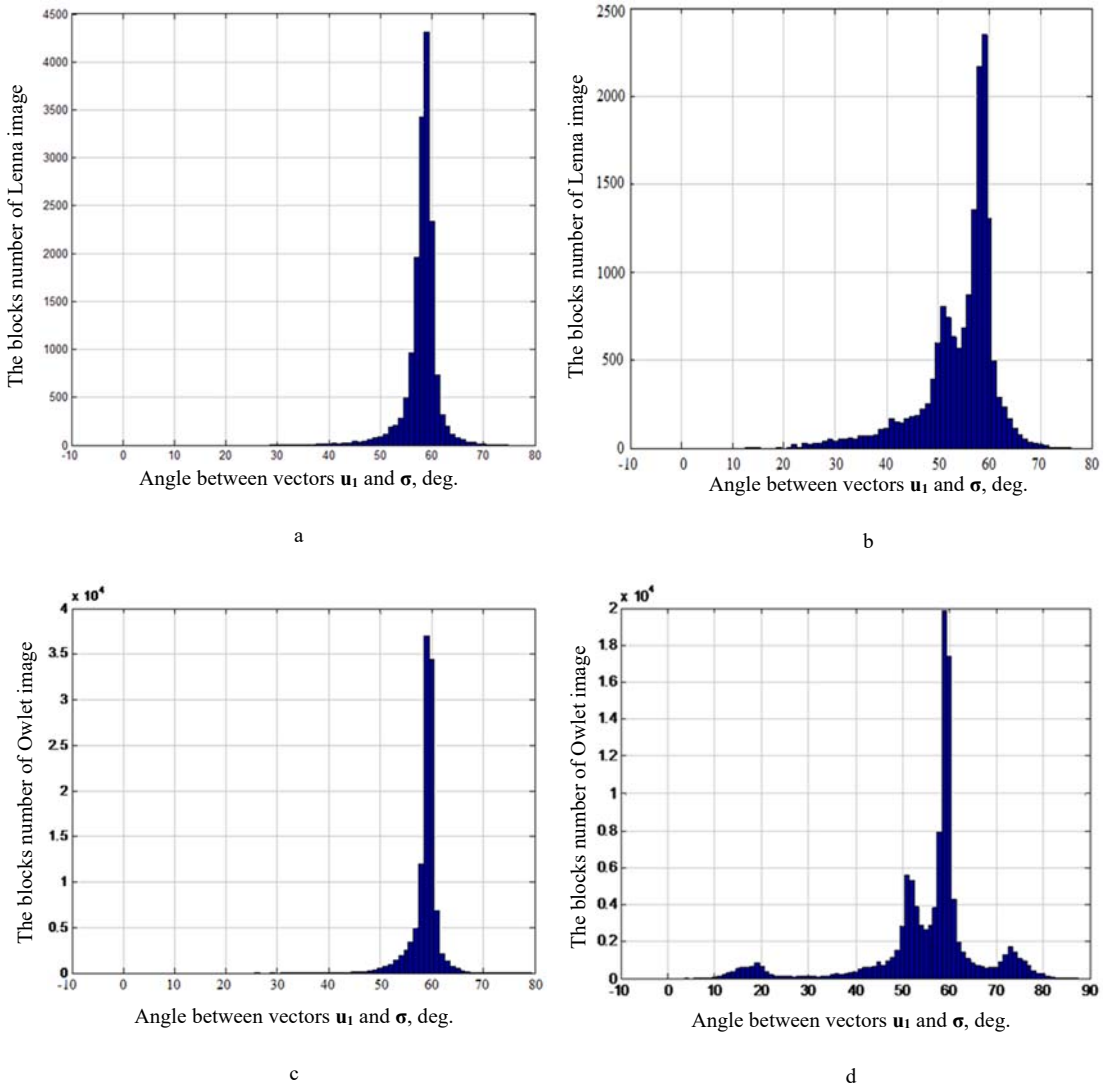


Figure 5. The histograms Γ_U: a — for the original Lenna digital image; b — for the digital image obtained by "Salt-Pepper" noise superimposition with d = 0.02 for Lenna digital image; c — for the original Owlet digital image; d — for the digital image obtained by "Salt-Pepper" noise superimposition with d = 0.02 for Owlet digital image

4. Conclusions

This paper discusses the developed basics of the new general approach for organizing the detection process of the integrity violation of digital images. The efficiency of the proposed algorithm does not depend on the specific type and method of implementation of these forgeries and image format. It was shown that for most blocks of an original image (regardless the format of the digital image container: lossy or lossless) the angle between the left (right) singular vector corresponding to the largest singular value of the $l \times l$ -block of image's matrix and vector composed of the singular values of the block is defined by the angle between the *n*-optimal vector and the first vector of the standard basis $\mathbf{R}^l$. It is proved and experimentally confirmed that the obtained feature of formal parameters of image with integrity violation will take place in a much lower number of image's blocks compared to the original image. The Γ_U-, Γ_V-histograms are also qualitatively different.

The presented results after obtaining of qualitative estimations of the detected differences were used during the development of the new method KBG for digital images violation integrity detection. Using a computational experiment, it was shown that the efficiency of KBG is comparable to the efficiency of the best modern steganalytical methods, along with this it detects the digital images integrity violation, that are different from steganography transformation results.

Table 3. The integral parameter ρ value for various steganalytical methods of LSB-method results detection under various hidden communication channel throughput

Steganography methods / Embedding rate, Bpp	Ker's	Liu's	NDH COM	RLH COM	Fused feature	KBG
0.5	0.5846	0.9608	0.5212	0.8298	0.7324	**0.9296**
0.75	0.9052	0.9885	0.765	0.8468	0.9138	**0.9615**
1	0.9376	0.9931	0.9244	0.851	0.9376	**0.9807**

There are no principal objections against the use of the offered approach based on particular characteristic features of the singular numbers and singular vectors of blocks for development of methods of the analysis of digital video (for the purpose of identification of its integrity violations, i.e. steganalysis) and digital audio (after its preliminary representation in the form of two-dimensional matrix) (Kobozeva and Khoroshko, 2009).

References

1. Rey, C. and Dugelay, J.-L. (2002) A survey of watermarking algorithms for image authentication. *EURASIP Journal on Advances in Signal Processing*, 6, 613–621. DOI: 10.1155/S1110865702204047.
2. Amerini, I., Ballan, L., Caldelli, R., Del Bimbo, A., Del Tongo, L. and Serra, G. (2013) Copy-move forgery detection and localization by means of robust clustering with J-Linkage. *Signal Processing: Image Communication*, 28(6), 659–669. DOI: 10.1016/j.image.2013.03.006.
3. Farid, H. (2009) Image forgery detection. *IEEE Signal Processing Magazine*, 26(2), 16–25. DOI: 10.1109/MSP.2008.931079.
4. Gul, G. and Kurugollu, F. (2010) SVD-based universal spatial domain image steganalysis. *IEEE Transactions on Information Forensics and Security*, 5(2), 349–353. DOI: 10.1109/TIFS.2010.2041826.
5. Bobok, I.I. and Kobozeva, A.A. (2011) Steganalysis as a special case of the analysis of the information system. *Suchasna Spetsialna Tekhnika*, 1, 21–34.
6. Natarajan, V. and Anitha, R. (2012) Blind image steganalysis based on contourlet transform. *International Journal on Cryptography & Information Security*, 2(3), 77–87. DOI: 10.5121/ijcis.2012.2307.
7. Kobozeva, A.A. and Khoroshko, V.A. (2009) *Analysis of Information Safety*. Kyiv: DUT.
8. Kobozeva, A.A. (2014) A basis of common approach to the development of universal steganalysis methods for digital images. *Odes'kyi Politechnichnyi Universytet. Pratsi*, 2, 136–146. DOI: 10.15276/opu.2.44.2014.25.

9. Koch, E. and Zhao, J. (1995) Towards Robust and Hidden Image Copyright Labeling. In: *Proc. of 1995 IEEE Workshop on Nonlinear Signal and Image Processing*, Neos Marmaras, Greece, June 1995. Neos Marmaras, Greece: IEEE CAS and ASSP Societies, pp. 123–132.
10. Kutter, M., Jordan, F. and Bossen, F. (1998) Digital signature of color images using amplitude modulation. *Journal of Electronic Imaging*, 7(2), 326–332.
11. Xia, Z., Yang, L., Sun, X., Liang, W., Sun, D. and Ruan, Z. (2011) A Learning-Based Steganalytic Method against LSB Matching Steganography. *Radioengineering*, 20(1), 102–109.
12. Li, B., He, J., Huang, J. and Shi, Y.Q. (2011) A survey on image steganography and steganalysis. *Journal of Information Hiding and Multimedia Signal Processing*, 2(2), 142–172.
13. Fridrich, J. (2004) Feature-Based Steganalysis for JPEG Images and its Implications for Future Design of Steganographic Schemes. In: *6th International Workshop, IH 2004*, Toronto, Canada, May 2004. Berlin: Springer, pp. 67–81.