Steganalysis Method for Detecting LSB Embedding in Digital Video, Digital Image Sequence

Alla Kobozieva[a], Ivan Bobok[a], Nataliya Kushnirenko[a]

[a] *Odesa Polytechnic National University, Shevchenko av., 1, Odesa, 65044, Ukraine*

Abstract

Steganography currently remains one of the most rapidly and effectively developing areas of information security. It leads to an increase in the relevance of steganalysis to avoid the negative consequences of covert communication for the purpose of illegal actions. Preference in the organization of a covert communication channel today is given to digital video. However, modern video steganalysis is behind the required level, particularly in conditions of low capacity of the covert channel. This paper is dedicated to developing a new effective steganalysis method for detecting embedded additional information in digital video (a sequence of digital images) by one of the most common steganographic methods today, which is the LSB method. The developed method is based on the sensitivity of linearity of singular vectors frequency in the corresponding original content matrices to disturbing influences. The authors determined this property in previous works. The current work established qualitative and quantitative differences between the properties of function, which represents the dependency of the singular vector frequency in the image/video frame matrix on its number for original contents and steganographic messages, which made it possible to develop an algorithmic implementation of the proposed method. The efficiency of this implementation in the case of a low capacity of a covert communication channel (<0.25 bit/pixel), including at a low frame embedding rate (<50%), exceeds the efficiency of analogues, which made it possible to increase the efficiency of steganalysis of digital video (sequence of digital images) as a whole.

Keywords

digital video, digital image, LSB method, steganalysis, covert channel capacity1

1. Introduction

One of the most rapidly and effectively developing areas in information security in recent decades is steganography, the art of covert communication. The critical question is in whose interests this communication is being carried out. If its goal is illegal actions, the result of which may cause negative consequences for individual people, enterprises, banks, etc., and the state as a whole, then it becomes critically important to ensure the possibility of identifying such a communication channel, obtaining hidden information, which is within the competence of steganalysis [1].

The preference for organizing a covert communication channel is increasingly given to digital video nowadays. There are several reasons for this. The main ones are as follows. Firstly, video traffic is the most significant part of all consumer Internet traffic today. Secondly, a video makes it possible to provide a high capacity of a covert communication channel, particularly in real-time [2]. Thirdly, video steganalysis is behind the required level due to its complexity, and the development activity in this field is relatively low. Research here is only taking initial steps, compared with the steganalysis of individual digital images [2]. Although methods that work with digital images are sometimes adapted for video [3,4], this is not always possible, especially when video steganalysis is desirable in real-time [5].

ICST-2023: Information Control Systems & Technologies, September 21-23, 2023, Odesa, Ukraine.
EMAIL: alla_kobozeva@ukr.net (A. Kobozieva); onu_metal@ukr.net (I. Bobok); infsec2011@gmail.com (N. Kushnirenko)
ORCID: 0000-0001-7888-0499 (A. Kobozieva); 0000-0003-4548-0709(I. Bobok); 0000-0003-3722-0229 (N. Kushnirenko)


All steganalysis methods, including those working with video, depending on whether they need additional information about the analyzed content, can be divided into two large classes: universal [6,7], which determine the presence/absence of additional information in the information content without taking into account the specifics of the steganographic algorithm used to embed it into the container, and directed [8], which take into account the characteristics of a particular/specific steganographic algorithm and used for revealing their results. Due to the broadest range of different steganographic methods and approaches, which is expanding daily with the rapid development of steganography, the relevance of developing universal steganalysis methods is growing. However, suppose a stegano analyst has the necessary information about how a covert communication channel is established (in particular, about the used steganographic algorithm), which in practice has a significant probability. In that case, he will prefer to use the appropriate directed method as a tool, which is more efficient than the universal one when applied under the same conditions. This conclusion became the main motivational component for the authors of this work to develop a directed steganalysis method for video.

2. Related works

Note that video can be considered a sequence of digital image frames. Therefore, in this work, such information contents are not distinguished. A video or an arbitrary sequence of images saved in the same format is considered a container.

The steganalysis process can be carried out in the spatial domain of the container or in one of the transformation domains, among which much attention is paid to the frequency domain, the singular value decomposition domain of the corresponding matrix, etc. The important thing here is that the domain chosen for the content examination should not depend on which domain was used for embedding the additional information [2, 6, 9].

One of the most common steganographic methods today is the LSB method [10]. The simplicity of its implementation, the possibility of providing a high capacity of a covert communication channel, and the possibility of embedding and decoding additional information in real-time guarantee this method does not lose popularity in the coming years. At the same time, the task of effectively detecting the additional information embedded with this method will still be relevant.

The problems of detecting the results of video steganographic transformation using the LSB method have already been raised by experts in many works. Thus, in [11], a new metric for video steganalysis is proposed. This metric makes it possible to detect disturbances in the video frame in areas with minor differences in brightness values (background areas). The main advantage of this method is achieved by considering the direction and distance of the current video frame from the reference one.

In [12] proposed a frame-by-frame video steganalysis method designed to detect additional information embeddings made by the LSB method (LSB-matching implementation), which was the authors' reaction to the H265 video coding standard. The detailed experimental results presented by the authors in the paper, including the case of a low-capacity covert communication channel (CC), show the efficiency of the proposed video steganalysis method, and together with the applicability conditions (frame-by-frame analysis, LSB-matching implementation, and, most importantly, its viability at low capacity of a covert communication channel, which is not even studied in most works), makes it a priority for a comparative analysis of efficiency with the method proposed in this paper.

In [13], based on cross-correlation analysis, a video steganalysis technique is proposed, where attention is paid to detecting the results of additional information embedding using the implementation of LSB-matching.

The method [4] is based on analysis of the number of blocks with the same brightness values in the matrices of color components of digital contents. The main advantage here is the use of the spatial domain of video in the process of steganalysis, which makes it possible to avoid additional computational costs and additional accumulation of computational errors during the transition from the spatial domain to the transformation domain and back.

However, none of the steganalysis methods mentioned above allows us to speak about the final solution to the problem of video steganalysis, in particular, under conditions of low capacity of the covert channel.

Recently, the authors of this work have developed a new approach to the problem of detecting integrity violations of a digital image based on the analysis of the dependency function of the frequency of the image matrix singular vector (SNV) on its number (SNV approach), information about which will soon be published in the open sources. The basis of the SNV approach is the property of the SNV frequency linearity for the original image determined by the authors. This property is sensitive to disturbing influences, which makes it possible to separate the original content from the one whose integrity is violated, particularly under conditions of minor disturbing influences. Taking into account the possibility of considering video as a set of images and the process of steganographic transformation as a particular case of a disturbance [6], it becomes possible to use the SNV approach to develop steganalysis methods for video. The SNV approach, taking into account the mentioned sensitivity of the linearity of the SNV frequency, should ensure the efficiency of the corresponding methods under conditions of low capacity of the communication channel.

3. Aim and tasks of the study

The *aim* of the work is to increase the efficiency of steganalysis of video, a sequence of digital images, by developing a steganalysis method for detecting the results of LSB transform, which is effective, including cases with low communication channel capacity, based on the SNV approach.

The low covert communication channel capacity is further understood as CC<0.25 bpp, the justification for which can be found in [3].

To achieve this goal, the following tasks are solved in the work:

1. The choice of a quantitative indicator for the violation of the linearity property of the SNV frequency;
2. Research of the quantitative characteristics of the dependency function of the SNV frequency of the image matrix/video frame on its number for original contents and steganographic messages obtained using the LSB method with different covert channel capacity;
3. Development of a steganalysis method for video and its algorithmic implementation;
4. Analysis of the efficiency of the elaborated method.

4. Development of a steganalysis method

4.1. Singular vector frequency, its properties

Let us formulate the foundations of the SNV approach. Let F be an $n\times n$-matrix of the digital image/video frame,

$$F = U\Sigma V^T = \sum_{i=1}^{n} \sigma_i u_i v_i^T \quad (1)$$

is unequivocally defined normal singular value decomposition F [14], where U, V are orthogonal $n\times n$-matrices whose columns $u_i, v_i, i=\overline{1,n}$, are left and right SNVs, respectively, while left SNV are additionally lexicographically positive [14]; $\Sigma = diag(\sigma_1,...,\sigma_n)$, $\sigma_1 \geq ... \geq \sigma_n \geq 0$ are singular values of F. The use of only one matrix for the formal representation of a digital image in no way limits the generality of the reasoning. In the case of a color image, F can be a matrix of any (consecutively all) color component (RGB scheme), a luminance matrix (YUV scheme).

The SNV u_i (v_i), the elements of which, within the SNV approach, are considered as the values of some discrete function on the interval [1, n], is associated with a quantitative characteristic, which is the frequency $\bar{\eta}$, defined as follows [15]:

$$\bar{\eta} = \begin{cases} \frac{\eta}{2}, \text{ if } \eta \text{ is even} \\ \frac{\eta+1}{2}, \text{ if } \eta \text{ is odd} \end{cases} \quad (2)$$

where η is the number of sign changes of the function on the considered interval. Let us define $fr(i)$, $i=\overline{1,n}$, as a function that reflects the dependency of the frequency of SNV u_i (v_i) on its number *i*. As a result of the study of the $fr(i)$ properties, it was found that for the original images (in a lossless format) the rate of increase for the trend of this function is practically constant over almost the entire interval [1, n], which results in a property called by the authors the linearity of the SNV frequency (both left and right) for the image/video frame, the integrity of which is not violated, which means that the function $fr(i)$, $i=\overline{1,n}$, is well approximated almost on all [1, n] by a linear monotonically increasing function $l(i)$, $i=\overline{1,n}$ for the original image without losses (Fig. 1(a, b)); the linearity of the SNV frequency is a characteristic that is sensitive to any disturbing influences, including steganographic transformation (Fig. 1(c)).

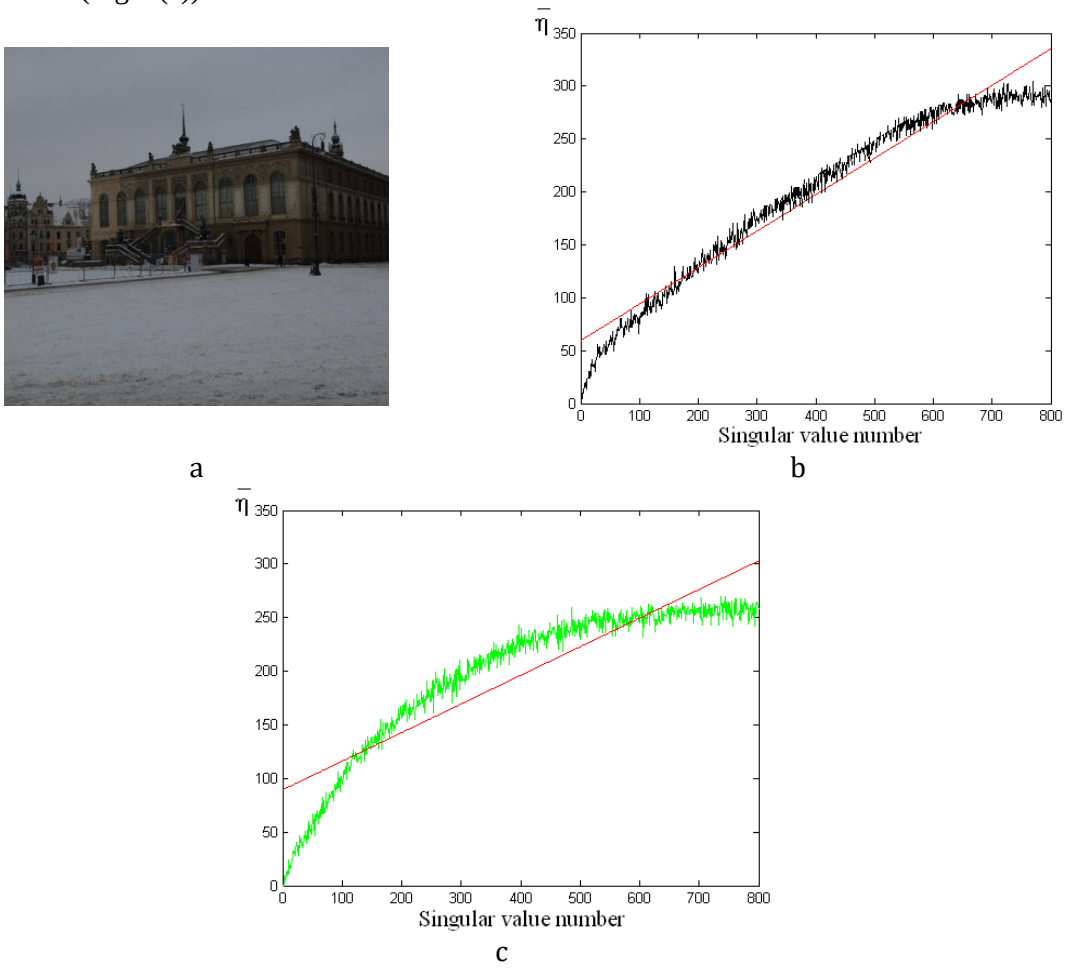

Figure 1: Illustration of the linearity of the SNV frequency for the original image and its violation in the case of a steganographic message: a – original image; b – graphs of the function $fr(i)$ and its linear approximation $l(i)$ for the original image; c – graphs of the function $fr(i)$ and $l(i)$ for the image-steganographic message generated by the LSB method with a capacity of a covert communication channel of 0.5 bpp

Violating the linearity of the SNV frequency for a non-original image/video frame with embedded additional information will make it possible to separate it from an image/video frame whose integrity has not been violated (parts of an empty container). Following the SNV approach, such a fundamental possibility can be effectively implemented even in the case of a low capacity of a covert channel. However, to develop an appropriate steganalysis method, it is necessary to obtain quantitative estimates of the linearity violation of the SNV frequency, which is one of the problems this work solves.

Note that, given the poor resistance of the LSB method to any attacks against an embedded message, in particular to a compression attack, the obtained steganographic messages will be stored in lossless formats, while the containers used can be both lossy and lossless, which requires a separate study.

4.2. Quantitative estimates of the linearity violation of the singular vector frequency

As possible quantitative indicators of the violation of the linearity of the SNV frequency for a video frame (image), consider the following:

$$P = \left(\sum_{i=1}^{n} \left(fr(i) - l(i) \right)^2 \right)^{\frac{1}{2}} \quad (3)$$

$$L = \max_i \left| fr(i) - l(i) \right| \quad (4)$$

We examine indicators (3) and (4) for individual images (video frames) depending on whether the content is original or non-original (part of the container/part of the steganographic message), on the content format (lossy, lossless), on the capacity of the covert communication channel.

Based on the foregoing, theoretically, a natural indicator of content integrity violation will be an increase in both (3) and (4) compared to the original image/frame of the original video stored in a lossless format, with any changes, including a steganographic transformation. Storing in a lossy format is also a disturbance. It should be noted that the indicators (3) and (4), which were introduced naturally, unfortunately, as the computational experiment shows, do not fully provide the ability to separate the original content (a separate image, video frame) from the one whose integrity is violated, taking into account only their values. Although such a separation does not raise questions when examining the graphs of the functions $fr(i)$ and $l(i)$, where the violation of the linearity of the SNV integrity is obvious, which is illustrated (Fig. 2) for the image presented in Fig.1(a) for which P=531, L=35. These indicators can be lower for images disturbed by compression (Fig. 2). However, as the computational experiment shows, the number of such contents (individual video frames, individual images in a sequence), for which there is no increase in indicators (3), (4) in case of integrity violations, is small, less than 7% for various disturbing influences. They are practically absent in the case of steganographic transformation by the LSB method. Because of this, parameters (3), (4) are used below to quantify the violation of the linearity of the SNV frequency. Consider the values of parameters (3), (4) for original images in lossless format (to be specific, Tif). Due to the features of the function $fr(i)$ (lack of monotonicity in the domain of a function), it is obvious that for any image/video frame, including the original one, the following is true $P \neq 0, L \neq 0$. As a result of a computational experiment that involved more than 600 digital images from the database img_Nikon_D70s (n=800) [16] found that the mean value for the indicator P, hereinafter referred to as P_a, is defined as $P_a = 549.82$, and the analogous value L_a for the indicator L is 34.97. On the basis of these images, groups of steganographic messages were formed using the LSB-matching method with CC=0.1, 0.25, 0.5, 1 bpp. For each of the obtained groups P_a, L_a were determined (Fig. 3). Dependency graphs of P_a, L_a on the value of the CC behave following theoretical expectations, monotonically increasing: with an increase in the capacity of the covert channel – the disturbing influences on the original image, the reaction $fr(i)$ increases, which is expressed in an increase in the difference between the values $fr(i)$ from the corresponding linear approximation. Since lossy image compression is an additional disturbing action for the original lossless container in addition to steganographic transformation, when using an image in lossy format as a content container, it is evident that the difference between P_a, L_a for steganographic messages and the values of the same parameters for original images increases, which is illustrated in Fig. 3. Judging by the obtained experimental results, the values of P_a, L_a are significantly different for sequences of original images (in a lossless format) and image sequences, which are steganographic messages formed by LSB-matching, with subsequent saving in a lossless format, the need of which was mentioned above. This difference occurs regardless of whether the container is in a lossy or lossless

format. Here, a clear quantitative difference in P_a, L_a is significant with a small CC=0.1 bpp, which is a theoretically expected consequence of the sensitivity of the linearity of the SNV frequency of the original lossless content to disturbing influences.

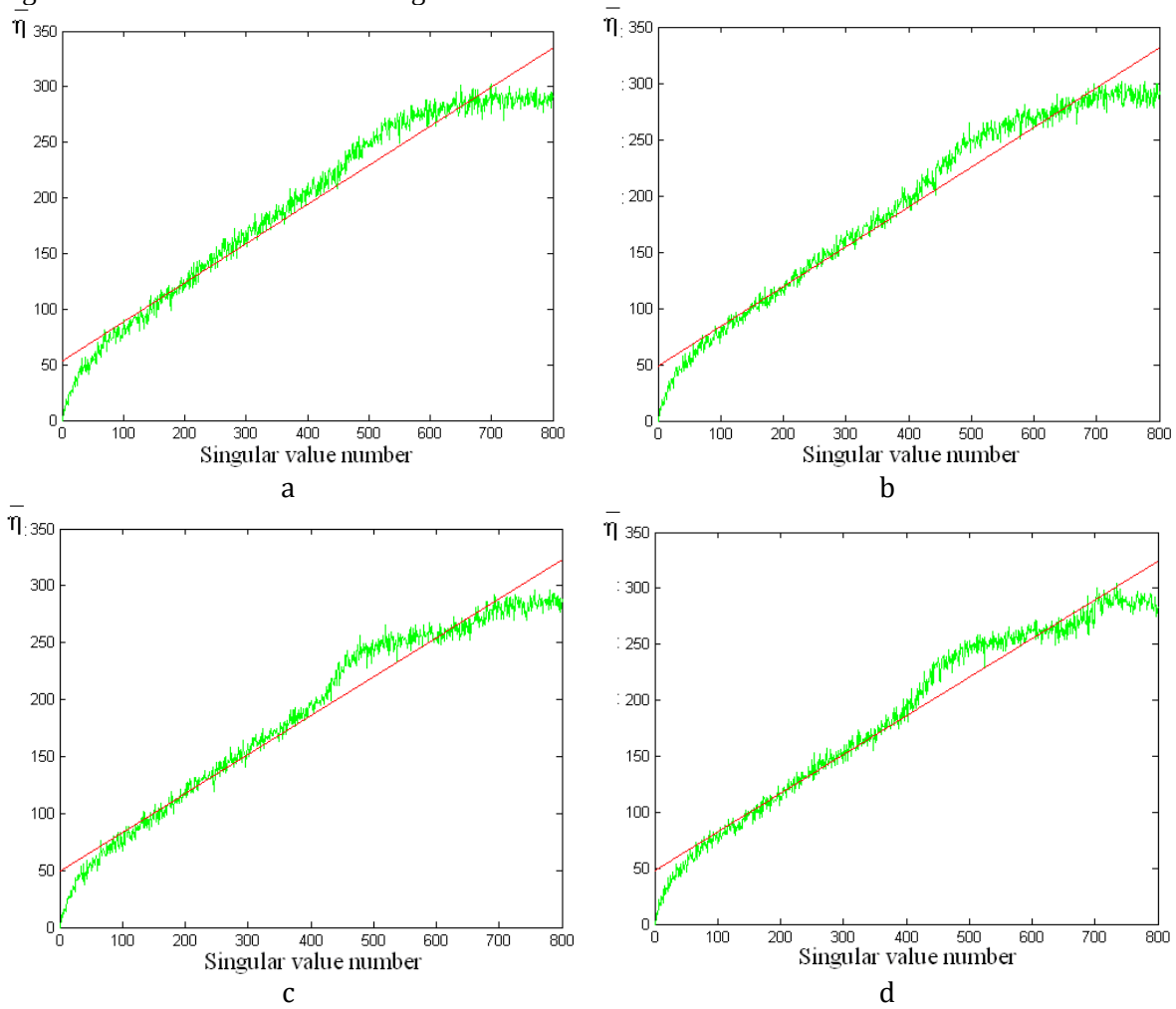

Figure 2: Functions $fr(i)$ and $l(i)$ for an image which has undergone lossy compression: a – QF=85 (P=496, L=33); b – QF=75 (P=441, L=41); c – QF=65 (P=440, L=43); d – QF=55 (P=431, L=37)

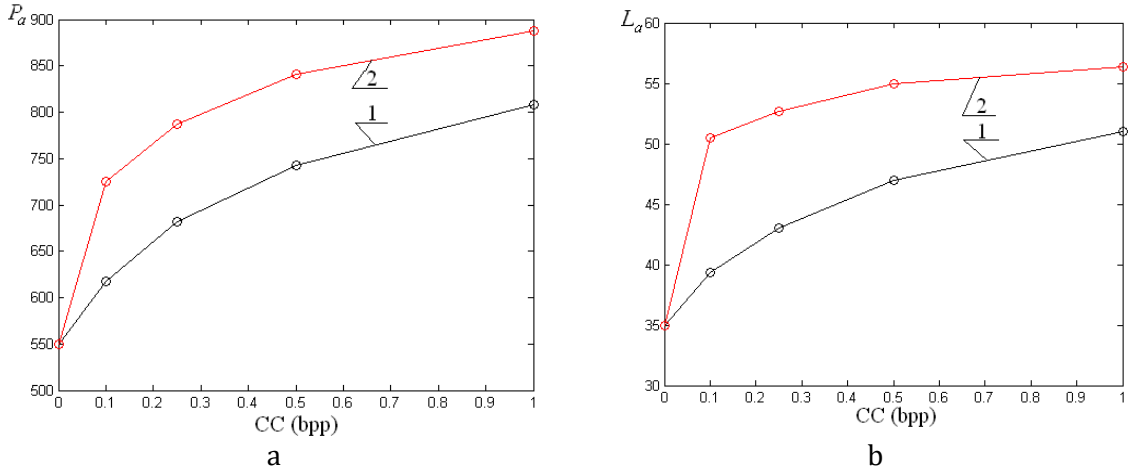

Figure 3: Dependency graphs of P_a, L_a on CC: a – for containers in the lossless format; b - for lossy containers (Jpeg, *QF*=85)

Taking into account that the differences in the parameters P_a and L_a for both original and non-original contents are comparable to each other (at CC = 0.1 bpp for P_a the increase with the embedding

of additional information was 11.5%, for L_a it was 12.6%), then for further research it was decided to leave only one of the two considered parameters, namely (4).

The average value carries information about the values of the entire set for which it is determined. However, for the work, taking into account that not every frame of the video (not every image of the sequence) [12] can be used to embed additional information during the steganographic transformation of a video/sequence of images. It is also essential to know how often in a sequences of images/video frames, the same/close L values are accepted and which of the possible values is accepted more often than others. The histograms of L values obtained for individual video frames or individual images of a sequence can be used to get such information. Based on the theoretical assumptions (SNV method) and the results regarding L_a, it can be assumed that the histograms of L values for the container – the original (in lossless format) sequence of video frames or images and for the steganographic message – a non-original sequence, which is the result of the embedding of additional information into a container will qualitatively differ from each other:

- the histogram Γ_S for the sequence of video frames/images of the steganographic message will be shifted to the right along the OL axis relative to the histogram Γ_O for the original sequence for any CC (the more, the larger the C);
- modes $m(\Gamma_S)$, $m(\Gamma_O)$ of histograms Γ_S and Γ_O respectively will be related by the following equation:

$$m(\Gamma_S) \geq m(\Gamma_O); \tag{5}$$

- with an increase in the CC, the difference (5) between $m(\Gamma_S)$, $m(\Gamma_O)$ will increase due to the increase in $m(\Gamma_S)$.

All theoretical expectations have been confirmed in practice (Fig. 4). To develop a steganalysis method, it is necessary to determine quantitative differences for $m(\Gamma_S)$, $m(\Gamma_O)$. Most often in practice, when using a video or a sequence of images as a container, additional information is embedded in separate frames/images with an unchanged CC. Then, by obtaining the corresponding histograms, it is possible not only to separate the original video from the one that carries hidden additional information but also to estimate the CC using the direct value of the mode (Fig. 4), which is the direction of the further work of the authors. If, however, the CC changed during the embedding of additional information from frame to frame, this does not interfere in any way with revealing the presence of additional information by the value of the mode of the corresponding histogram, which follows from the results presented in Fig. 5(a), where the mode is 43. In contrast, for the original frame sequence/image, this value is much smaller (Fig. 4(a)).

Most often in practice, a video/sequence of images in a lossy format is used as a container, which, after the embedding of additional information, will be saved in a lossless format, taking into account the vulnerability of the LSB method to any attacks against the embedded message. In this case, the difference in the modes of the histograms L for the initial original sequence (in the lossless format) and the steganographic message created based on the container obtained by re-saving the primary sequence in the lossy format will be even more apparent. Indeed, the creation of a container in a lossy format itself will already violate the linearity of the SNV frequency of the image/video frame of initial sequence (Fig. 6 (compare with Fig. 4(a))), and the steganographic transformation will only increase this deviation from linearity (Fig. 7). When changing the CC from frame to frame, a significant superiority of $m(\Gamma_S)$ compared to $m(\Gamma_O)$ does not cause problems in identifying the steganographic message (Fig. 5(b)). It should be noted that when the container is a video/sequence of images in a lossy format, it is impossible to systematically estimate the value of the CC from the value $m(\Gamma_S)$, even if it does not vary from frame to frame. This is a consequence of the "imposition" of two disturbing influences on the original content in a lossless format: compression and steganographic transformation by the LSB method. Their impacts on the singular triples (σ_i, u_i, v_i) (1) of the matrix F occur independently of each other, sometimes enhancing and somewhere reducing the impact of each other, which may result in the observed non-monotonicity of the $m(\Gamma_S)$ increase in Fig. 7. However, for the vast majority of the considered videos in the lossy format, a monotonic increase of $m(\Gamma_S)$ with an increase in the CC did take place (the results of the experiment are given below).

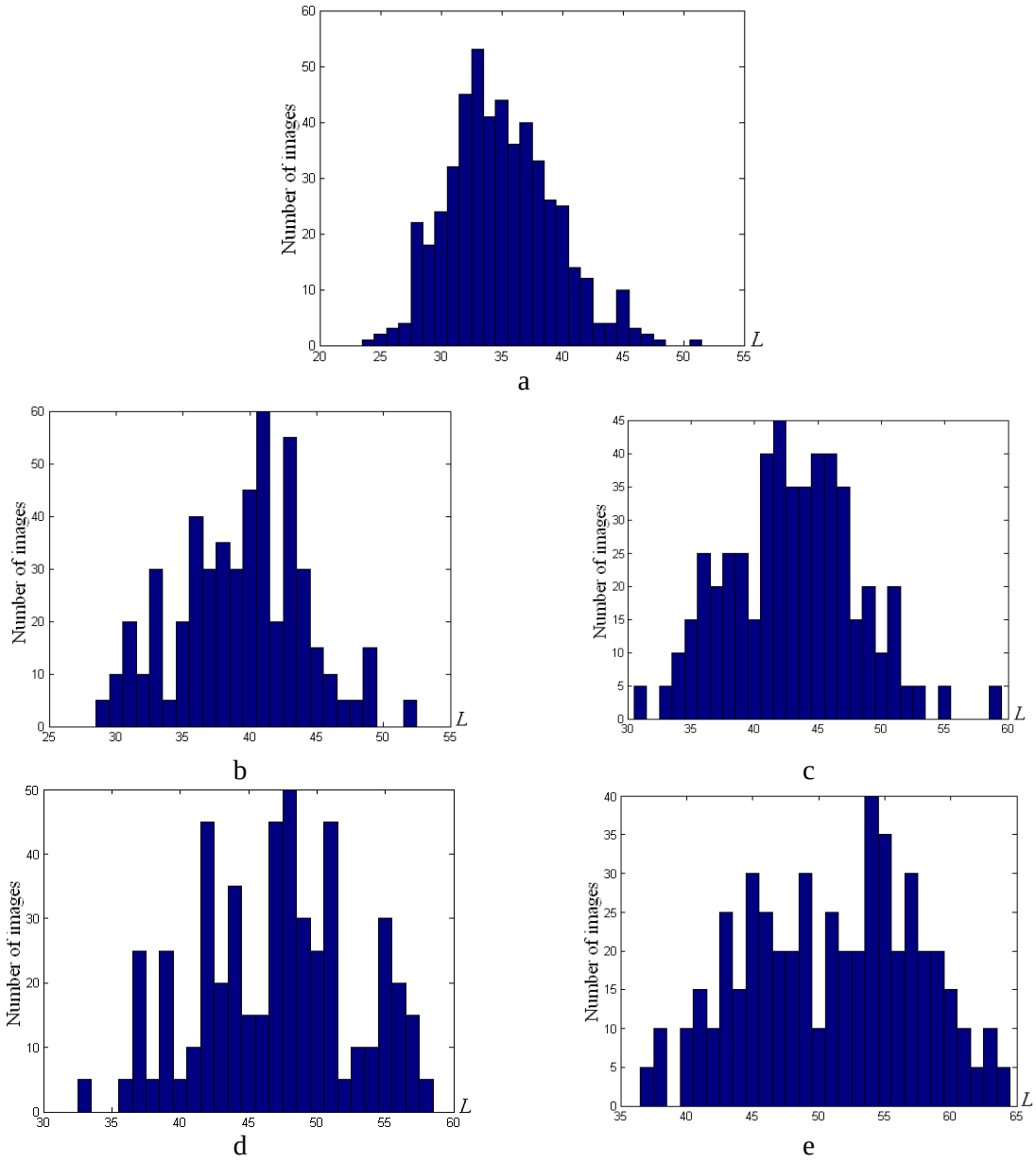

Figure 4: Histograms of *L* values: a – for a container representing a sequence of 500 original images in Tif format; b, c, d, e – for steganographic messages generated by the LSB method with CC=0.1, 0.25, 0.5, 1bpp, respectively

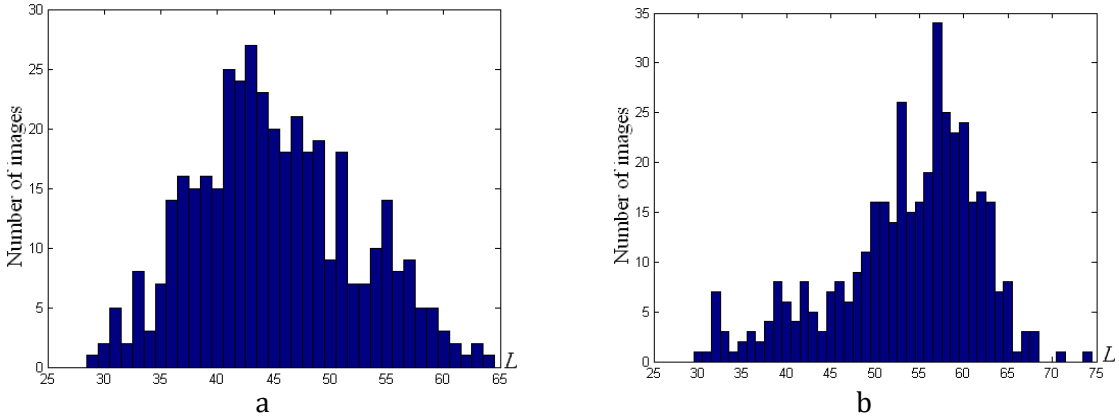

Figure 5: Histograms of L values of individual images for a steganographic message generated by the LSB method (the CC took different values for different images: 0.1, 0.25, 0.5, 1 bpp), obtained based on a container representing a sequence of 400 images in the format: a – Tif; b - Jpeg (QF=85)

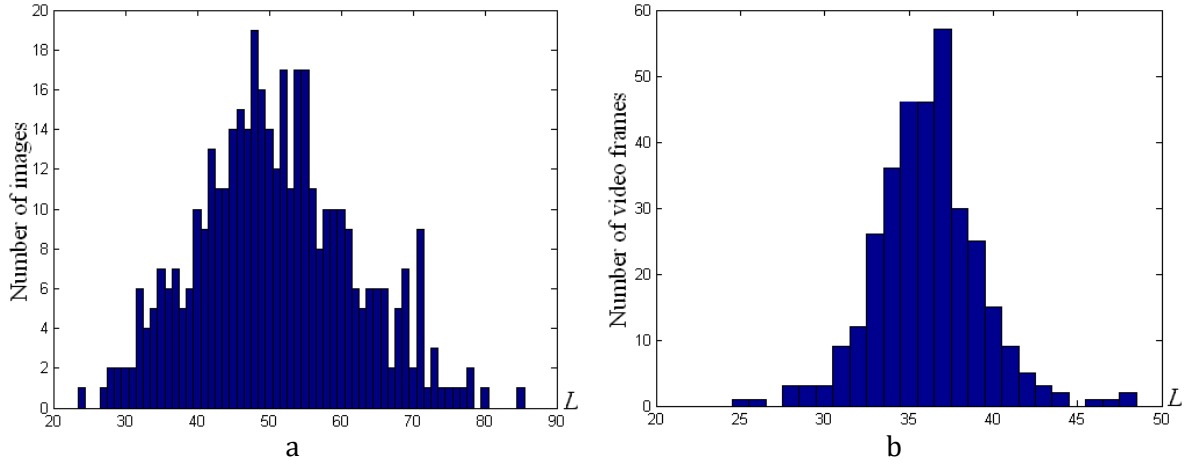

Figure 6: Histograms of L values: a – for the sequence of corresponding images in Jpeg format (QF∈{55,65,75,85}); b - for video in MPEG4 format

Note that although most of the results obtained above are demonstrated on image sequences, due to the authors considering video as a set of individual image frames and video analysis as a sequential analysis of frames, this does not limit the generality of reasoning and conclusions, which is confirmed by the results of the experiments, some of which are presented in Table 1, where V1-V4 are videos (MPEG-4) obtained by a Realme 7 Pro mobile phone (64 MP, f/1.8, 26mm (wide), 1/1.73", 0.8µm, PDAF), V5 – video (MPEG-4) taken by a Canon PowerShot A520 – CCD, 4MP video camera; I1 (Jpeg format (QF=85)), I2 (Tif format) – image sequences, where I2 contains images from the database [16] and I1 obtained by re-saving images from I2 to lossy format.

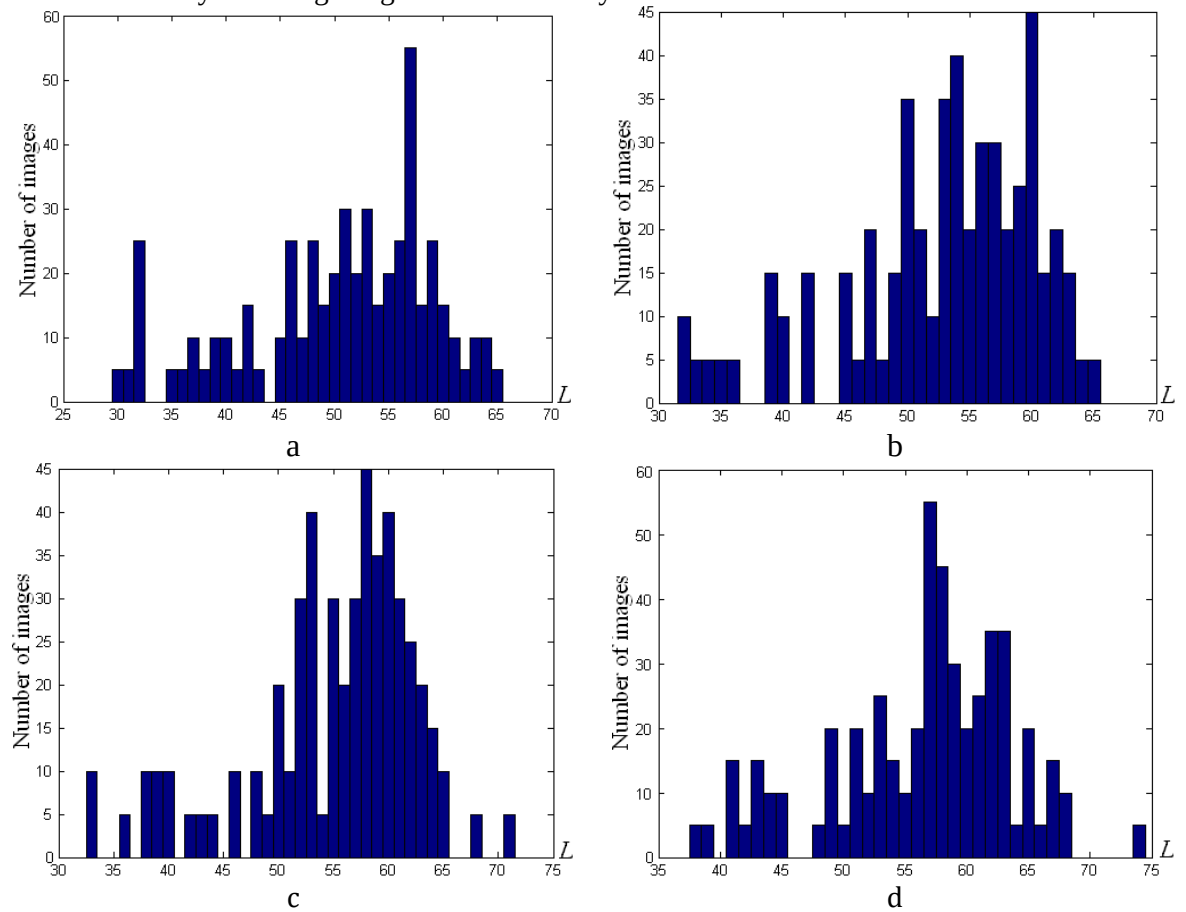

Figure 7: Histograms of *L* values of individual images for a steganographic message formed based on a container representing a sequence of 500 images in Jpeg format (*QF*=85) using the LSB method with CC: a – 0.1 bpp; b – 0.25 bpp; c – 0.5 bpp; d – 1 bpp

Considering that the properties of the corresponding left and right SNVs of the matrix F of the image/video frame within the framework of the SNV approach do not qualitatively differ, but are quantitatively comparable, only left lexicographically positive SNVs are analyzed in the proposed method.

4.3. Steganalysis method

Based on the results obtained, the steganalysis method's main steps for examining a video containing N frames, or a sequence of N images, formally saved in a lossless format, are as follows.

Step 1. For each of N video frames / each image of the sequence with matrix F_j, $j=\overline{1,N}$, size $n\times n$:

1.1. Calculate the normal singular value decomposition (1).

1.2. Determine the frequencies (2) of each left SNV $u_i, i=\overline{1,n}$ of matrix F_j for video/image sequence.

1.3. Construct a function $fr(i)$, $i=\overline{1,n}$, the dependency of the SNV frequency u_i on its number i.

1.4. Construct a linear approximation $l(i)$ for the function $fr(i)$.

1.5. Determine the value of L for F_j — $L\left(F_j\right)$ (4).

Step 2. Determine

$$L_a=\frac{1}{N}\sum_{j=1}^{N}L\left(F_j\right).$$

Step 3. Construct a histogram Γ of values $L\left(F_j\right)$, $j=\overline{1,N}$.

Step 4. Determine the mode $m(\Gamma)$ of the histogram Γ obtained at the previous step.

Step 5

If $\left(m(\Gamma)<T_1\right)\&\left(L_a<T_2\right)$,

where T_1, T_2 are threshold values obtained experimentally

then video/image sequence does not contain an additional information

otherwise video/image sequence is a steganographic message

The following parameter values correspond to the algorithmic implementation of the method: n=800, T_1=35, T_2=36.5.

The efficiency of the developed method was evaluated using the standard parameter for such tasks which is the accuracy of detecting integrity violations [17] (*accuracy* (*ACC*)):

$$ACC=\left(TP+TN\right)/\left(TP+FN+TN+FP\right), \quad (6)$$

where *TP* (*True Positive*) is the number of correctly identified steganographic messages; *TN* (*True Negative*) is the number of correctly identified containers; *FP* (*False Positive*) is the number of containers erroneously identified as steganographic messages (type II errors); *FN* (*False Negative*) is the number of missed steganographic messages (type I errors).

A computational experiment was carried out to evaluate the efficiency of the algorithmic implementation of the developed steganalysis method. The experiment involved 35 video and image sequences containers, with the number of frames/images from 100 to 1000 elements. Videos were obtained with several video cameras (Olympus SP-820 – CMOS, 14MP; Nikon COOLPIX P100 – CMOS, 10MP; Canon PowerShot A520 – CCD, 4MP; Realme 7 Pro mobile phone video camera (64 MP, f/1.8, 26mm (wide), 1/1.73", 0.8μm, PDAF). Image sequences in lossless format were formed by images from the img_Nikon_D70s database [16], re-saving them in Jpeg format with $QF\in\{55,65,75,85\}$ resulted in image sequences in lossy format. For each of the described 35 contents, steganographic messages were formed using the LSB-matching method, where the CC for a video frame/image was taken sequentially 0.1, 0.25, 0.5, 1 bpp. Additional information was embedded in 100, 80, 60, 40% frames of the video/image sequence. Thus, the total number of steganographic messages was 560. The results of evaluating the efficiency of the method using the indicator (6), including comparison with the analogue [12], are given in Tables 2,3. As follows from the results (Table 2), the developed method provides high efficiency in embedding additional information into each video frame,

increasing this efficiency by 1.5% under the conditions of CC=0.1 bpp. At the same time, type I errors were not detected when testing the developed method, which is its significant advantage compared to analogues [4, 12]. The sensitivity of the property of the linearity of the SNV frequency allowed to get a more significant opportunity for the developed steganalysis method to gain efficiency in comparison with analogues with a small CC: The maximum ACC indicator is increased by 11.69% under conditions of a frame embedding rate of 40% (Table 3).

Table 1
Embedding additional information in each video frame

Video/image sequence	CC, bpp	L	$m(\Gamma_S)$
V1 (100 frames	0.1	42.12	40
	0.25	47.10	46
	0.5	51.33	51
	1	54.47	52
V2 (100 frames)	0.1	41.61	41
	0.25	45.84	47
	0.5	50.50	50
	1	54.36	54
V3 (100 frames)	0.1	40.42	41
	0.25	44.72	47
	0.5	50.27	51
	1	56.90	54
V4 (325frames)	0.1	41.35	41
	0.25	46.98	46
	0.5	50.68	50
	1	55.60	54
V5 (1000 lossy frames)	0.1	57.24	56
	0.25	62.74	61
	0.5	64.66	63
	1	66.04	65
I1 (100 images)	0.1	50.46	57
	0.25	52.64	60
	0.5	54.94	58
	1	56.36	57
I2 (100 images)	0.1	39.37	41
	0.25	43.05	42
	0.5	46.95	48
	1	51.01	54

Table 2
The results of a comparative analysis of the efficiency, determined by the ACC indicator (%), of the developed method when additional information is embedded into all video/image frames of the sequence

Method	Single frame/image embedding rate, bpp			
	1	0.5	0.25	0.1
Developed	**98.86**	**98.86**	**98.86**	**98.86**
Method [12]	99.95	99.91	99.88	97.44

Table 3
The results of a comparative analysis of the efficiency, determined by the ACC indicator (%), of the developed method depending on the frame embedding rate used for embedding additional information

Single frame/image embedding rate, bpp	Frame embedding rate, %					
	80		60		40	
	Method [12]	Developed	Method [12]	Developed	Method [12]	Developed
0.5	100	**98.86**	99.78	**98.86**	100	**98.86**
0.25	100	**98.86**	100	**98.86**	99.26	**96.00**
0.1	93.81	**98.86**	92.76	**98.86**	79.74	**91.43**

5. Conclusions

In the paper we solved an important scientific and practical problem of increasing the efficiency of identifying a steganographic communication channel in the case when a digital video (digital image sequence) is used as a container. An effective steganalysis method, based on the SNV approach, has been developed to detect the results of embedding additional information into a video/image sequence using the LSB method, which is based on the sensitivity of the linearity of the SNV frequency to disturbing influences.

During development, quantitative differences were established between the characteristics of the dependency function of the SNV frequency of the image matrix/video frame on its number for original contents and steganographic messages obtained with the LSB method using different CC. As a result of a reasonable choice, these characteristics were: the average value of the maximum deviation of the $fr(i)$ $fr(i)$ function from its linear approximation over all video frames/all images of the sequence (function $fr(i)$ determines the frequency of the SNV depending on its number), as well as the histogram mode of the maximum deviations $fr(i)$ from the linear approximation obtained for each video frame/each image sequence.

The established quantitative differences made it possible to develop an algorithmic implementation of the proposed method, the efficiency of which, in the case of a small CC exceeds the efficiency of its analogue, determined using the ACC parameter. At the same time, the maximum increase corresponds to CC=0.1 bpp under conditions of a frame embedding rate of 40%. It is more than 11 %, which is the main practical result of the work, and made it possible to increase the efficiency of steganalysis for video and image sequences.

At the moment, the authors' efforts are aimed at adapting the developed method to work in conditions of a small number of digital video frames, or digital images in a sequence (10 or less), where the informativeness of the histograms under consideration decreases; as well as ensuring the possibility of using the method in real time, since at the moment to organize the process of steganalysis, the transformation area is used here – the singular value decomposition of the frame matrix of the digital image/digital frame.

The mathematical foundations of the proposed method make it possible in principle to use it not only as a steganalysis method for detecting LSB attachments, but also as an expert method for detecting a violation of one of the information content security criteria – the integrity of the digital image/digital frame sequence under conditions of small perturbations, which is today one of the main problems in the field of information security.

6. References

[1] W.M. Eid, S.S. Alotaibi, H.M. Alqahtani, S.Q. Saleh, Digital Image Steganalysis: Current Methodologies and Future Challenges, IEEE Access 10 (2022) 92321-92336. doi: 10.1109/ACCESS.2022.3202905.

[2] M. Bouzegza, A. Belatreche, A. Bouridane, M. Tounsi, A comprehensive review of video steganalysis, IET Image Process. 16 (2022) 3407–3425. doi:10.1049/ipr2.12573
[3] I.I. Bobok, Steganalysis method for detection of the hidden communication channel with low capacity, Telecommunications and Radio Engineering 77(2018) 1597–1604. doi:10.1615/TelecomRadEng.v77.i18.20
[4] A.V. Akhmametieva, A.A. Efimenko, Comparative efficiency analysis of steganalytic algorithms for detecting the presence of attachments of confidential information in digital video, Informatics and Mathematical Methods in Simulation 7 (2017) 96-102.
[5] K. Tasdemir, F. Kurugollu, S. Sezer, Spatio-Temporal Rich Model-Based Video Steganalysis on Cross Sections of Motion Vector Planes, IEEE Transactions on Image Processing 25 (2016) 3316-3328. doi: 10.1109/TIP.2016.2567073
[6] A.A. Kobozeva, I.I. Bobok, A.I. Garbuz, General Principles of Integrity Checking of Digital Images and Application for Steganalysis, Transport and Telecommunication Journal 17 (2016) 128-137. doi:10.1515/ttj-2016-0012
[7] M. Dalal, M. Juneja, Steganography and Steganalysis (in digital forensics): a Cybersecurity guide. Multimed Tools Appl 80 (2021) 5723–5771. doi:10.1007/s11042-020-09929-9
[8] R. Rasras, M. Abu Sara, Z. AlQadi, R. Abu zneit, Comparative Analysis of LSB, LSB2, PVD Methods of Data Steganography, International Journal of Advanced Trends in Computer Science and Engineering 8 (2019) 748-754.
[9] S. Li, X. Ma, P. Liu, Q. Dai, H. Deng, Detection of Information Hiding by Modulating Intra Prediction Modes in H.264/AVC, in: Proceedings of the 2nd International Conference on Computer Science and Electronics Engineering (ICCSEE 2013), 2013, pp. 590-593. doi:10.2991/iccsee.2013.151
[10] M. Fateh, M. Rezvani, Y. Irani, A New Method of Coding for Steganography Based on LSB Matching Revisited, Security and Communication Networks 2021 (2021). doi:10.1155/2021/6610678
[11] K. Tasdemir, F. Kurugollu, S. Sezer, Video steganalysis of LSB based motion vector steganography, in: European Workshop on Visual Information Processing (EUVIP), Paris, France, 2013, pp. 260-264.
[12] K. Wu, Research of Video Steganalysis Algorithm Based on H265 Protocol, in: MATEC Web of Conferences 25, 03003 (2015). doi:10.1051/matecconf/20152503003
[13] M. Fan, P. Liu, H. Wang, et al., Cross correlation feature mining for steganalysis of hash based least significant bit substitution video steganography, Telecommun Syst 63 (2016) 523–529. doi:10.1007/s11235-016-0139-5
[14] C. Bergman, J. Davidson, Unitary embedding for data hiding with the SVD, 2205. URL: https://dr.lib.iastate.edu/entities/publication/bb2b5041-1c92-4ff5-b7f4-ff73c3483eed
[15] A.A. Kobozeva, A.V. Sokolov, The Sufficient Condition for Ensuring the Reliability of Perception of the Steganographic Message in the Walsh-Hadamard Transform Domain, Problemele Energeticii Regionale 2 (2022) 84-100. doi:10.52254/1857-0070.2022.2-54.08
[16] T. Gloe, R. Bцhme, The “Dresden Image Database” for benchmarking digital image forensics, 2010 ACM Symposium on Applied Computing (SAC ’10), New York, 2010. P. 1585–1591.
[17] S. Geetha, S. Sindhu, N. Kamaraj, Close Color Pair Signature ensemble Adaptive Threshold based Steganalsis for LSB Embedding in Digital Images, Trans. Data Privacy 1 (2009) 140–161.