Method for Estimating the Bandwidth Capacity of a Steganographic Communication Channel

[1]Bobok I.I., [2]Kobozieva A.A., [3]Laptiev O.A., [4]Savchenko V.A., [5]Salii A.G., [5]Kurtseitov T.L.
[1]Odesa Polytechnic National University, Odesa, Ukraine
[2]Odesa National Maritime University, Odesa, Ukraine
[3]Taras Shevchenko National University of Kyiv, Kyiv, Ukraine
[4]State University of Information and Communication Technologies, Kyiv, Ukraine
[5]National Defense University of Ukraine, Kyiv, Ukraine

Abstract. Ensuring information security in critical infrastructure, particularly in the energy sector, is highly relevant today. Steganographic methods are among the most effective for information protection, but they can also be misused for unauthorized extraction of classified data. This makes effective steganalysis crucial. One key task of steganalysis is estimating the bandwidth capacity of a covert communication channel, which remains unsolved, especially for digital video or image sets under low-bandwidth conditions. The main objectives of the study are to develop a steganalytic method for estimating the bandwidth capacity of a covert channel using an improved approach to analyzing information systems. The method is designed to be effective in low-bandwidth scenarios and independent of container format (lossy or lossless). To achieve these objectives, the study examines how singular value matrix perturbations of video frames/images depend on frame sequence after steganographic embedding. It also defines conditions for the disruption of the stabilization region of singular values, previously identified by the authors in original content. The most important results of this research include the development of an algorithmic implementation of the proposed steganalytic method, which demonstrates high efficiency under low-bandwidth conditions (≤25%) and is independent of the container format. Testing of the algorithm revealed no cases of incorrect bandwidth estimation. The significance of the obtained results lies in the demonstrated feasibility of adapting the proposed steganalytic method to assess other types of perturbation effects beyond steganographic embedding. This is particularly relevant for digital content integrity verification and forensic analysis.
Keywords**:** steganalysis, steganographic channel capacity, digital video, digital image, general approach to analyzing the state of information systems, singular value.

DOI: https://doi.org/10.52254/1857-0070.2025.2-66.08
UDC: 004.056

Metodă de estimare a capacității de lățime de bandă a unui canal de comunicare steganografic

[1]Bobok I.I., [2]Kobozieva A.A., [3]Laptiev O.A., [4]Savcenko V.A., [5]Salii A.G., [5]Kurțeitov T.L.
[1]Universitatea Națională Politehnică din Odesa, Odesa, Ucraina
[2]Universitatea Națională Maritimă din Odesa, Odesa, Ucraina
[3]Universitatea Națională Taras Shevchenko din Kiev, Kiev, Ucraina
[4]Universitatea de Stat de Tehnologii Informaționale și Comunicații, Kiev, Ucraina
[5]Universitatea Națională de Apărare a Ucrainei, Kiev, Ucraina

Rezumat. Asigurarea securității informațiilor în infrastructura critică, în special în sectorul energetic, este extrem de relevantă astăzi. Metodele steganografice sunt printre cele mai eficiente pentru protecția informațiilor, dar pot fi folosite greșit și pentru extragerea neautorizată a datelor clasificate. Acest lucru face ca steganaliza eficientă să fie crucială. O sarcină cheie a steganalizei este estimarea capacității lățimii de bandă a unui canal de comunicație ascuns, care rămâne nerezolvată, în special pentru seturi video digitale sau imagini în condiții de lățime de bandă redusă. Obiectivele principale ale studiului sunt dezvoltarea unei metode steganalitice pentru estimarea capacității lățimii de bandă a unui canal sub acoperire folosind o abordare îmbunătățită a analizei sistemelor informaționale. Metoda este concepută pentru a fi eficientă în scenarii cu lățime de bandă redusă și independentă de formatul containerului (cu pierderi sau fără pierderi). Pentru a atinge aceste obiective, studiul examinează modul în care perturbațiile matricei cu valori singulare ale cadrelor/imaginilor video depind de secvența de cadre după încorporarea steganografică. De asemenea, definește condiții pentru perturbarea regiunii de stabilizare a valorilor singulare, identificate anterior de autori în conținutul original. Cele mai importante rezultate ale acestei cercetări includ dezvoltarea unei implementări algoritmice a metodei steganalitice propuse, care demonstrează eficiență

ridicată în condiții de lățime de bandă redusă (≤25%) și este independentă de formatul containerului. Testarea algoritmului nu a evidențiat niciun caz de estimare incorectă a lățimii de bandă. Semnificația rezultatelor obținute constă în fezabilitatea demonstrată a adaptării metodei steganalitice propuse pentru a evalua alte tipuri de efecte de perturbare dincolo de încorporarea steganografică. Acest lucru este deosebit de relevant pentru verificarea integrității conținutului digital și analiza criminalistică.
Cuvinte-cheie: steganaliza, capacitatea canalului steganografic, video digital, imagine digitală, abordare generală a analizei stării sistemelor informaționale, valoare singulară.

Метод оценки пропускной способности стеганографического канала связи

[1]Бобок И.И., [2]Кобозева А.А., [3]Лаптиев О.А., [4]Савченко В.А., [5]Салий А.Г., [5]Курцеитов Т.Л.
[1]Одесский национальный политехнический университет, Одесса, Украина
[2]Одесский национальный морской университет, Одесса, Украина
[3]Киевский национальный университет имени Тараса Шевченко, Киев, Украина
[4]Государственный университет информационно-коммуникационных технологий, Киев, Украина
[5]Национальный университет обороны Украины, Киев, Украина

Аннотация. Вопросы защиты информации, циркулирующей в критической, в частности энергетической, инфраструктуре на сегодняшний день, являются чрезвычайно важными и актуальными. Одними из наиболее эффективных для защиты информации являются стеганографические методы. Однако эти же методы могут использоваться противоправными структурами для несанкционированного получения секретной информации, относящейся, в частности, к энергетическому сектору, что делает здесь критически актуальной проблему организации эффективного стеганоанализа. Одной из задач стеганоанализа является определение/оценка пропускной способности скрытого канала связи, не имеющей в настоящий момент удовлетворительного решения, в частности, когда в качестве контейнера используется цифровое видео или совокупность изображений в условиях малой пропускной способности стеганоканала. Целью работы является разработка на основании усовершенствованного общего подхода к анализу состояния информационных систем стеганоаналитического метода оценки пропускной способности скрытого канала связи для цифрового видео/пакета изображений, использованных в качестве контейнера, эффективного, в том числе, в условиях малой пропускной способности стеганоканала независимо от формата (с/без потерь) контейнера. Цель была достигнута путем исследования свойств функции зависимости возмущения сингулярного числа матрицы видеокадра/изображения от его номера в результате стеганопреобразования; определения формальных условий разрушения области стабилизации сингулярных чисел, наличие которой для оригинального контента установлено авторами ранее. Наиболее важным результатом работы является разработка алгоритмической реализации предложенного стеганоаналитического метода, эффективной, в частности в условиях малой пропускной способности стеганоканала (≤25%), без ограничений на формат (с/без потерь) используемого контейнера, что обеспечивается универсальной теоретической базой метода. В ходе тестирования разработанного алгоритма не было зафиксировано случаев ошибочной оценки пропускной способности стеганоканала. Значимость проведенных в работе исследований заключается в установлении принципиальной возможности адаптации разработанного стеганоаналитического метода для оценки величины возмущающего воздействия, отличного от стеганопреобразования, что актуально при проведении экспертизы целостности цифрового контента.
***Ключевые слова*:** стеганоанализ, пропускная способность стеганоканала, цифровое видео, цифровое изображение, общий подход к анализу состояния информационных систем, сингулярное число.

INTRODUCTION

The protection of information circulating within critical infrastructure, particularly in the energy sector [1], is currently of utmost importance. The digital transformation of energy sector organizations provides significant benefits but also introduces new cybersecurity challenges. Energy-related assets are vital for any country, and cyberattacks on these critical infrastructure facilities can lead to strategic, financial, and human losses. The energy sector is typically divided into three main areas: the oil and gas industry, the electric power industry, and the nuclear energy sector. Each has its own specific characteristics and challenges; however, cybersecurity and information protection are crucial for all of them [1–5].

One of the most effective methods for information protection today is steganographic techniques [6], including in the field of power systems [7, 35-37]. However, when used by hostile entities or terrorist groups—often the case nowadays [8]—for unauthorized acquisition of classified information, including data related to the energy sector [1], the role of steganalysis

becomes critical [6,9]. The key steganalysis tasks include:

1. Detecting the presence of hidden information within digital content (the primary objective);
2. Determining/assessing the Covert Communication Channel Bandwidth (CCCB);
3. Decoding the hidden information.

Most scientific efforts are directed toward detecting covert communication. However, steganalysis is most effective when all these tasks are addressed. The latter tasks, beyond detection, are significantly more complex both theoretically (mathematically) and in terms of practical implementation, and they currently lack satisfactory solutions [10]. This highlights the ongoing need to develop new and enhance existing steganalytical methods.

Digital Videos (DVs) and sets of Digital Images (DIs) are increasingly used as containers in steganographic systems. This trend is driven by several factors, including their high capacity, complex structure, and greater resistance to hidden communication detection compared to individual images, particularly in real-time scenarios. These advantages make DVs preferable to other carriers, such as individual images, text, or audio [11]. However, these same factors complicate both the steganographic embedding process and steganalysis. Although research in this field is ongoing [12], existing studies remain limited and do not fully address all challenges associated with using DVs in steganographic systems. Therefore, this study focuses on DVs and DI sets as steganographic containers.

The estimation of information transmitted through a steganographic communication channel is discussed in the scientific literature in various contexts, including the maximum allowable amount of Additional Information (AI), the evaluation of embedded message length, and the direct assessment of covert channel capacity.

The allowable volume of embedded information in a container [13] depends on both the steganographic algorithm used and the container's characteristics, such as size and format in the case of DIs and DVs [14,15]. At the same time, the probability of reliably perceiving a steganographic message, directly linked to the system's resistance to detection, decreases as the volume of AI increases [10]. It has been shown [16] that exceeding a certain threshold for embedded message size simplifies steganalytic detection. Moreover, the effectiveness of steganalytic methods largely depends on the CCCB value in covert communication. Many methods become ineffective when CCCB is low [17].

This has led to the adaptation of steganographic techniques for low CCCB conditions, such as the least significant bit (LSB) modification method [18]. Although this approach seemingly contradicts one of the core requirements of steganographic systems, namely ensuring significant CCCB, it effectively conceals the presence of additional information, which is the primary objective of covert communication. As a result, steganalysis under low CCCB conditions remains an open challenge.

The study of the total volume of securely transmitted information in a container of size N, where the container size corresponds to possible additional information embedding locations, is addressed in [15]. This work is significant as it presents a series of experiments demonstrating that, when other factors affecting the container (format, additional processing, etc.) are excluded, the amount of securely transmitted information (i.e., information that is unlikely to be detected) is proportional to the container size. This result, previously obtained for packet steganography [19], is important from a theoretical perspective. However, in practice, it does not provide a direct means of determining the CCCB value or the exact volume of transmitted additional information, which, considering modern steganographic techniques, can be significantly lower. Additionally, with the advancement of steganalysis, the concept of "secure information" has become highly dynamic. Moreover, since it is practically impossible to exclude all factors affecting the container except for size, even the obtained formula presents difficulties in practical use. For example, it remains unclear whether doubling the container size would necessarily lead to a proportional increase in the volume of securely transmitted information at an equivalent risk level.

An estimation of CCCB can evidently be derived from solving the problem of determining the embedded message size for a given container size. This issue is discussed for DIs in [20], where a neural network approach is proposed. The authors claim high accuracy for their method; however, all experiments were conducted on very small DIs (28×28 pixels) with a fixed vector of possible embedded message lengths. It is evident that with an increase in container size, the number of possible variations in embedded message length also grows, making practical implementation highly

challenging despite its theoretical significance in the proposed method.

A neural network approach is also considered in a method for estimating embedded message length in DIs [21], where 486 features are used for each image. However, the proposed algorithm is specifically designed for Lossy Image Formats (LIF), such as JPEG, leveraging intra-block and inter-block correlations characteristic of LIF. This significantly limits its applicability.

The direct determination of CCCB is addressed in [13], but the authors' approach, as well as their perspective on steganographic system security—defined as resistance to detection, effectively reducing it to the core problem of steganalysis—remains purely theoretical, lacking practical recommendations for CCCB evaluation.

Based on the conclusions from [16], a method for calculating the maximum covert channel capacity in steganographic communication systems is proposed in [22]. Despite the significance of this result, it only provides an upper bound for estimating the possible CCCB value without considering its actual value in a given steganographic system. A similar limitation applies to [23], which quantitatively evaluates the maximum CCCB at which data can be hidden and correctly decoded within a multimedia container subjected to attacks.

In [24], a steganalytic method for estimating CCCB is proposed, designed for a modified steganographic method introduced in [25], as well as for steganographic techniques that use pixel brightness differences for embedding additional information. This method is based on five different neural networks and is positioned by the authors as highly effective. However, it has a significant limitation: it is only applicable for CCCB values of at least 20%. Moreover, testing was conducted on a very limited number of DIs, calling into question the claimed effectiveness of 88%.

As can be observed, modern effective methods for estimating CCCB, embedded message length, and secure embedded information volume are increasingly based on neural networks. However, in the authors' opinion, such an approach cannot be considered a universal solution, as it inherently carries the traditional drawbacks and potential threats associated with neural networks. These include overfitting, anomaly detection issues in training datasets, and the difficulty of understanding how decisions are made. Additionally, artificial neural networks struggle to function effectively in dynamically changing environments, such as steganographic systems, as they cannot reliably "remember" past experiences. This limits the advantages of neural networks over other approaches in information security tasks.

It is important to note that most modern steganalytic methods experience a critical decline in effectiveness when CCCB≤25% [17, 25, 26]. Further, this assessment of covert channel capacity quantitatively defines low CCCB in this study.

Due to its complexity, video steganalysis is not frequently addressed in open sources, though research in this area is ongoing, and significant results have been achieved [27]. A common belief is that steganalytic methods for DIs can be easily adapted for video analysis, which is often attempted by researchers [12]. However, this assumption is not always valid [28]. Most attention in video steganalysis is focused on assessing the boundary of data volume that can be safely embedded in video signals [29].

Thus, open-source research on the analysis of DIs, DI sets, and DVs primarily emphasizes estimating the maximum possible volume of secure information and the maximum volume of embedded information that preserves the reliability of steganographic message perception [30]. However, the task of assessing the capacity of an actual covert channel remains underexplored. While the first two tasks are relevant for ensuring an effective steganographic transformation process, efficient steganalysis requires addressing the latter issue, which remains relevant and demands new, effective approaches—especially considering the rapid development of steganography today.

One of the most commonly used steganographic methods for covert channel organization remains the Least Significant Bit (LSB) method [18], due to its well-known advantages. Most existing steganalytic methods aim to detect its use. However, the specifics of its modern application—under low CCCB conditions—and the increasing use of digital video as a container keep the challenge of its steganalysis relevant.

The goal of this study is to develop a steganalytic method for estimating the covert channel capacity established using the LSB method in digital video or DI sets used as containers. The proposed method aims to be effective even under low CCCB conditions, regardless of whether the container format is lossy or lossless.

The focus on detecting the results of LSB-based steganographic transformation in this study is not solely due to its widespread use. Steganographic transformations using this method, as well as numerous other steganographic methods that are modifications of LSB result in minimal disturbances to the container. It can be assumed that a steganalytic method effective under such conditions has the potential for easy adaptation to other steganographic methods that introduce more significant distortions when embedding AI. This suggests the possibility of developing a universal steganalytic method based on this approach.

METHODS, RESULTS AND DISCUSSION

In 2024 and 2025, a series of articles by the authors of this study were published in this scientific journal, focusing on the development of a General Approach to analyzing the state of information systems. This approach is based on perturbation theory and matrix analysis, with one of its applications being the integrity assessment of digital content, a special case of which is steganalysis.

Let F be an $n\times n$-matrix representing a digital image or a video frame. According to General Approach, any transformation of a DI or DV, including steganographic transformation, can formally be represented as: $\overline{F} = F + \Delta F$, where $\overline{F}$, ΔF is an n×n matrix representing the perturbed content, and Perturbing Impact (PI), respectively. The consequence of this is the possibility of formally representing the results of the PI, in particular the results of the introduction of the PI into the container F, as a set of disturbances of Singular Numbers (SN) and Singular Vectors (SV), uniquely determined for F, while it does not matter in which region of the container (spatial, transformation region) the steganotransformation occurred. The uniqueness of the resulting SN, SV can be ensured by calculating them by constructing a normal singular decomposition of the matrix [31]: $F = U\Sigma V^T$, where U and V are orthogonal $n\times n$-matrices, whose columns $u_i, v_i, i = \overline{1,n}$ are the left and right singular vectors, respectively, and $\Sigma = diag\left(\sigma_1(F),..., \sigma_n(F)\right)$, $\sigma_1(F) \geq ... \geq \sigma_n(F) \geq 0$ - contains the singular values of F.

The authors have previously studied the properties of the discrete function $y(\sigma_i, \Delta F) = \Delta\sigma_i$, which describes the dependence of the perturbation of the singular values $\Delta\sigma_i = |\sigma_i(F) - \sigma_i(F + \Delta F)|$ of the DI/DV matrix on its index due to PI ΔF. Differences in the properties of $y(\sigma_i, \Delta F)$ for original and non-original content were established:

- Starting from a certain index *i,* the function $y(\sigma_i, \Delta F)$ becomes monotonically decreasing (in terms of trend), defining the stabilization region of SNs for an original DI/DV.
- If the content integrity is violated, such that the magnitude of the secondary PI is smaller than that of the primary PI, the monotonicity of the trend in $y(\sigma_i, \Delta F)$ is disrupted in the right part of the singular spectrum.

These theoretical findings are general, independent of the specifics of PI, and can be applied to the development of methods for digital content integrity assessment.

The authors have previously substantiated the fundamental possibility of estimating the strength of the applied PI within this approach by analyzing the properties of $y(\sigma_i, \Delta F)$. Based on this, the process of estimating the CCCB for a steganographic message container can be divided into the following steps:

1. The investigated DI/DV undergoes multiple (iterative) steganographic transformations with varying CCCB values, followed by the construction of the function $y(\sigma_i, \Delta F)$.
2. Two CCCB values are determined: one at which the trend $y(\sigma_i, \Delta F)$ has not yet reached a stabilization region, and another at which this region is restored. These values will serve as the lower and upper bounds for the estimated CCCB.

The previously obtained conclusions are qualitative in nature. To utilize them in the development of a practical CCCB estimation method, the following tasks need to be addressed:

- Justify the selection of a specific method for constructing the approximating function for $y(\sigma_i, \Delta F)$.
- Define the formal conditions for the destruction of the stabilization region of SNs.

It is well known that trends can be described by various functions: linear, power-law, logarithmic, etc. or determined using an averaging

function. It is evident that, in practical applications, the choice of trend modeling method will influence the final result. Given the nature of the problem under consideration, the primary focus should be on the overall tendency of $y(\sigma_i, \Delta F)$ rather than its specific values.

It should be noted that directly using $y(\sigma_i, \Delta F)$ to distinguish original content from non-original content may present difficulties. This issue is illustrated in Figure 1(a) for a specific DI, where slight deviations from strict monotonicity in the right part of the singular spectrum still occur due to the perturbation of the original DI. However, for non-original DI, the violation of monotonicity in the right part of the spectrum is evident (Figure 1(b)). Insufficient consideration of this possible scenario for original content may lead to Type II errors, where original content is mistakenly classified as a steganographic message.

Let us denote $s(i)$ – an approximating function for $y(\sigma_i, \Delta F)$ in a certain sense. Let us consider possible options for constructing $s(i)$. In mathematics, an approximating function is used as an approximating function $y(\sigma_i, \Delta F)$ for a discrete function, such as , the construction of which is determined by the conditions and purpose of the approximation. Thus, the approximating function can be interpolating, the condition for which is the coincidence of the values in the existing nodes of the approximated function: $s(i) = y(\sigma_i, \Delta F)$ for $\forall i$; can be selected from a given class of functions (for example, polynomials) as a solution to the least squares problem; can be selected by satisfying the condition of uniform approximation: $|s(i) - y(\sigma_i, \Delta F)| < \varepsilon$, where ε is the value of the permissible deviation [32].

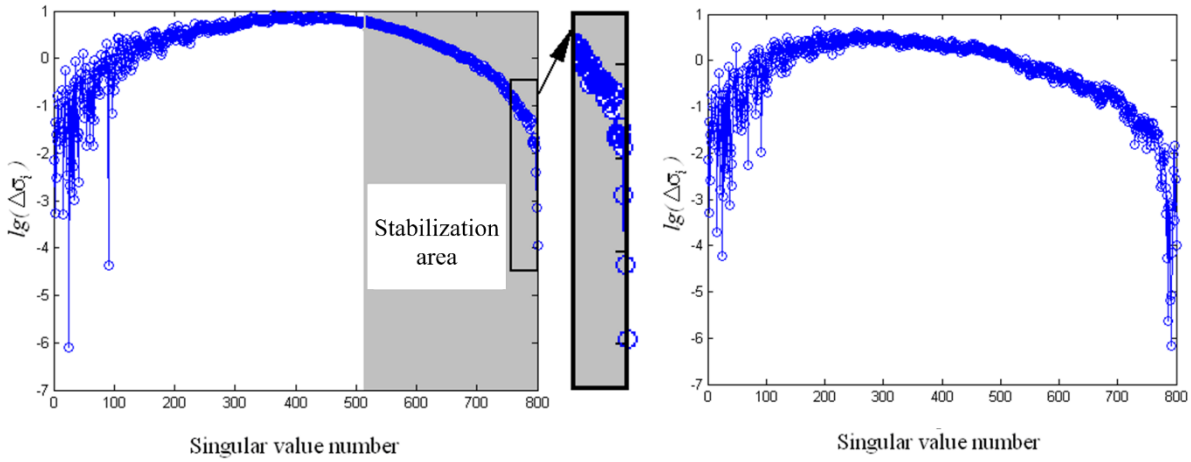
Given the above considerations, the approximating function for $y(\sigma_i, \Delta F)$ cannot be a "classical" interpolating function, i.e., one constructed using all nodes of $y(\sigma_i, \Delta F)$. This is because the previously mentioned issue of minor deviations from monotonicity in the right part of the singular spectrum for original content would persist. This is illustrated in Figure 1, where the graphs $y(\sigma_i, \Delta F)$ correspond to first-degree interpolation splines.

An alternative approach to constructing the interpolating function $s(i)$, considering the purpose of it $y(\sigma_i, \Delta F)$, could involve using only some of the nodes instead of all of them. In this case, in the right part of the spectrum of an original DI/DV, the goal of "smoothing out" minor monotonicity violations would lead to the removal of those nodes that introduce non-monotonicity; whereas for non-original content, the opposite selection criterion would be applied. However, since a steganalyst typically has access only to the content under examination, using an interpolating function as a formal research tool in this context becomes highly impractical.

Other possible approximation methods for $y(\sigma_i, \Delta F)$ impose a requirement for minimal deviation between the approximated and approximating function, which can be expressed in different formal ways, as noted earlier. However, such "closeness" is not required for solving the given problem. The key aspect here is preserving the overall trend of the function's behavior in terms of the presence or absence of conditional monotonicity in the right part of the singular spectrum. Therefore, it is fundamentally possible to abandon the requirement that must be close $s(i)$ to $y(\sigma_i, \Delta F)$ by any specific criterion. Moreover, imposing a "closeness" requirement in any formal expression would complicate the elimination of minor deviations from monotonicity in the right part of the spectrum for an original DI/DV.

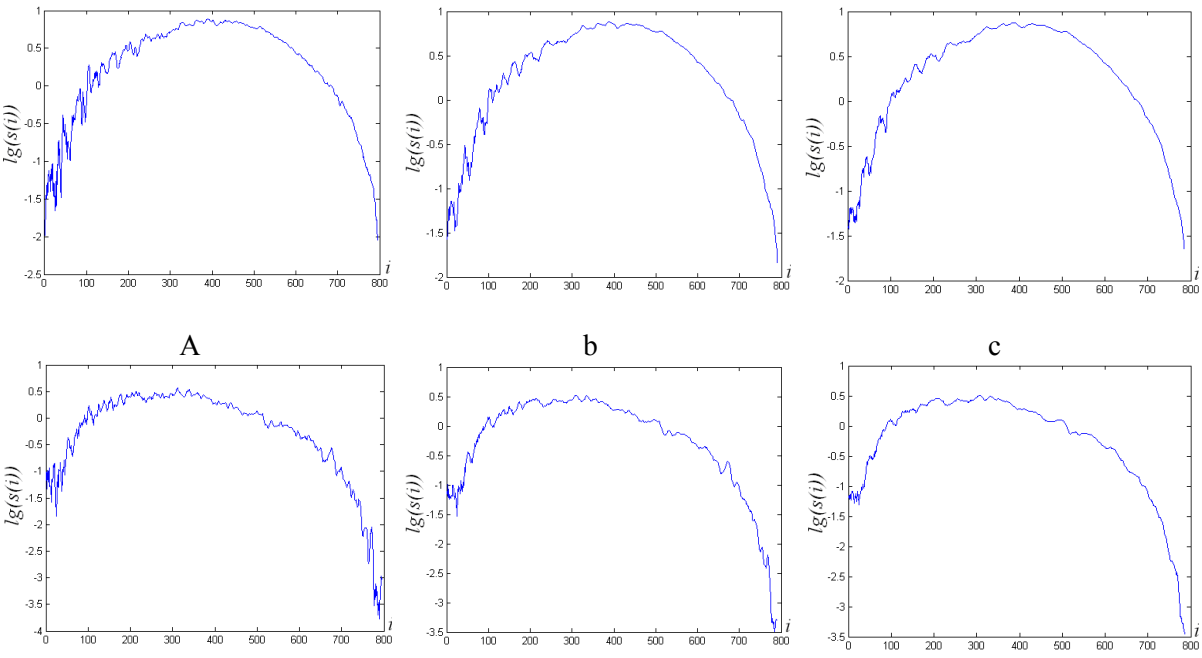
The need for the function $s(i)$ to smooth out minor monotonicity violations in $y(\sigma_i, \Delta F)$ for original content while ensuring that non-monotonicity remains apparent for non-original content in the right part of the singular spectrum makes it reasonable to use an averaging function as $s(i)$. The degree of smoothing would be determined or adjusted by the number i_0 of nodes $y(\sigma_i, \Delta F)$ used for averaging. When selecting i_0 for constructing $s(i)$, the following factors must be taken into account: small i_0 may not adequately smooth $y(\sigma_i, \Delta F)$ for original DI/DVs; a large i_0 may excessively smooth $y(\sigma_i, \Delta F)$ for non-original DI/DVs. This is illustrated in Figure 2 for a specific DI: here, $i_0 = 15$ provides an "ideal" result for original content (Figure 2(c)), but under the same i_0, monotonicity is also smoothed out for non-original content (Figure 2(f)); whereas for $i_0 = 5$, the effect is reversed.

As a result of a computational experiment involving 400 DIs from the database [33], 400 DIs from the database [34], and 100 DIs captured using non-professional video cameras, the "compromise" value of $i_0 = 10$.



a b

Fig. 1. Graphs of the function for steganization by the LSB method with CCCB=10%, when the original DI is: a – original in a lossless format; b – a steganization message obtained by the LSB method with CCCB=50%.



A b c

D e f

Figure 2. Graphs of the Averaging Function $s(i)$ for $y(\sigma_i, \Delta F)$: (a, b, c) – Original DI under perturbation (steganographic transformation) with CCCB = 10% (Figure 1(a)), respectively; (d, e, f) – Steganographic message obtained with CCCB = 50% under secondary perturbation (steganographic transformation) with CCCB = 10%, respectively (Figure 1(b)).

Given that the value $i_0 = 10$ is a "compromise", it is possible that for the original DI/frame of the DV, strict monotony $s(i)$ in the right part of the singular spectrum will still be violated. This means that for organizing a formal search for the stabilization zone SV, the condition is sufficient $s(k) \le s(k-1)$, but not necessary. Taking this into account $\Delta\sigma_k$, the condition for

entering the SV stabilization region will be determined as follows:

$$\begin{cases} s(k) \le s(k-1), \\ 0 < s(k) - s(k-1) < \varepsilon, \end{cases} \quad (1)$$

where $\varepsilon > 0$ is a parameter determined empirically during the development of the algorithmic implementation of the method proposed below. Then the formal condition for the violation of monotonicity $s(i)$ obtained from (1) will be:

$$s(k) - s(k-1) \ge \varepsilon . \quad (2)$$

Previously, the authors showed that in the case of non-original DI, the destruction of monotony $s(i)$ regardless of the specifics of the DI, it is guaranteed to occur when the value of the repeated PI is less than the primary one, in the region of the singular spectrum at $i \to n$. Due to this, the organization of the search for a violation of monotony $s(i)$ it makes sense to carry out in reverse order, starting from the largest value $i = n$ to $i = 1$. This will make it possible to significantly reduce the computational complexity of the method being formed. Under these conditions, we denote by T – the largest number of the VLF such that for $s(T), s(T-1)$ condition (2) is satisfied. It is obvious that for the sequence of original DI (frames of the original DV) the spread of values T for the same explosive (the same CCCB) in general it can be quite large: for DI/frame DV, the greater part of which corresponds to minor differences in pixel brightness values, i.e. has an insignificant high-frequency component, T will be less important than for content that contains multiple areas with significant differences in brightness values.

In accordance with the theoretical results obtained earlier, regardless of the type of explosive T for original digital image processing/frame digital image processing with matrix F in primary PI $(\Delta F)_0$ will be less than for the corresponding non-original one with the matrix $\overline{F} = F + (\Delta F)_1$, i.e. one that has suffered a breach of integrity due to $(\Delta F)_1$, after which they were subjected to secondary explosives $(\Delta F)_0$. It should be noted that the increase in value T for non-original DI/frame DV, compared to the corresponding original ones, with a high probability will lead to the fact that for a large number of disturbed DI the values T will be comparable, and the overall spread of these values will be no greater than for the original, regardless of the type of explosive, and therefore in the case of steganotransformation, which can be used to solve the main problem of steganalysis.

Thus, to implement the 2nd step of the process of assessing the strength of the used PV - the value of the CCCB within the framework of the approach under consideration, it makes sense to record the moment of a relatively large difference in the values of T corresponding to different CCCBs used in the examination process (hereinafter, such CCCBs and the corresponding PV will be called expert): when the CCCB used in the examination is less than the real one, the DI/frame of the PV behaves like non-original content; when the expert CCCB is greater than the desired one, its behavior is comparable to the behavior of the original content. As the desired interval containing the CCCB of the analyzed DI/frame of the PV, which is further designated k_0, can be used $\left\lfloor \underline{k}, \underline{\underline{k}} \right\rfloor$, where $\underline{k}$, $\underline{\underline{k}}$ - values of expert CCCBs that correspond $maxT / minT$ respectively. However, this gap can be very significant in size (Fig. 3(a)), and the values $minT$ and $maxT$ may differ in absolute value only slightly from the existing values in the resulting population T with various expert CCCBs, which will also qualitatively determine the difference between the values T. An illustration of this is shown in Fig. 3(a) for the lossless format (LFF) digital signal, where $\left\lfloor \underline{k}, \underline{\underline{k}} \right\rfloor = [10,50]$, it is obvious that the right boundary of the segment can be significantly refined due to a small difference in values T at CCCB=35,40,45,50% from $minT$, determined by the CCCB=50%. A similar picture takes place for the frame of the CV in the LIF in Fig. 3(b), where the refinements obviously affect both boundaries of the segment $\left\lfloor \underline{k}, \underline{\underline{k}} \right\rfloor$. Dependency graphs T from the value of the expert CCCB can differ significantly (compare Fig. 3(a) – the "ideal" option, corresponding to theoretical expectations, and Fig. 3(c)), the quantitative spread of values T may be relatively small (Fig. 3(b)) or relatively large (Fig. 3(g)), but the qualitative characteristics are preserved: a sharp drop in the value of T before and after the expert CCCB passes the desired value k_0. Thus, the key role here is played by the nature of the behavior,

and not the absolute values of the dependence function *T* from the value of the expert CCCB.

METHOD FOR ESTIMATING OF CCCB VALUE AND ITS ALGORITHMIC IMPLEMENTATION

Let the content that is a digital medium containing *m* frames, or a package of *m* DI, while this content is a stegano message formed by the LSB method with CCCB = k_0.

The main steps of the steganalytic method for estimating the value of the CCCB in the DI/set of DI are as follows.

Step 1. *Application of expert explosives*. For every *r*-frame of digital video/digital image with matrix *F*, $r = \overline{1,m}$:

1.1. Perform stegano transformation with CCCB= $k_1, k_2, ..., k_l$, $k_i \neq k_j$ at $i \neq j$, to be clear: $k_1 < k_2 < ... < k_l$. Result: digital contents with matrices $F_1, F_2, ..., F_l$ respectively;

1.2. For $\forall t = \overline{1,l}$:

1.2.1. For a couple F, F_t build $y^{(t)}(\sigma_i, \Delta F) = \Delta\sigma_i$ - the function of the dependence of the disturbance of the VLF on its number;

1.2.2. For $y^{(t)}(\sigma_i, \Delta F)$ construct an averaging function $s^{(t)}(i)$;

1.2.3. For $s^{(t)}(i)$ define $T^{(t)}$ – the number of the first from the end of the VLF for which condition (2) is satisfied.

1.3. Define: $\overline{k} \in \{k_1, k_2, ..., k_l\}$ - the meaning of the CCCB, which corresponds to $T_{max} = \max\limits_t T^{(t)}$; $\overline{\overline{k}} \in \{k_1, k_2, ..., k_l\}$ - the meaning of the CCCB, which corresponds to $T_{min} = \min\limits_t T^{(t)}$. Result: $k_0 \in \left[\overline{k}, \overline{\overline{k}}\right]$.

1.4. Clarification of the boundaries of the interval containing the value of the desired CCCB:

1.4.1. Clarification of the lower limit, which is designated as $k_{min}^{(r)}$:

among $k_j > \overline{k}$, $k_j \in \{k_1, k_2, ..., k_l\}$, find such k_{j_i}, to $\left(\left|T^{(k_{j_i})} - T_{max}\right| \leq P\right) \& \left(k_{j_i} < \overline{\overline{k}}\right)$. Then $k_{min}^{(r)} = \min k_{j_i}$.

1.4.2. Clarification of the upper limit, which is designated as $k_{max}^{(r)}$:

among $k_j < \overline{\overline{k}}$, $k_j \in \{k_1, k_2, ..., k_l\}$, find such k_{j_i}, to $\left(\left|T^{(k_{j_i})} - T_{min}\right| \leq P\right) \& \left(k_{j_i} > \overline{k}\right)$. Then $k_{max}^{(r)} = \max k_{j_i}$.

Here and in step 1.4.1 *P* – a parameter that is determined during the construction of the algorithmic implementation of the method.

1.4.3. Result: $k_0 \in \left[k_{min}^{(r)}, k_{max}^{(r)}\right]$.

Step 2. Based on the set of results obtained in step 1: $k_0 \in \left[k_{min}^{(r)}, k_{max}^{(r)}\right]$, $r = \overline{1,m}$, determine the number of hits *K* each of the possible values of the CCCB from $[k_1, k_l]$ в $\bigcup_{r=1}^{m} \left[k_{min}^{(r)}, k_{max}^{(r)}\right]$.

Step 3. Determine the two largest values *K*. The minimum/maximum of these will give k_{min} / k_{max} respectively, the interval containing the desired value k_0. The final result: $k_0 \in [k_{min}, k_{max}]$.

For the algorithmic implementation of the method, the following parameter values were used: $\varepsilon = 0.009$, P=50 (for LLF), P=25 (for LIF), established experimentally. Visual difference of the parameter P for contents in LIF and LLF is illustrated by Fig. 3 (compare Fig. 3(a, b) and Fig. 3(c, d)). The values determined for the parameters correspond to $i_0 = 10$ – number of function nodes $y^{(t)}(\sigma_i, \Delta F)$, used in construction $s(i)$.

The developed algorithm was tested under conditions of steganotransformation using the LSB method with CCCB<50%, including with small CCCB≤25%. The experiment involved 35 original digital contents – digital video and digital video sequences, the number of frames/digital video in which initially ranged from 320 to 1000 units. The digital video was obtained by several video cameras (Olympus SP-820 – CMOS, 14MP; Nikon COOLPIX P100 – CMOS, 10MP; Canon PowerShot A520 – CCD, 4MP); a mobile phone video camera Realme 7 pro (64 MP, f/1.8, 26mm (wide), 1/1.73", 0.8µm, PDAF)); The DIs were taken from the database [33]. The containers were formed as subsequences of the above-described sequences of frames/CIs of different lengths. $r \geq 100$. The total number of original

containers of different lengths was 100. For each of the containers, steganomessages were formed using the LSB-matching method [18], where the CCCB for the TS/TS frame was taken as 16, 25, 38%. The total number of stegano messages was 300. The stegano transformations were taken as expert ones with CCCB from 5 to 50% with constant pitch h=5%. The values of the CCCB when forming stegano messages were deliberately chosen so that among them there were both those that do not coincide with the expert CCCB, and one that coincides with one of the expert ones.

Typical results of the proposed algorithm for clarity in the form of graphs of the dependence of K on the CCCB are shown in Fig. 4 for a specific DI package and a specific CV. Here, as in all other cases of tested stegano messages, the obtained intervals $[k_{min}, k_{max}]$ (in Fig. 4 they are highlighted with bold lines), the length of which was equal to h, contained the desired value k_0.

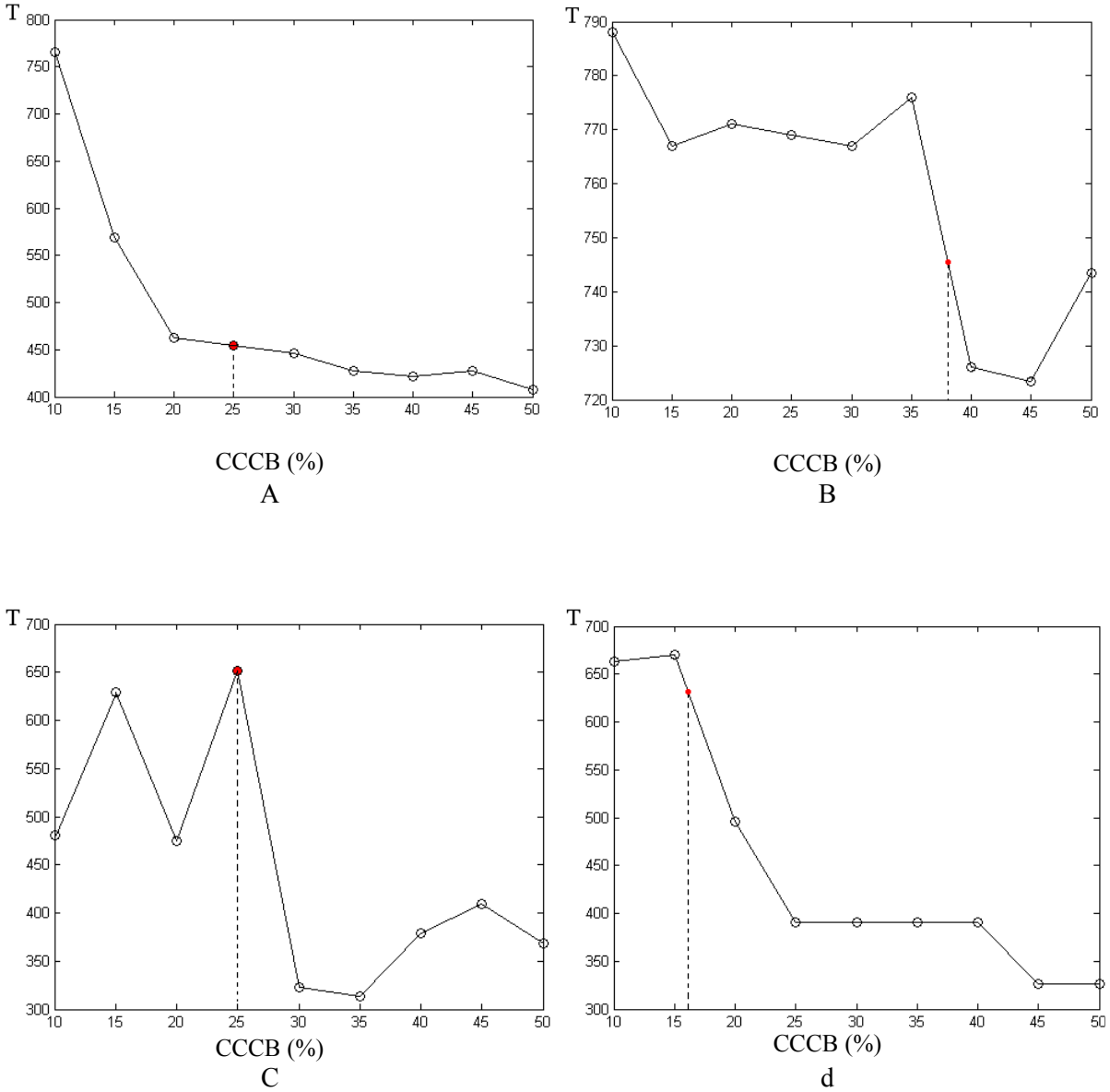


Fig. 3. Examples of graphs of the dependence of *T* on the value of expert CCCB for specific DI/frames of the DV: a – frame of the DV (in LIF), in which the DI with CCCB=25% is embedded; b – frame of the DV (in LIF), in which the DI with CCCB=38% is embedded; c – DI (LLF) with CCCB of 25%; d – DI (LLF) with CCCB of 16%.

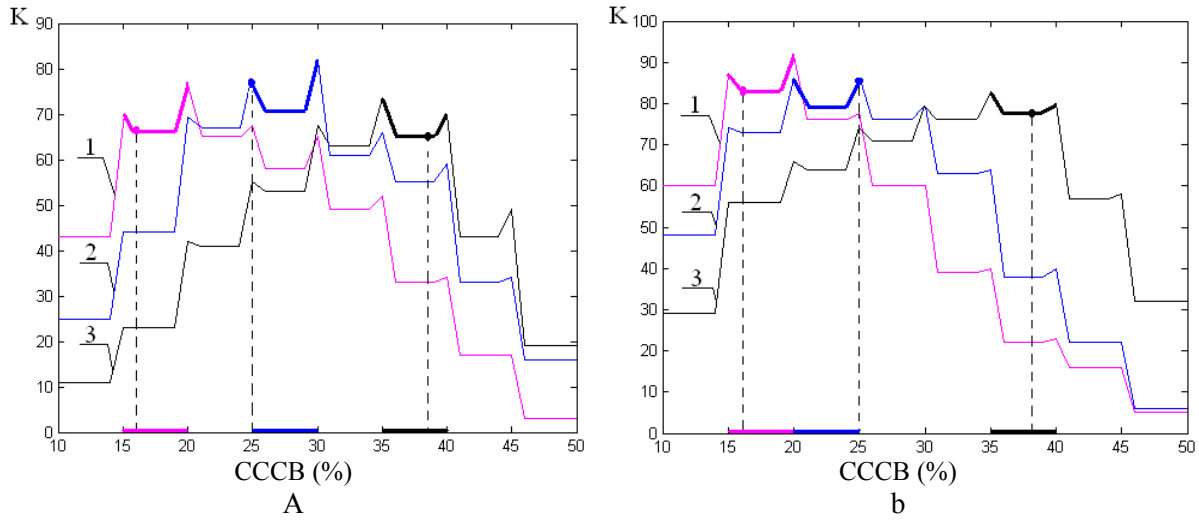


Fig. 4. Frequency *K* of CCCB Values for: a – a Digital Image Package in Lossless Format (100 Images); b – Video Content in Lossy Format (100 Frames): 1, 2, 3 – Stego Message with CCCB=16%, 25%, 38%, respectively.

Based on the theoretical foundations of the developed method, it is possible to use impacts other than steganotransformation as expert PIs during its operation, which expands the expert's capabilities in practice. It is important here that the set of expert PIs contains both those whose magnitude, formally expressed as $\|\Delta F\|$, where $\|\cdot\|$ - the matrix norm, would be greater, and those for which $\|\Delta F\|$ would be less than the magnitude of the perturbing effect corresponding to the steganotransformation performed. An illustration of this statement is Fig. 5, where the result of step 2 of the developed method is presented by a graphical dependence K from the magnitude of the dispersion *d* Gaussian noise with zero mathematical expectation, used as an expert PI instead of a steganotransform, with the variance selected from the set $D = \{d | d = 10^{-6} \cdot i, i = \overline{1,9}\}$, which allowed us to create a set of the required explosives to estimate the value of the desired explosive – a steganotransformation with a small CCCB=18%. The correspondence between the average value $\|\Delta F\|$ and the noise dispersion is presented in Table 1. Such insignificant dispersions for expert PI were chosen taking into account that the value of PI, which is the result of steganotransformation by the LSB method, is very small: for CCCB=18% value $\|\Delta F\| \approx 23.8$. As a result of the method, the interval corresponding to the sought-after CCCB, the length of which is equal to the step of the variance change, is determined correctly (see Table 1). The graphs of the dependence of T on d, the typical form of which for a specific DI and a specific DV frame are presented in Fig. 6, fully correspond to theoretical expectations and do not differ qualitatively from the variant when steganotransformations with different CCCB were used as expert PI (compare Fig. 6 and Fig. 3): the sought-after PI value for the content subject to examination is in the zone of the function jump $T(d)$.

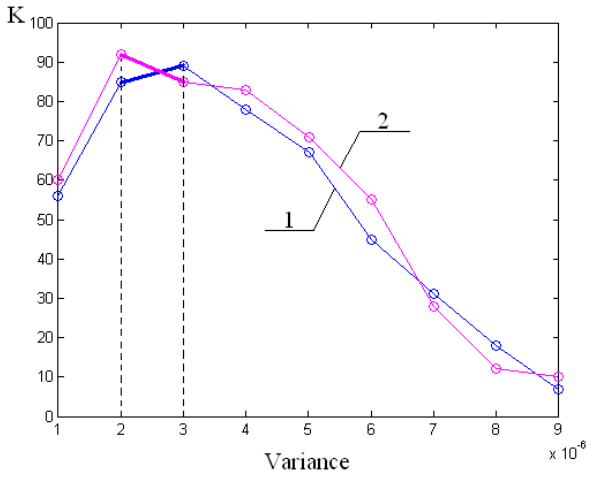


Fig. 5. Frequency *K* of Different Variance Values of Gaussian Noise Used in the Examination of a Stego Message with PSCC=18% for: 1 – a Sequence of 100 Digital Images in LLF; 2 – Video Content of 100 Frames in LIF.

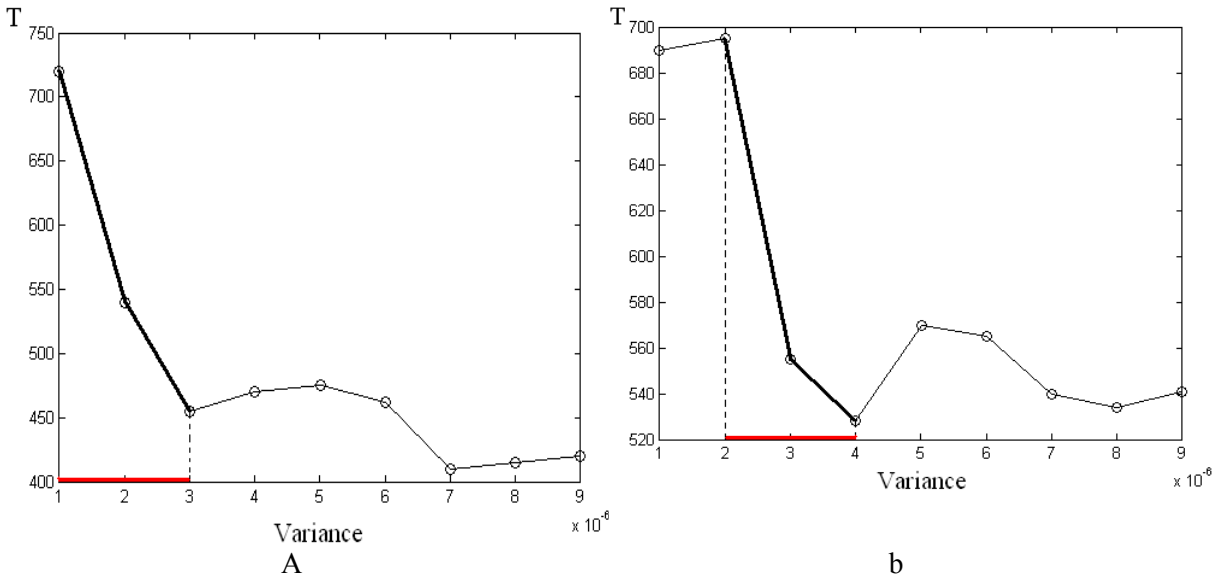
In Fig. 6, the areas that are highlighted by the algorithm are marked with bold lines. The possibility of using several different types of expert PI is a significant advantage of the proposed method: this can serve to clarify/confirm the results obtained initially, in addition, the choice of the step for the values of expert PIs other than the steganotransformation, for example, Gaussian noise, and the starting point here can be more flexible than in the steganotransformation, where the CCCB can only take a finite fixed set of values, the power of which is maximum equal to 100, which is not typical of Gaussian noise. The idea of dynamically changing the step values for a set of expert PIs is currently being investigated by the authors of this paper for the possibility of improving the proposed method.

The developed method provides an absolute result when evaluating the CCCB: throughout the entire computational experiment, there was no situation where the interval determined by the algorithm did not contain the true value of the applied CCCB. The interval can be refined by reducing the step size *h* and, consequently, increasing the number of expert PIs. However, from a practical standpoint, a significant increase in the number of expert PIs is not advisable: constructing the function $y^{(t)}(\sigma_i, \Delta F)$ describing the dependence of the SN DI/frame DI perturbation on its number at step 1.2.1 for each pair F, F_t requires finding these SNs for F, F_t $t = \overline{1,l}$. Singular value decompositions (SN) of the corresponding matrices are recommended for this operation, as using iterative methods to compute the singular spectrum here is undesirable because it would introduce additional methodological error into the total SN error. However, the developed steganalytical method is sensitive to errors in the SN when detecting the fact of monotonicity $s(i)$ violation or its absence. Singular value decomposition does not introduce methodological error but is computationally relatively expensive: for an *n*×*n*-matrix, it requires $O(n^3)$ operations. For the analysis of one or a small number of DIs, this does not pose a problem, but for analyzing CVs containing a large number of frames, increasing the number of expert PIs may lead to significant time costs, which is clearly undesirable.

Table 1

Correspondence Between the Variance *d* of Gaussian Noise with Zero Mean and the Average Disturbance Magnitude of Digital Content of Size 800×800 Resulting from Noise Application

d	10^{-6}	$2\cdot10^{-6}$	$3\cdot10^{-6}$	$4\cdot10^{-6}$	$5\cdot10^{-6}$	$6\cdot10^{-6}$	$7\cdot10^{-6}$	$8\cdot10^{-6}$	$9\cdot10^{-6}$
$\|\Delta F\|$	12.5	22.5	28	32	35.5	38.5	41.5	43.5	46



A b

Fig. 6. Examples of Graphs Showing the Dependence of *T* on *d* for Digital Content Embedded with Hidden Information at CCCB=18%: (a) Digital Image (in LLF); (b) Video Frame (in LIF).

CONCLUSION

This work, based on an improved general approach to analyzing the state of information protection systems grounded in perturbation theory and matrix analysis, proposes a steganalytical method for estimating the capacity of a Steganographic Communication Channel (SCC) organized using the LSB method. In this case, Digital Video (DV) or a set of Digital Images (DI) is used as the container.

The new method has no restrictions on the format (lossy/lossless) of the container used, and it provides a positive result within the framework of its proposed algorithmic implementation – the determined intervals of small length always contain the true value of the SCC, including in cases of low SCC.

The proposed method can use expert perturbing impacts, different from steganographic transformations, to detect the presence of embedded information. This provides flexibility and wide applicability. The main theoretical idea used here is general: the behavior of a stego message (non-original content) under external impacts will mainly depend on the magnitude of the impact rather than its specific type.

Thus, the diversity of characteristics of an infinite number of perturbing effects can be reduced primarily to one characteristic – its magnitude, which, in the case of the matrix representation of perturbing impacts, is defined by its norm.

This fundamental idea can be applied in organizing steganalysis even when neural networks are used during their training. It also indicates the potential for adapting the developed steganalytical method to estimate the magnitude of perturbing impacts different from steganographic transformation, which the authors are currently working on.

If successful, such adaptation will lead, in particular, to a universal steganalytical method, allowing the expert to conduct effective steganalysis without relying on the presence or absence of prior information about the specifics of the steganographic method used to organize the covert communication channel.

References

[1] Saeed S. et al. Digital transformation in energy sector: Cybersecurity challenges and implications. *Information*, 2024, vol. 15, no. 12, 764.

[2] Pettersen S., Grøtan T.O. Exploring the grounds for cyber resilience in the hyper-connected oil and gas industry. *Safety Science*, 2024, vol. 171, 106384.

[3] Patel S. Cybersecurity in electric distribution: The one weak link in an interconnected power grid and the threat it poses. *The George Washington Journal of Energy and Environmental Law*, 2023, vol. 14, no. 2, pp. 138–152.

[4] Bobok I., Kobozeva A., Maksymov M., Maksymova O. Checking the Integrity of CCTV Footage in Real Time at Nuclear Facilities. *Nuclear & Radiation Safety*, 2016, no. 2, pp. 68–72.

[5] Petrivskyi V. et al. Development of a modification of the method for constructing energy-efficient sensor networks using static and dynamic sensors. *Eastern-European Journal of Enterprise Technologies*, 2022, vol. 1, no. 9, pp. 15–23.

[6] Fridrich J. *Steganography in Digital Media: Principles, Algorithms, and Applications*. Cambridge University Press, 2009.

[7] Kumar, A., & Raghava, N. S. (2019). *Chaos-based steganography technique to secure information and integrity preservation of smart grid readings using wavelet. International Journal of Computers and Applications, 1–7.* doi:10.1080/1206212x.2019.1692511

[8] CyberSecureFox. *Advanced steganography techniques emerge in targeted cyberattacks by PhaseShifters Group*. Available at: https://cybersecurefox.com/en/phaseshipters-steganography-cyberattacks-eastern-europe/ (accessed 26.12.2024).

[9] Dumitrescu S., Wu X., Wang Z. Detection of LSB steganography via sample pair analysis. *IEEE Transactions on Signal Processing*, 2003, vol. 51, no. 7, pp. 1995-2007. doi: 10.1109/TSP.2003.812753.

[10] Kusnetsov O., Evseev S., Korol O. *Steganography*. Kharkiv: KhNEU, 2011. 232 p.

[11] Kunhoth J., Subramanian N., Al-Maadeed S., Bouridane A. Video steganography: recent advances and challenges. *Multimedia Tools and Applications*, 2023, vol. 82, pp. 41943–41985.

[12] Kobozieva A., Bobok I., Kushnirenko N. Steganalysis method for detecting LSB embedding in digital video, digital image sequence. *Proceedings of the 11th Information Control Systems & Technologies (ICST-2023)*. Odesa, Ukraine, 2023. P. 78–90.

[13] Chandramouli R., Memon N.D. Steganography capacity: a steganalysis perspective. *Proc. SPIE 5020, Security and Watermarking of Multimedia*

Contents V, (20 June 2003); https://doi.org/10.1117/12.479732

[14] Kobozeva A.A., Alfaludji S. The basis of new approach of providing high carrying capacity of covert communication channel. *Proceedings of International Conference on Modern Problem of Radio Engineering, Telecommunications and Computer Science*. Lviv, Ukraine, 2012. P. 263.

[15] Ker A.D., Pevný T., Kodovský J., Fridrich J. The square root law of steganographic capacity. *Proceedings of the 10th ACM Workshop on Multimedia and Security (MM&Sec '08)*. Oxford, UK, 2008. P. 107–116.

[16] Chandramouli R., Memon N. Analysis of LSB based image steganography techniques. *Proceedings of the 2001 International Conference on Image Processing (Cat. No.01CH37205)*. Thessaloniki, Greece, 2001. P. 1019–1022.

[17] Al-Jarrah M.M, Al-Taie Z.H., Abuarqoub A. Steganalysis using LSB-focused statistical features. *Proceedings of the International Conference on Future Networks and Distributed Systems (ICFNDS '17)*. Cambridge, United Kingdom, 2017. Article 54. P. 1–5.

[18] Aslam M.A. et al. Image Steganography using Least Significant Bit (LSB) – A Systematic Literature Review. *Proceedings of the 2022 2nd International Conference on Computing and Information Technology (ICCIT)*. Tabuk, Saudi Arabia, 2022. P. 32–38.

[19] Ker A.D. Batch steganography and pooled steganalysis. *Proceedings of the 8th International Conference on Information Hiding (IH '06)*. Alexandria, USA, 2006. P. 265–281.

[20] Gomis F.K., Bouwmans T., Camara M.S., Diop I. Estimation of the hidden message length in steganography: A deep learning approach. *Proceedings of the Machine Learning for Networking: Second IFIP TC 6 International Conference (MLN 2019)*. Paris, France, 2019. P. 333–341.

[21] Gomis F.K. et al. Multiple linear regression for universal steganalysis of images. *Proceedings of the 3rd International Conference on Intelligent Systems and Computer Vision (ISCV2018)*. Fez, Morocco, 2018. P. 1–4.

[22] Ibrahimov B.G., Tahirova K.M. Method for calculation maximum throughput hidden channels in systems of steganographic communications. *T-Comm*, 2022, vol. 16, no. 9, pp. 40–45.

[23] Sarkar A., Sullivan K., Manjunath B.S. Steganographic capacity estimation for the statistical restoration framework. *Proc. SPIE 6819, Security, Forensics, Steganography, and Watermarking of Multimedia Contents X*, 681916 (18 March 2008); https://doi.org/10.1117/12.767841

[24] Sabeti V., Samavi S., Mahdavi M., Shirani S. Steganalysis and payload estimation of embedding in pixel differences using neural networks. *Pattern Recognition*, 2010, vol. 43, no. 1, pp. 405–415.

[25] Wu D.-C., Tsai W.-H. A steganographic method for images by pixel-value differencing. *Pattern Recognition Letters*, 2003, vol. 24, no. 9-10, pp. 1613–1626.

[26] Natarajan V., Anitha R. Universal steganalysis using contourlet transform. *Proceedings of the 2nd International Conference on Computer Science, Engineering and Applications (ICCSEA 2012)*. New Delhi, India, 2012. Vol. 2, p. 727–735.

[27] Bouzegza M., Belatreche A., Bouridane A., Tounsi M. A comprehensive review of video steganalysis. *IET Image Processing*, 2022, vol. 16, no. 13, pp. 3407–3425.

[28] Tasdemir K., Kurugollu F., Sezer S. Spatio-Temporal rich model-based video steganalysis on cross sections of motion vector planes. *IEEE Transactions on Image Processing*, 2016, vol. 25, no. 7, pp. 3316–3328.

[29] Khalilian H., Ghaemmaghami S. Estimation of data hiding capacity of digital video based on human visual model in temporal domain. *Proceedings of the 2008 2nd International Conference on Signal Processing and Communication Systems*. Gold Coast, Australia, 2008. P. 1–4.

[30] Ghouti L. Estimation of data hiding capacities in Spatio-Chromatic Fourier Transform (SCFT) representations of color images. *Arabian Journal for Science and Engineering*, 2019, vol. 44, pp. 3699–3718.

[31] Bergman C., Davidson J. Unitary embedding for data hiding with the SVD. Available at: https://dr.lib.iastate.edu/entities/publication/bb2b5041-1c92-4ff5-b7f4-ff73c3483eed (accessed 23.09.2022)

[32] Gupta R.K. *Numerical Methods: Fundamentals and Applications*. Cambridge University Press, 2019. 824 p.

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

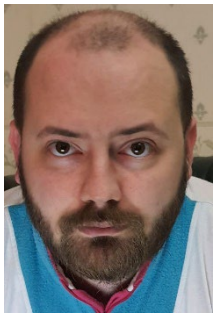
[34] NRCS Photo Gallery. United States Department of Agriculture. Washington, USA. Available at: https://www.nrcs.usda.gov/ (accessed: 26.07.2012).

[35] Xiao-Guang Zhang, Guang-Hong Yang, Ren Xiu-Xiu. Network steganography based security framework for cyber-physical system Information Sciences, 2022. № 609, p. 963-983.

[36] Abuadbba, A. Wavelet based steganographic technique to protect household confidential information and seal the transmitted smart grid

readings Information Systems, 2015, № 53. p. 224-236.
[37] Qasim O., Golshannavaz S. Data protection enhancement in smart grid communication: An efficient multi-layer encrypting approach based on chaotic techniques and steganography Advances in Electrical Engineering, Electronics and Energy. 2024.№ 10.p. 2-9.

Information about authors.



Ivan Bobok
Doctor of Technical Science, Professor of Department of Computerized Systems and Software Technologies. Odesa Polytechnic National University
Research interests: Steganography, Steganoanalysis, Social engineering.
E-mail:
i.i.bobok@op.edu.ua

Alla Kobozieva
Doctor of Technical Science, Professor.
Department of Technical Cybernetics and Information Technology.
Odesa National Maritime University. Research interests:steganography, steganoanalysis, Mathematics in information security
Email:
alla_kobozieva@ukr.net

Oleksandr Laptiev
Doctor of Technical Science, Senior Researcher.
Department of Cyber Security and Information Protection.
Taras Shevchenko National University of Kyiv.
Research interests: Cybersecurity, Information Protection.
E-mail:
alaptiev64@ukr.net

Vitalii Savchenko
Doctor of Technical Science, Professor.
Department of Cybersecurity Management.
State University of Information and Communication Technologies
Research interests: Cybersecurity, Information Protection.
E-mail:savitan@ukr.net

Anatolii Salii
PhD of Military Sciences, Professor.
Aviation and Air Defence Institute.
National Defense University of Ukraine.
Research interests: Logistics, Inventory Management.
E-mail:
a.salii@ed.nuou.org.ua

Tymur Kurtseitov
Doctor of Technical Science, Professor.
Department of Electromagnetic Warfare.
National Defense University of Ukraine.
Research interests: Radio Jamming, Electronic Counteraction.
E-mail: kurttimur@ukr.net