Application of Graph Theory to Ensure the Reliability of Steganographic Message Perception in the Creation of a Covert Communication Channel

Alla Kobozieva[1,*,†], Ivan Bobok[2,†], Oleksandr Laptiev[3,†] and Vitalii Savchenko[4,†]

[1] *Odesa National Maritime University, 34 Mechnikova str., 65029 Odesa, Ukraine*
[2] *Odesa Polytechnic National University, 1 Shevchenko av., 65044 Odesa, Ukraine*
[3] *Taras Shevchenko National University of Kyiv, 60 Volodymyrska str., 01033 Kyiv, Ukraine*
[4] *State University of Information and Communication Technologies, 7 Solomyanska str., 03110 Kyiv, Ukraine*

Abstract

The rapid advancement of information technologies and the pervasive digitalization of all areas of human activity have made the protection of digital information a critically important issue in modern society. Steganography has emerged as one of the most promising and effective approaches to information security. Among the key requirements for a steganographic system is the reliability of steganographic message perception. However, many existing methods do not systematically meet this requirement and are not designed to operate effectively with randomly selected containers. The purpose of this work is to improve the qualitative and quantitative indicators of the reliability of perception of a steganographic message generated by an arbitrary steganographic algorithm. Also, ensuring the possibility of operation of a steganographic message in conditions of a random container, without any modifications to the algorithm, by developing a method for selecting blocks of a digital image container for introducing additional information into them. The goal was achieved through the reasonable use of a specific oriented graph, which is associated with the image, for dividing container blocks into classes with the same indicators of the contribution of the high-frequency component. The most important result of the work is a theoretically substantiated definition of the block parameter, which gives an integral quantitative characteristic of its high-frequency component – the normalized separation of the maximum singular value of the block. The practical significance of the obtained results lies in the development of an algorithmic implementation of the proposed method for selecting blocks for steganographic transformation, which allows improving, when applied, both qualitative (established by subjective ranking) and quantitative (estimated using the peak signal-to-noise ratio) indicators of the reliability of perception of a steganographic message generated by an arbitrary steganographic method.

Keywords

reliability of perception of a steganogram, directed graph, binary relation, singular value

1. Introduction

The rapid development of information technology and the widespread digitalization of all areas of human activity have made the problem of protecting digital information critically important in modern society [1,2]. This issue is particularly acute for the critical infrastructure of the state [3-6], where insufficient information security, allowing for the possibility of unauthorized access, can

ICST-2025: Information Control Systems & Technologies, September 24-26, 2025, Odesa, Ukraine
* Corresponding author.
† These authors contributed equally.
alla_kobozeva@ukr.net (A. Kobozieva); onu_metal@ukr.net (I. Bobok); alaptev64@ukr.net (O. Laptiev); savitan@ukr.net (V. Savchenko)
0000-0001-7888-0499 (A. Kobozieva); 0000-0003-4548-0709 (I. Bobok); 0000-0002-4194-402X (O. Laptiev); 0000-0002-3014-131X (V. Savchenko)

lead to catastrophic consequences not only for individuals, organizations, and enterprises, but also for the state as a whole.

One of the most promising and effective areas of information protection today is steganography – the art and science of hiding information [7,8]. The primary objective of steganography is to conceal the very fact of the existence of secret data during their transmission, storage, or processing.

In steganographic systems, a secret message is embedded using a steganographic algorithm into a container object that does not attract attention. In this study, the container is a digital image (DI), and the secret message is first pre-encoded. The steganographic transformation must be performed in such a way that an external observer does not suspect the presence of any additional information (AI) within the resulting steganographic message. The resulting steganographic message is then transmitted openly to the recipient or stored in its received form [9].

A number of key requirements are imposed on a steganographic system, including:

- ensuring the reliability of perception of the steganographic message – i.e., it should be visually indistinguishable from the original container [10];
- resistance to attacks aimed at extracting or damaging the embedded message [11];
- resistance to steganalysis, including both statistical and machine-learning-based detection methods [12, 13];
- sufficient throughput of the covert communication channel, enabling the transmission of a meaningful amount of data [14];
- low computational complexity, ensuring the efficiency and practicality of the system in real-world applications.

One of the most critical requirements for organizing a covert communication channel is the first: ensuring the reliability of perception. If this requirement is not met, the steganographic system fails to conceal the very existence of secret information and thus becomes fundamentally ineffective [15]. At the same time, an objective and quantitative assessment of the reliability of perception remains an open and unsolved problem. Traditionally used visual distortion metrics such as signal-to-noise ratio (SNR), peak signal-to-noise ratio (PSNR), and similar indicators [16] are insufficient for providing a consistent and objective evaluation of the presence or absence of visual artifacts in a steganographic message. As a result, subjective ranking remains a relevant method of assessment. Indeed, one of the most commonly applied metrics in steganography – PSNR, even at high values does not guarantee reliable perception of the steganographic message in the general case [10]. The continued reliance on differential indicators for evaluating visual distortion only emphasizes the fact that modern steganographic systems still lack robust quantitative measures with a higher level of objectivity. In practice, steganographic messages with PSNR values above 40 dB are typically considered visually acceptable [17]. Furthermore, a higher PSNR value is usually associated with a lower probability of visual degradation after the embedding of additional information.

All containers used in steganographic systems can be classified into three categories: selected, random, and imposed [18]. While the deliberate selection of a container plays a significant role in ensuring key properties of a steganographic message, especially its perceptual invisibility, in real-world applications containers are most often chosen randomly. Therefore, it is highly desirable that the effectiveness of a steganographic algorithm be independent of the specific properties of the container. However, many existing methods are not adapted for operation with random containers, limiting their applicability, particularly when it comes to guaranteeing the reliability of perception. This limitation is a clear disadvantage of such systems [7,8,19].

Although ongoing research aims to establish sufficient conditions for reliable perception of steganographic messages [10], and its findings may inform the development of improved methods, many existing approaches still cannot systematically ensure perceptual reliability without substantial modification. Thus, this issue remains an open and relevant research challenge.

2. Problem analysis

Most modern steganographic methods are block-based, primarily for the following reasons [20]: resistance to compression attacks, relatively low computational complexity, and the natural suitability for parallel processing. For these reasons, block-based methods are the focus of the discussion below.

When creating a covert communication channel, the requirement for reliability of perception, as noted above, is key. However, modern steganographic methods cannot always ensure this condition for a random container.

The issues of developing sufficient conditions for ensuring the reliability of perception of a steganographic message have been repeatedly raised by steganographers. It is known [21] that modification of high-frequency components leads to the least visual distortions of the original image, while modification of medium frequencies corresponds to greater distortions. The greatest distortions of the original image occur when modifying low-frequency components. However, the practical application of this fact in the field of steganography is not always justified due to the fact that when using a high-frequency component (block) of an image for the implementation of the AI, the resulting steganographic message will be sensitive to any attacks against the embedded message, in particular to compression, which forces us to look for other, compromise, possibilities for ensuring the necessary properties of the steganographic message.

In [10], a sufficient condition for ensuring the reliability of perception of a steganographic message was obtained in the Walsh-Hadamard transform domain by using a General Approach to the Analysis of the State of Information Systems (General Approach) based on perturbation theory and matrix analysis. Based on General Approach, relationships were established between Walsh-Hadamard transforms, discrete cosine transform coefficients, and components of the singular decomposition of the corresponding matrices, which made it possible to obtain a sufficient condition for ensuring the reliability of perception of a steganographic message. The obtained condition can be applied regardless of the container region (spatial, transformation domain) in which the AI is introduced. In addition, due to the mathematical approach used, it makes it possible to prevent local violations of the reliability of perception associated not only with the steganographic transformation, but also with other disturbing effects, where the differential indicators of visual distortions of the DI are often unable to signal the artifacts that have arisen. Thus, the General Approach based on perturbation theory is one of the most promising approaches to solving the problem considered in the paper.

As a result of further development of the General Approach in [22,23], new properties of the formal parameters of the DI were established: the presence of regions of stabilization of perturbations of singular values and singular vectors of the matrix of the original DI, which are destroyed as a result of the steganographic transformation. The obtained conclusions confirmed that in order to ensure the reliability of perception of the formed steganographic message, it is sufficient that its result is a perturbation of singular triplets (blocks) of the container matrix, corresponding to several of the smallest singular values. Such a sufficient condition is preferable, compared to [21] in the frequency domain of content, since singular triplets do not separate the frequency components of the signal so "sharply": each singular triplet carries information to some extent about all frequency components, allowing even when using only the smallest singular values in the steganographic transformation to ensure the sensitivity of the corresponding block to disturbing effects is less than when using only high-frequency components.

However, all sufficient conditions require their consideration when developing a steganographic method. For existing methods, satisfying the existing sufficient conditions may be difficult without their specific modification or not feasible at all, although the reliability of perception by such methods may not be systematically ensured. Thus, in [19], a block steganographic method is proposed that implements the introduction of AI in the region of the singular decomposition of a container block by specific disturbance of a pair of maximum singular values. This method remains one of the most resistant among existing methods to compression

attacks with small quality factors. However, artifacts may appear on the steganographic message in the case when the container has significant areas with small differences in brightness values. The PSNR value for some DI-containers here fluctuates within the range of 33–37 dB when using all container blocks in the steganographic transformation process, i.e. with a covert communication channel throughput of 1/64 bits/pixel. This leaves the task of ensuring the possibility of effective operation of this method in the conditions of a random container relevant.

In [24], a block method is proposed that implements the immersion of the AI in the spatial region of the container by perturbing the pixels of the next block used in the steganographic transformation by $\pm\Delta b$ (depending on the value of the embedded bit), ensuring that the disturbance during the embedding of the AI is not less than the possible disturbance of the pixel during an attack against the embedded message for the fundamental possibility of decoding. This method does not guarantee the reliability of perception of the steganographic message, is not designed to work with a random container, in particular, having significant areas with small differences in brightness values, which is noted by one of the authors in a later work [25], where its modification is proposed.

The properties of the steganographic method often depend on the format of the DI container [26], on the values of the parameters used in its algorithmic implementation. Thus, the properties of the well-known block method of Koch and Zhao [16], which embeds the AI in the area of the discrete cosine transform by establishing a certain correspondence between the values of a pair of pre-selected coefficients, depend on how significant the difference between the moduli of these coefficients, determined by the parameter *P*, will be. The larger *P*, the more resistant the corresponding algorithm will be to attacks against the embedded message. However, increasing *P* can lead to the appearance of visible artifacts on the steganographic message, which results in the need to decrease *P*, and hence a decrease in the stability of the algorithm to be able to use a random container, leaving the task of simultaneously ensuring the reliability of perception of the steganographic message and significant resistance to attacks against the embedded message relevant.

Based on the results of the conducted analysis of literary sources, the objective of this work is to improve the qualitative and quantitative characteristics of the reliability of perception of a steganographic message generated by an arbitrary steganographic algorithm, including to ensure the possibility of its operation in a random container, without any modifications to the algorithm, by developing a method for selecting DI container blocks for implementing AI into them.

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

1. Determining a method for formally representing DI that gives an integral picture of the distribution of blocks depending on the contribution of the high-frequency component to them;
2. Determining a block parameter that gives a quantitative characteristic of its high-frequency component regardless of the storage format (with/without losses) of DI;
3. Developing a method for selecting DI container blocks for steganographic transformation and its algorithmic implementation.

3. Digital image graph

Let *F* – *n*×*n*-matrix of DI. We divide *F* in the standard way [27] into square non-intersecting *l*×*l*-blocks, any of which is further designated as $B_{ij}, i, j = \overline{1,\lfloor n/l \rfloor}$, where $\lfloor\cdot\rfloor$ – the integer part of the argument. Each of the blocks is considered as a potential "candidate" for the implementation of the AI, which is a binary sequence: $p_1, p_2, \ldots, p_t, p_i \in \{0,1\}$. As is known [21], due to the peculiarities of the human visual system, the blocks that contain small details and contours are preferable for minor changes during steganographic transformation of a container, i.e. where there is a relatively significant high-frequency component. To isolate such blocks, it is necessary to determine such a parameter (parameters) of the block, the quantitative expression of which will be an indicator of

the presence of contours – the contribution of the high-frequency component. The presence of such a parameter (parameters) will allow us to construct a binary relation ρ on a set of DI blocks according to the following rule: block B_{ij} will be in relation ρ [28] with B_{km}, i.e. ordered pair $< B_{ij}, B_{km} > \in \rho$, if their high-frequency component contribution rates are equal. This binary relation is reflexive, symmetrical and transitive, i.e. it is an equivalence relation, and therefore defines the partition of the set of AI blocks into subsets – equivalence classes. Based on the value of the selected parameter for one block from the class, it will be possible to draw a conclusion about the expediency/inexpediency of the entire class for steganographic transformation, since each class here is completely determined by any of its elements. Among these formed classes, i.e. among their representative blocks, it is proposed to make a choice for implementing AI.

To simplify the process of such a choice, we will associate the DI with a directed graph $G_{DI}(V, X)$ the binary relation defined above ρ [29]. Set of vertices *V* a graph is defined by a set of image blocks, an ordered pair of blocks $< B_{ij}, B_{km} > \in X$, i.e. there is a directed edge $< B_{ij}, B_{km} >$, coming from the top B_{ij} to the top B_{km}, if $< B_{ij}, B_{km} > \in \rho$. Based on the properties of the introduced binary relation ρ, graph $G_{DI}(V, X)$ will have the following properties:

- at each vertex of the graph $G_{DI}(V, X)$ there will be a loop (reflexivity ρ),
- for each edge of the graph there will be an oppositely directed edge (symmetry ρ);
- the graph will be disconnected, the number of its connectivity components will be determined by the number of equivalence classes for the set of DI blocks.

To achieve the goal of the work, it makes sense to simplify the obtained graph $G_{DI}(V, X)$ from the point of view of reducing the cardinalities of sets *V*, *X*, applying a simple homomorphic convolution to each of its connected components, resulting in a macrograph $G_{DI}^{M}(V, X)$, each macro-vertex of which corresponds to an equivalence class of a binary relation ρ, is isolated, and the choice of blocks preferred for steganographic transformation will be reduced to the choice of certain macrovertices. To ensure greater informativeness of the graph $G_{DI}^{M}(V, X)$ it is proposed to make it weighted, where the weight of any macro-peak will be determined by the value of the parameter (or some quantitative characteristic of their totality, if there is more than one parameter), which is an indicator of the presence of contours in the block – the contribution of the high-frequency component.

4. Selection of the integral quantitative indicator of the high-frequency component of the block

The main issue for the implementation of graph construction $G_{DI}^{M}(V, X)$, corresponding to the DI, is the question of choosing a parameter (parameters) – a quantitative indicator of the high-frequency component of the block. On the surface, here lies the use of the values of the high-frequency coefficients of the block, but the rationality of such use is not obvious. A number of questions arise here: how many such coefficients to use in the analysis process; will this number depend on the block size; how exactly to quantitatively take into account the combined contribution of the selected frequency coefficients. And the main question: if there are several such parameters, then how to compare them when comparing blocks to select from them (blocks) more preferable for steganographic transformation. And although all these questions can be answered as a result of the studies, the main disadvantage of directly using high-frequency coefficients to achieve the goal of the work is a significant difference in their values for DI blocks in different (with/without loss) storage formats [10], which will not ensure the independence of the developed method for selecting container blocks for steganographic transformation from the container format.

Obviously, it is preferable to achieve the goal of the work to determine/form one integral parameter of the block, which characterizes the presence of contours in this block, the specific choice of which is justified below.

From the point of view of ensuring the requirement for a steganosystem of insignificant computational complexity, for the method being developed, preference should be given to the block parameters used by the method for analysis, from its spatial domain, since the analysis of such parameters will not require additional computational costs when moving from the spatial domain to the transformation domain and back. An indicator of the presence of a high-frequency component in the spatial domain of the block B_{ij} with elements $b_{rt}^{(ij)}, r, t = \overline{1,l}$, is the presence of significant differences in pixel brightness, which is characterized by the magnitude of the amplitude of brightness fluctuations:

$$A = \max_{r,t} b_{rt}^{(ij)} - \min_{r,t} b_{rt}^{(ij)}. \quad (1)$$

However, for the purposes of work, such a parameter is not indicative for use, since a situation is possible here when the difference in brightness values in a block is caused by only a few pixels, while all the others form a background area:

$$\begin{pmatrix} 122 & 153 & 153 & 151 \\ 151 & 152 & 152 & 151 \\ 150 & 151 & 152 & 152 \\ 151 & 153 & 152 & 152 \end{pmatrix}.$$

The matrix shown corresponds to the DI block in Fig. 1(b), highlighted in red. There is only one pixel (1,1), due to the presence of which a noticeable difference in brightness is obtained: $A = 31$. It is obvious that such a block is inappropriate to use in the process of steganographic transformation for several reasons. Firstly, if any of the block transformation areas (frequency, singular value decomposition area, etc.) is used for the embedding of the AI, then this will most likely lead to the perturbation of most pixels, which means that there will be a high probability of artifacts occurring within the boundaries of its background part. Secondly, if the embedding of the AI occurs directly in the spatial area, then the localization of those pixels, due to the perturbation of which this embedding will be carried out, is obvious here, which reduces the level of secrecy of the steganosystem. Thirdly, such a block structure significantly limits the value of the throughput of the covert communication channel, which, although not critical, is not desirable. Taking into account the above, parameter (1) is inappropriate to use as a characteristic for selecting blocks for embedding the AI.

In accordance with the General Approach, all properties of the DI and their changes, in particular as a result of the steganographic transformation, can be formally estimated by the properties (perturbations) of the full set of its formal parameters – the singular values and singular vectors F, uniquely determined by means of normal singular value decomposition [30]:

$$F = U\Sigma V^T, \quad (2)$$

where U, V – orthogonal matrices where columns $u_i, v_i = \overline{1,n}$, are left and right singular vectors respectively, with left singular vectors being lexicographically positive, $\Sigma = diag\big(\sigma_1(F), \dots, \sigma_n(F)\big)$,

$$\sigma_1(F) \geq \cdots \geq \sigma_n(F) \geq 0, \quad (3)$$

– singular values F, $(\sigma_1, u_i, v_i), i = \overline{1,n}$, – singular triplets. The presence/absence of contours in an arbitrary block of the image is assessed by its singular spectrum – a set of singular values, which in principle can become the subject of analysis for solving the problem under consideration. At the same time, the number of singular values – parameters from which it is necessary to select the most "useful" for analysis, is an order of magnitude less than the number of frequency coefficients discussed above.

Information about high frequencies (of the block) of the DI is carried mainly by singular triplets corresponding to the smallest singular values (of the block) of the matrix F. It can be argued that

the singular values in these triplets are responsible for the high-frequency component (of the block) of the image [22,23]. Indeed, the energy *E* of DI with *n*×*n*-matrix *F* with elements $f_{ij}, i,j = \overline{1,n}$, is defined as:

$$E = \sum_{i=1}^{n}\sum_{j=1}^{n} f_{ij}^2 = \sum_{u=0}^{n-1}\sum_{v=0}^{n-1} P(u,v) \quad (4)$$

where $P(u,v)$, $u = \overline{0,m-1}, v = \overline{0,n-1}$, – energy spectrum *F*. The expansion (2) can be equivalently represented as a sum of outer products [31]: $F = U\Sigma V = \sum_{i=1}^{n} \sigma_i u_i v_i^T$. This idea is disconcerting *F* on n signals $\sigma_i u_i v_i^T$, the total energy of which gives *E*.

Signal energy $\sigma_i u_i v_i^T = \sigma_i (u_{1i}, \dots, u_{ni})^T (v_{1i}, \dots, v_{ni})$ in the spatial domain in accordance with (4) is defined as:

$$\sigma_i^2 \left(u_{1i}^2 v_{1i}^2 + \dots + u_{1i}^2 v_{ni}^2 + u_{2i}^2 v_{1i}^2 + \dots + u_{2i}^2 v_{ni}^2 + \dots + u_{ni}^2 v_{1i}^2 + \dots + u_{ni}^2 v_{ni}^2\right) = \sigma_i^2 (u_{1i}^2 \left(v_{1i}^2 + \dots + v_{ni}^2\right) +$$
$$+ \dots + u_{ni}^2 \left(v_{1i}^2 + \dots + v_{ni}^2\right)) = \sigma_i^2 \left(u_{1i}^2 + \dots + u_{ni}^2\right)\left(v_{1i}^2 + \dots + v_{ni}^2\right) = \sigma_i^2 ,$$

that is

$$\sum_{u=0}^{n-1}\sum_{v=0}^{n-1} P(u,v) = \sum_{i=1}^{n} \sigma_i^2 .$$

Thus, it is the singular values in singular triplets that directly correspond to the frequency components of the image (of the block), including high-frequency ones. Although the number of singular values, as noted above, is an order of magnitude less than the number of frequency coefficients, the use of even small singular values still does not provide the opportunity to determine a single block parameter characterizing the contribution of its high-frequency component. In addition, in (blocks) of DI data in lossy formats, it is the smallest singular values that "suffer" the most during compression, being zeroed out in the process of quantization and rounding of the discrete cosine transform coefficients in more than 98% of image blocks, regardless of whether contours and small details are present in the block or not. When DI data is restored after compression, the smallest singular values of blocks, although they will be different from zero, however, this difference is due only to the roundings that occur during the restoration process, i.e. is associated with the peculiarities of machine arithmetic and the need for "transitions" between sets of real (singular values) and integer (values of pixel brightness) numbers. This makes it inappropriate to use such singular values as a subject of analysis for solving the problems of this work, taking into account the required independence of the developed method from the format of the DI.

Further, DI that differ only in the storage format (with/without losses) will be called corresponding.

For DI blocks, regardless of the storage format, the relation (3) can be clarified:

$$\sigma_1(B) \gg \sigma_2(B) \geq \dots \geq \sigma_l(B)$$

in this case, the smaller the high-frequency component of the block, the greater the relative difference between the first singular value and all other singular values spectrum. Due to this, as an integral parameter that characterizes the contribution of high frequencies to the block, we will consider the normalized separation of the maximum singular value $\sigma_i(B)$. Normalized separation $svdgap_n(i)$ arbitrary singular value $\sigma_i(B)$ is determined in accordance with the formula:

$$\mathrm{svdgap}_n(i) = \min_{i \neq j} \left|\overline{\sigma_j} - \overline{\sigma_i}\right|, \quad (5)$$

where $\overline{\sigma_i}, i = \overline{1,l}$ – vector components $\bar{\sigma} = (\overline{\sigma_1}, \overline{\sigma_2}, \dots, \overline{\sigma_l})^T$, at the same time $\bar{\sigma} = \sigma / \|\sigma\|$, where $\|\sigma\|$ vector norm $\sigma = \left(\sigma_1(B), \sigma_2(B), \dots, \sigma_l(B)\right)^T$. In accordance with (5):

$$\mathrm{svdgap}_n(1) = \overline{\sigma_1} - \overline{\sigma_2}. \quad (6)$$

It can be concluded that the value $svdgap_n(1)$ will be the closer to unity, the smaller the high-frequency component, regardless of the storage format of the DI – with/without losses. This conclusion was practically confirmed in the course of a computational experiment, typical results of which are demonstrated in Fig. 2 for the DI presented in Fig. 1. Properties of the histograms of

values $svdgap_n(1)$ for blocks of original lossless DI and corresponding lossy DI (JPEG, QF=75) are comparable, although quantization of frequency coefficients during compression contributes to the features of the above-mentioned histogram. Thus, the histogram mode as a result of image compression is slightly shifted to the right both for DI with large areas of small differences in pixel brightness values (hereinafter referred to as background images), and for DI where areas with small differences in brightness are few in number and insignificant in relative area, i.e. containing a large number of details, contours (hereinafter referred to as contour image), while for contour DI, after compression, blocks appear (or the number increases), for which $svdgap_n(1)$ comparable to one, and for the background in the lossy format in one, the histogram mode will most likely be observed.

A b

Figure 1: 560×560 pixel DI in lossless format (TIF): a – DI containing a large number of contours, small details (with a significant high-frequency component); b – DI with a significant background area

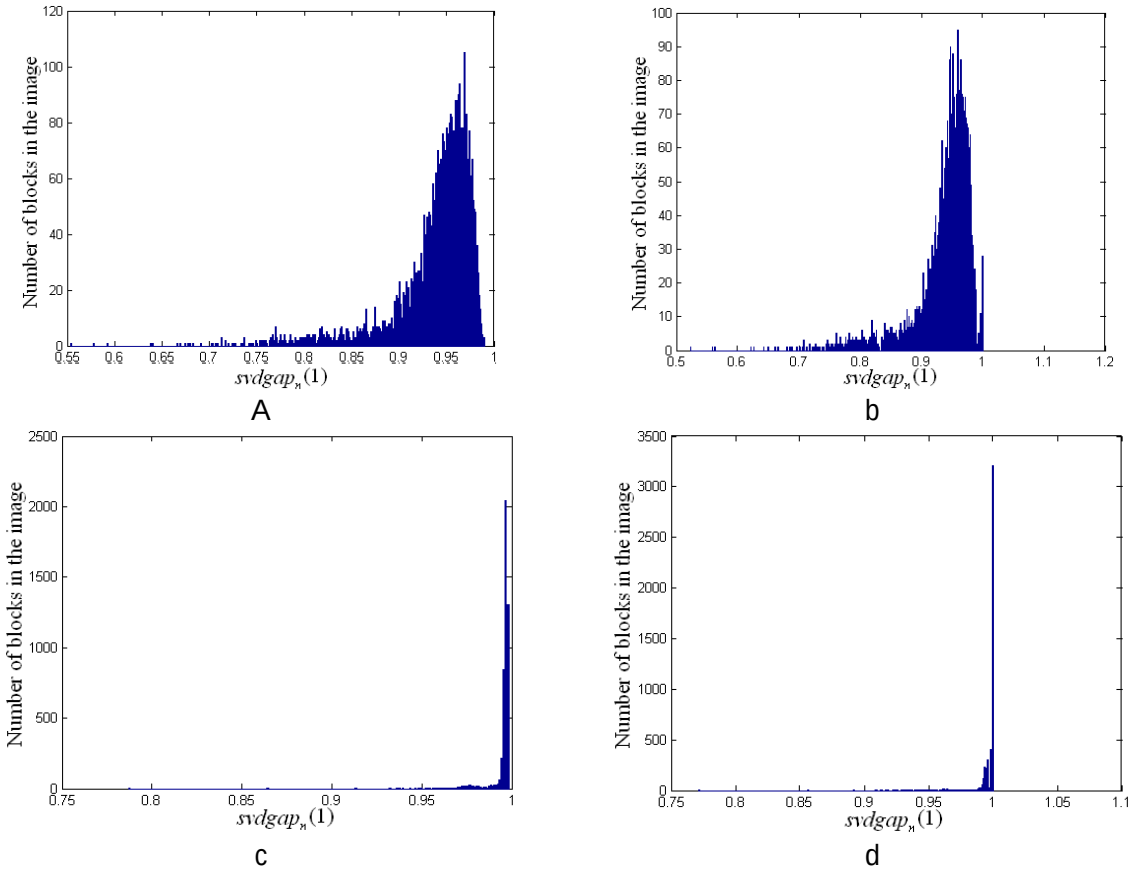


Figure 2: Histograms of values $svdgap_n(1)$ for blocks of original DI in lossless format and corresponding DI in lossy format (JPEG, QF=75): a, b – for DI (Fig. 1(a)) and corresponding DI with losses, respectively; c, d – for DI (Fig. 1(b)) and corresponding DI with losses, respectively

However, there is no fundamental difference for the histograms of the corresponding DI. Let us designate Γ_F and Γ_K – histograms $svdgap_n(1)$ for background and contour DI respectively.

Differences in properties Γ_F and Γ_K are determined only by the degree of contribution of the high-frequency component to the DI, i.e. by whether it is background or contour:

- in Γ_F range of possible values $svdgap_n(1)$ less than in Γ_K;
- histogram modes $m(\Gamma_F)$ and $m(\Gamma_K)$ are related by the inequality: $m(\Gamma_F) > m(\Gamma_K)$;

values in modes $V\big(m(\Gamma_F)\big)$ and $V\big(m(\Gamma_K)\big)$ correspond to the inequality: $V\big(m(\Gamma_F)\big) \gg V\big(m(\Gamma_K)\big)$. At the same time, more than 90% blocks of DI usually responds for a little neighborhood of mode Γ_F, while for a contour image outside such a neighborhood there will be a significant number of blocks (more than 50%). This occurs due to the fact that for blocks with small differences in pixel brightness values $svdgap_n(1) \approx 1$, and for the background image of such blocks the majority, and only for a small number of blocks containing contours, small details, $svdgap_n(1)$ will differ significantly from 1.

The presented results support the use of expression (6) as an integral parameter for evaluating the contribution of the high-frequency component to a digital signal block. They also provide practical confirmation of the effectiveness of the proposed approach to block selection for steganographic transformation based on the analysis $svdgap_n(1)$.

However, when considering the presence of contours in the DI block as an indicator of the normalized separation of the maximum singular value when constructing the binary relation defined above ρ and the corresponding directed weighted graph $G_{DI}(V,X)$ it is necessary to determine in which case the values of the normalized separation of the maximum singular values are considered equal. Since $svdgap_n(1) \in [0,1] \subset R$, where R – is a set of real numbers, the set [0,1] is infinite, and the computation $svdgap_n(1)$ is in a floating-point number system, then, due to the specifics of machine arithmetic, computational errors may accumulate, causing two real numbers that are actually equal to appear slightly or even noticeably different after calculation. The degree of difference here will be determined, firstly, by the sensitivity/insensitivity of the parameter in question to disturbing effects, and secondly, by the different number and order of arithmetic operations performed to calculate them, which, in the general case, will lead to different errors for the two numbers. Significant differences in the values $svdgap_n(1)$, if in fact they are equal, it cannot arise, since the singular values, and therefore $svdgap_n(1)$, are insensitive to disturbing effects [31]. But minor differences even for naturally equal normalized separations of the first singular value in the general case may take place, which must be taken into account in the practical verification of their equality. Moreover, the equality of the calculated values may be a consequence of the peculiarities of machine arithmetic $svdgap_n(1)$ while their actual values differ from each other. Taking into account all of the above, it is proposed that when calculating $svdgap_n(1)$ round off a value to significant digits, thus moving into a discrete range of values $svdgap_n(1)$, i.e. replacing an infinite set [0,1] to a finite discrete bounded set $[0,1]_d$, for which the exact lower and upper bounds will be equal, respectively: $inf[0,1]_d = 0$, $sup[0,1]_d = 1$.

Example of construction $G_{DI}(V,X)$ for a small-sized DI that is part of the image (Fig. 1(b)), is shown in Fig. 3 (in order not to clutter the figure, each pair of oppositely directed edges is The constructed graph is disconnected. Its connectivity components are strongly connected subgraphs, each of which corresponds to the equivalence class of the introduced binary relation . The corresponding weighted macrograph G_DI^M (V,X) is shown in Fig. 4 (for each vertex its label is entered, and the weight is also indicated).designated by one bidirectional edge). When $\alpha = 2$ we have the following values $svdgap_n(1)$:

0.97, 0.99, 0.97, 0.97, 0.98, 0.98, 0.99, 0.99, 0.97.

Values $svdgap_n(1)$ correspond to the order of blocks from left to right, top to bottom.

The constructed graph is disconnected. Its connectivity components are strongly connected subgraphs, each of which corresponds to the equivalence class of the introduced binary relation ρ.

The corresponding weighted macrograph $G_{DI}^{M}(V,X)$ is shown in Fig. 4 (for each vertex its label is entered, and the weight is also indicated).

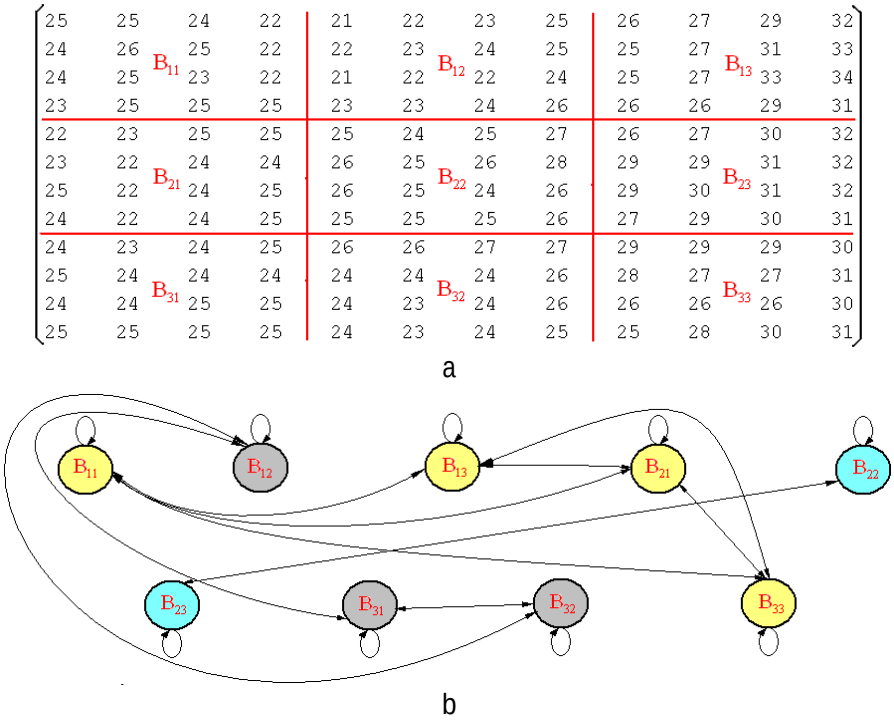


Figure 3: An example of constructing a graph corresponding to the DI: a – the DI matrix, divided into 4×4 blocks; b – $G_{DI}(V,X)$

Figure 4: Macrograph $G_{DI}^{M}(V,X)$, corresponding to the DI with the matrix shown in Fig. 3(a)

Usage $G_{DI}^{M}(V,X)$ allows computationally simple rejection of those blocks, the introduction of DI into which is undesirable. These are blocks for which the weight of the corresponding macrovertices is close to one. The number of such rejected classes-macrovertices will depend on the required throughput of the formed steganographic communication channel, or in other words, on the length of DI. The lower the throughput, the greater the number of formed classes of blocks (macrovertices) that can be rejected, the higher the quality of the choice of blocks for steganographic transformation will be – only with a significant high-frequency component (macrovertices with a relatively small weight), the higher the probability of ensuring the reliability of perception of the steganographic message.

5. Method for selecting image container blocks for embedding additional information

The main steps of the method for selecting blocks of the DI container for the implementation of AI are as follows:

Step 1. Matrix *F* of DI with size *n*×*n* is divided in the standard way into non-intersecting *l*×*l*-blocks $B_{ij}, i,j = \overline{1,[n/l]}$.

Step 2. For each block $B_{ij}, i,j = \overline{1,[n/l]}$:

2.1. Define $svdgap_n(1) = \overline{\sigma_1} - \overline{\sigma_2}$.

2.2. Round up $svdgap_n(1)$ to α significant figures. Result – $s(B_{ij})$.

Step 3. On a set of blocks $B_{ij}, i,j = \overline{1,[n/l]}$ of DI define binary relation ρ:

$$\langle B_{ij}, B_{km} \rangle \in \rho \quad \text{if} \quad s(B_{ij}) = s(B_{km}).$$

Step 4. Build a directed graph $G_{DI}(V,X)$, corresponding to a binary relation ρ.

Step 5. By simple homomorphic convolution of the connected components of the graph $G_{DI}(V,X)$ build a macrograph $G_{DI}^{M}(V,X)$.

Step 6. Determine the quantity T of blocks of the DI container, necessary for the immersion of the DI $p_1, p_2, \dots, p_t, p_i \in \{0,1\}$.

Step 7. For immersion of DI use T blocks corresponding to macro vertices $G_{DI}^{M}(V,X)$, starting from the macro-vertex with the smallest weight, in order of increasing weight of the vertices. Blocks from one equivalence class are selected according to the secret key.

For practical verification of the effectiveness of using the proposed method for selecting container blocks for steganographic transformation in order to improve/ensure the reliability of perception of the generated steganographic message, a computational experiment was conducted in which the following parameter values were used for the algorithmic implementation of the method: $l = 8$, $\alpha = 2$.

The experiment involved 300 DIs from the database 4cam_auth [32] (TIF format), 300 DIs from the base img_Nikon_D70s [33] (TIF format), 200 DIs obtained by non-professional video cameras (TIF format), 800 DIs from the NRCS database [34] (JPEG format). The following steganographic methods were used in the experiment: one of the most resistant to compression attacks, the steganographic method [19], which leads to the non-systematic occurrence of artifacts on the DI steganographic message; one of the most widely used and modifiable methods is Koch and Zhao [16], the violation of the reliability of perception in which can occur with an increase in the parameter used to modify the coefficients of the discrete cosine transform when embedding the DI bit into the next block. During the experiment, the same DI was embedded into the container with a random selection of blocks and in accordance with the graph $G_{DI}^{M}(V,X)$. Typical experimental results are illustrated in Fig. 5, 6 for specific DI.

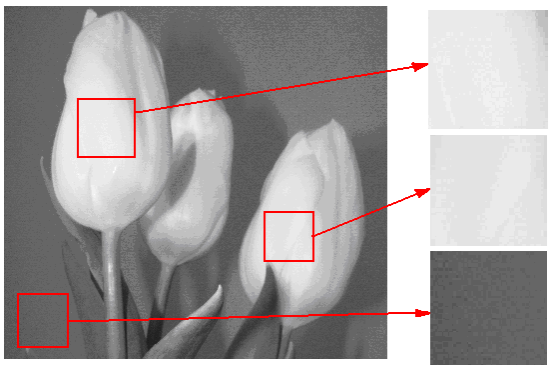
The visual quality of steganographic messages (perception reliability), established by subjective ranking, for all DI involved in the computational experiment turned out to be higher with the second method of immersion of DI – selection of blocks in accordance with the proposed method. It was found that the value of the difference indicator of visual distortion PSNR for the second immersion option was never less than this indicator for the first option, and for 52% of images PSNR was significantly increased: by 2–6 dB.

Of course, any choice of container blocks potentially reduces the possible throughput of the formed communication channel, which is undesirable. However, firstly, such a forced measure makes it possible to use existing effective methods without any modifications in the conditions of a random container, and secondly, taking into account the rapid development of steganalytical methods, the modern trend is to use steganographic methods in conditions of low throughput.

It should be noted that, of course, the use of this method cannot guarantee the absence of artifacts on the DI-steganographic message, established using subjective ranking, with a significant length of the DI. But it guarantees an improvement in visual quality when using it, compared to a set of blocks for steganographic transformation, selected randomly or in accordance with a secret key, which does not take into account the possibility of artifacts, i.e. does not take into account the fact that the steganographic method used is not designed for a random container.

The method for selecting container blocks for steganographic transformation proposed in the work is itself block-based, which determines its computational complexity for $n \times n$-DI as $\underline{O}(n^2)$, but this does not limit the scope of its application to block steganographic methods only: it can also be used for steganometric methods that are not block-based, for example, for the method of modifying the least significant bit [35], by selecting areas on the DI container in the form of a combination of blocks that are most/least favorable for embedding the DI from the point of view of ensuring the reliability of perception of the steganographic message.

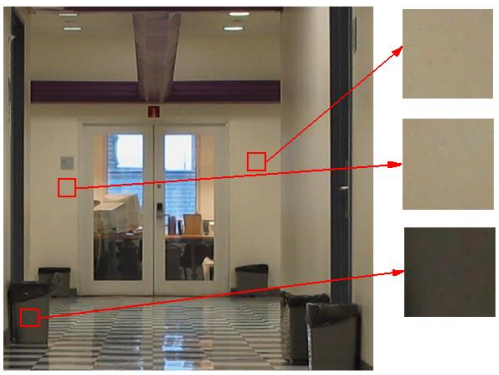
A b



c

Figure 5: Results of steganographic transformation using the steganographic method [19]: a – DI container; b – steganographic message with random selection of blocks; c – steganographic message, when the blocks were selected using the graph $G_{DI}^{M}(V, X)$

A b



c

Figure 6: Results of steganographic transformation using the method of Koch and Zhao: a – DI container; b – steganographic message with random selection of blocks; c – steganographic message, when the blocks were selected using the graph $G_{DI}^{M}(V, X)$

6. Conclusions

The paper solves a scientific and practical problem of increasing the qualitative and quantitative indicators of the reliability of perception of a steganographic message generated by an arbitrary steganographic algorithm, which is relevant for constructing a hidden (steganographic) communication channel, by developing a method for selecting blocks of the matrix of a DI container for embedding DI into them. The developed method ensures the possibility of operating the steganographic algorithm under conditions of a random container, which is most often used in practice. No direct analogues of the proposed method have been found in the open press.

The research yielded the following key results:

1. The expediency of formally representing a digital image as a weighted macrograph is substantiated. In this model, macrovertices are formed by a simple homomorphic convolution of strongly connected subgraphs derived from a directed graph. This graph corresponds to a binary equivalence relation defined on the set of DI blocks. Two blocks are considered equivalent if the quantitative contribution of their high-frequency components is equal.
2. A new block parameter was introduced – normalized separation of the maximum singular value. This parameter provides an integral quantitative characteristic of the block's high-frequency component, independent of the digital image's storage format (lossy or lossless). Based on this parameter, a method for selecting suitable DI container blocks for steganization was developed, along with its algorithmic implementation.
3. The proposed algorithm for block selection demonstrated significant improvements. In 52% of the test images, the PSNR increased by 2–6 dB compared to random block selection. Moreover, in all cases, the PSNR achieved using the proposed algorithm was never lower than that of random selection. The visual quality of the steganographic messages, as determined by subjective ranking, was also consistently maintained or improved across all test images.

The developed method for selecting blocks for steganographic transformation has a low computational complexity, which for $n \times n$-DI is defined as $\underline{O}(n^2)$, which provides the prospect of its use for a stream container.

Declaration on Generative AI

The authors have not employed any Generative AI tools.

References

[1] T.O. Abrahams, S.K. Ewuga, S.O. Dawodu, A.O. Adegbite, A.O. Hassan, A review of cybersecurity strategies in modern organizations: examining the evolution and effectiveness of cybersecurity measures for data protection, Computer Science & IT Research Journal 5 (2024) 1–25. URL: https://doi.org/10.51594/csitrj.v5i1.699

[2] X. Sun, The current status and challenges of cybersecurity risks, Internet of Things and Cloud Computing 12 (2024) 10–16. URL: https://doi.org/10.11648/j.iotcc.20241201.12

[3] S. Mukherjee, Implementing cybersecurity in the energy sector, 2019. URL: https://doi.org/10.6084/m9.figshare.9728051

[4] I. Bobok, A. Kobozeva, M. Maksymov, O. Maksymova, Checking the integrity of CCTV footage in real time at nuclear facilities, Nuclear & Radiation Safety 2 (2016) 68–72.

[5] F. Akpan, G. Bendiab, S. Shiaeles, S. Karamperidis, M. Michaloliakos, Cybersecurity challenges in the maritime sector, Network 2 (2022) 123–138. URL: https://doi.org/10.3390/network2010009

[6] J.I. Alcaide, R.G. Llave, Critical infrastructures cybersecurity and the maritime sector, Transportation Research Procedia 45 (2020) 547–554. URL: https://doi.org/10.1016/j.trpro.2020.03.058
[7] D. Srinivasan, K. Manojkumar, A. Syed, H. Nutakki, A comprehensive review on advancements and applications of steganography, 2024. URL: https://doi.org/10.13140/RG.2.2.13568.44807
[8] A.A. Abdulla, Digital image steganography: challenges, investigation, and recommendation for the future direction, Soft Computing 28 (2024) 8963–8976. URL: https://doi.org/10.1007/s00500-023-09130-8
[9] S. Pramanik, M.M. Ghonge, R.V. Ravi (Eds.), Multidisciplinary Approach to Modern Digital Steganography, Information Science Reference, 2021.
[10] A.A. Kobozieva, 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. URL: https://doi.org/10.52254/1857-0070.2022.2-54.08
[11] A.A. Kobozeva, A.V. Sokolov, Robust steganographic method with code-controlled information embedding, Problemele Energeticii Regionale 4 (2021) 115–130. URL: https://doi.org/10.52254/1857-0070.2021.4-52.11
[12] K.D. Michaylov, D.K. Sarmah, Steganography and steganalysis for digital image enhanced Forensic analysis and recommendations, Journal of Cyber Security Technology 9 (2024) 1–27. URL: https://doi.org/10.1080/23742917.2024.2304441
[13] A. Kobozieva, I. Bobok, N. Kushnirenko, Steganalysis method for detecting LSB embedding in digital video, digital image sequence, in Proceedings of the 11th International Conference on Information Control Systems & Technologies (ICST-2023), Odesa, Ukraine, 2023, pp. 78–90. URL: https://ceur-ws.org/Vol-3513/paper07.pdf
[14] B.G. Ibrahimov, K.M. Tahirova, Method for calculation maximum throughput hidden channels in systems of steganographic communications, T-Comm 16 (2022) 40–45. URL: https://doi.org/10.36724/2072-8735-2022-16-9-40-45
[15] M. Hassaballah (Ed.), Digital Media Steganography: Principles, Algorithms, and Advances (1st Ed.), Academic Press, 2020.
[16] G. Konakhovich, D. Progonov, O. Puzyrenko, Steganographic Processing and Analysis of Multimedia Data, Center for Educational Literature, 2018.
[17] A.S. Ansari, M.S. Mohammadi, M.T. Parvez, A comparative study of recent steganography techniques for multiple image formats, International Journal of Computer Network and Information Security 11 (2019) 11–25. URL: https://doi.org/10.5815/ijcnis.2019.01.02
[18] J. Fridrich, Steganography in Digital Media: Principles, Algorithms, and Applications, Cambridge University Press, 2009.
[19] M.A. Melnik, Compression-resistant steganography algorithm, Information Security 2 (2012) 99–106.
[20] I. Bobok, A. Kobozeva, Universal method for detecting violations in the integrity of a digital image based on analysis of blocks of its matrix, Problemele Energeticii Regionale 4 (2023) 98–112. URL: https://doi.org/10.52254/1857-0070.2023.4-60.08
[21] K. Karampidis, E. Kavallieratou, G. Papadourakis, A review of image steganalysis techniques for digital forensics, Journal of Information Security and Applications 40 (2018) 217–235. URL: https://doi.org/10.1016/j.jisa.2018.04.005
[22] I.I. Bobok, A.A. Kobozeva, Development of the theoretical approach based on matrix theory for analyzing the state of information security systems, Problemele Energeticii Regionale 3 (2024) 29–43. URL: https://doi.org/10.52254/1857-0070.2024.3-63.03
[23] I.I. Bobok, A.A. Kobozieva, Theoretical foundations of digital content integrity expertise, Problemele Energeticii Regionale 1 (2025) 105–120. URL: https://doi.org/10.52254/1857-0070.2025.1-65.08

[24] V.M. Rudnitsky, O.V. Kostyrka, Robust stegano transformation in spatial domain of cover image, Informatics and Mathematical Methods in Simulation 3 (2013) 353–360.
[25] O.V. Kostyrka, Modification of resistance to disturbance quilted transformation of spatial image container, Informatics and Mathematical Methods in Simulation 6 (2016) 85–93.
[26] Z. Liu, X. Yi, X. Zhao, Y. Yang, Content-aware robust JPEG steganography for lossy channels using LPCNet, IEEE Signal Processing Letters 29 (2022) 2253–2257. URL: https://doi.org/10.1109/LSP.2022.3217727
[27] R. Gonzalez, R. Woods, Digital Image Processing (4th Ed.), Pearson, 2018.
[28] S.K. Sarkar, A Textbook Of Discrete Mathematics, S Chand Publishing, 2019.
[29] J.L. Gross, J. Yellen, M. Anderson, Graph Theory and Its Applications (3rd Ed.), Chapman and Hall/CRC, 2018.
[30] C. Bergman, J. Davidson, Unitary embedding for data hiding with the SVD, 2005. URL: https://dr.lib.iastate.edu/handle/20.500.12876/54635
[31] J.W. Demmel, Applied Numerical Linear Algebra, SIAM, 1997.
[32] Y.-f. Hsu, S.-f. Chang, Detecting image splicing using geometry invariants and camera characteristics consistency, in Proceedings of the 2006 IEEE International Conference on Multimedia and Expo, Toronto, Canada, 2006, pp. 549–552. doi: 10.1109/ICME.2006.262447.
[33] T. Gloe, R. Böhme, The 'Dresden Image Database' for benchmarking digital image forensics, in: Proceedings of the 2010 ACM Symposium on Applied Computing (SAC '10). Association for Computing Machinery, New York, USA, 2010, pp. 1584–1590. doi: 10.1145/1774088.1774427
[34] NRCS Photo Gallery. United States Department of Agriculture. Washington, USA. URL: https://www.nrcs.usda.gov
[35] M.A. Aslam et al., Image steganography using Least Significant Bit (LSB) — A systematic literature review, in Proceedings of the 2022 2nd International Conference on Computing and Information Technology (ICCIT), Tabuk, Saudi Arabia, 2022, pp. 32–38. doi: 10.1109/ICCIT52419.2022.9711628