

Hierarchical block selection of a digital image container as a source for enhancing the efficiency of a steganographic system

Ivan Bobok^{1,*}, Svitlana Hryhorenko^{1,†}

¹ Odesa Polytechnic National University, 1 Shevchenko av., 65044 Odesa, Ukraine

Abstract

Today, information security has expanded beyond purely technical issues and has become one of the key tasks in ensuring the national security of the state. In the context of hybrid conflicts, information systems become one of the primary targets. This problem becomes particularly acute when applied to critical infrastructure. Within the context of critical infrastructure, steganography turns into a vital and highly relevant protection tool. One of the primary requirements for a steganographic system is ensuring the perceptual reliability of the generated stego-message, which is not always guaranteed by modern steganographic methods, leaving the task of improving the steganographic system highly relevant. The aim of this work is to enhance the efficiency of the steganographic system by improving the container block selection process, where a digital image serves as the container. The efficiency of the steganographic system is evaluated using a quantitative metric of the generated stego-message's visual quality – the peak signal-to-noise ratio (PSNR). The goal was achieved by enabling a systematic, in-depth analysis of the properties of individual block components in terms of their degree of texture. The most significant result of the work is the development of a hierarchical image structure based on an introduced binary strict order relation on the set R of image blocks, which defines its partial ordering and is mapped to a directed weighted graph. A quantitative metric of the corresponding block's degree of texture is used as the weight coefficient of a graph vertex. The hierarchical structure graph allows for increasing the efficiency of the block selection process compared to selection based on a stationary partitioning of the container matrix. The proposed hierarchical container structure and the corresponding graph, which allow for a coarse selection followed by its refinement, serve as a universal tool for achieving any arbitrary selection goal, reflected by the weight coefficients of the graph vertices.

Keywords

information security, steganography, perceptual reliability, digital image, hierarchical structure, directed weighted graph, binary relation

1. Introduction

Today, information security and cybersecurity have expanded beyond purely technical issues and have become one of the key tasks in ensuring the national security of the state. The rapid digitalization of all spheres of society – the economy, public administration, the military, healthcare, and energy – has led to the fact that information systems have become not merely an auxiliary tool, but the “supporting structure” of modern civilization. This has resulted in a fundamentally new vulnerability: today, the disruption of information systems can paralyze entire industries and state institutions far more effectively than traditional methods of impact. This problem becomes particularly acute when applied to critical infrastructure – a collection of facilities and systems whose disruption entails catastrophic consequences for society and the state [1–4]. Modern armed

ADT-ISMDDC 2026: *Advanced Digital Technologies: Intelligent Systems, Modeling, and Data-Driven Control*, September 22–24, 2026, Odesa, Ukraine

* Corresponding author.

† These authors contributed equally.

✉ onu_metal@ukr.net (I. Bobok); sngryhorenko@gmail.com (S. Hryhorenko)

ORCID 0000-0003-4548-0709 (I. Bobok); 0009-0006-4551-8243 (S. Hryhorenko)



© 2026 Copyright for this paper by its authors. Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0).

conflicts have convincingly demonstrated that cyberattacks on critical infrastructure are an integral element of hybrid warfare, preceding or accompanying kinetic strikes. Under the conditions of such hybrid conflicts, where information systems become the primary target, ensuring their information security and cyber defense requires not only reliable data encryption but also the very fact of data concealment coming to the forefront. Cryptography renders a message unreadable. Steganography goes a step further by concealing the very existence of the secret message [5–7]. In the context of critical infrastructure, steganography turns into a vital and highly relevant defense tool [8]: when an adversary cannot see the data transmission channel, they cannot attack or block it. During the steganographic embedding process, the secret message undergoes preliminary encoding, resulting in a digital sequence – additional information (AdInf). The AdInf is embedded into an inconspicuous object acting as a container, which in this work is considered to be a digital image (DI). One of the primary requirements for a stego-message – the result of AdInf embedding into a container – is ensuring its perceptual reliability: visually, the container and the stego-message must be indistinguishable [9,10]. Despite the fact that this requirement is intended to hinder the detection of hidden communication, there are currently steganographic methods that fail to systematically ensure it for various reasons [11], leaving the task of guaranteeing high visual quality of the generated stego-message highly relevant. Thus, improving the steganographic system with the aim of enhancing the visual quality of the generated stego-message becomes an important element for fault-tolerant control systems capable of functioning under conditions of direct digital aggression, under which Ukraine continuously finds itself today.

2. Problem Statement

One of the possible ways to solve the problem of meeting specific priority requirements for a steganographic system is to select a container from an available set of candidate DIs [12–16], which is used, in particular, to ensure a relatively high visual quality of the corresponding stego-message.

Artificial Intelligence is widely and successfully applied in this field. In [17], approaches based on convolutional neural networks and end-to-end generative adversarial networks are considered among the primary methods for addressing adaptive image steganography tasks. In [18], a novel approach utilizing an AI-based adaptive steganographic system is proposed, in which the system dynamically adjusts steganographic methods depending on the media format. In [19], a novel cover image selection framework is presented, which involves optimizing within the latent space of pre-trained generative models to identify the most suitable cover images.

However, the cover image selection operation is typically computationally expensive [20] and, in the practical use of a steganographic system – where time and other resources for organizing a covert communication channel may be severely limited (for instance, when using a steganographic system under UAV operational conditions, which is extremely relevant for Ukraine today) – it becomes unfeasible. The properties of the generated stego-message can be improved not only by selecting a container, but also by selecting subregions of an arbitrary (random) container that are most suitable for steganographic transformation.

This issue is the subject of research by many steganography scientists worldwide [21], where ensuring the visual quality of the stego-message arouses the greatest interest as the goal of container subregion selection.

Thus, in [22], a selective method based on a genetic algorithm is proposed, which is applied to determine suitable subregions in the original DI container with the aim of minimizing distortions resulting from the specific steganographic transformation. After determining the target subregions (blocks), the embedding of AdInf – the secret DI – is performed in the discrete cosine transform (DCT) domain of blocks with relatively low energy.

This method is not the only one tailored to a specific steganographic transformation [23–26]; which the authors of the present work consider a significant limitation, as it restricts its scope of application at a time when the number of existing and newly developed steganographic methods is rapidly growing every day.

For instance, in [23], the method of selecting 3×3-blocks of a DI container, obtained as a result of preliminary matrix partitioning, is tailored to steganographic algorithms based on Pixel Value Differencing (PVD). In each block, a median pixel is selected. The quantitative characteristic of the block during selection is defined as the distance between the minimum and maximum difference between the intensity of the median pixel and all other pixels in the block. Priority is given to blocks where this value is maximal. In [24], a method for selecting 2×2-blocks of a DI container is proposed, designed for embedding AdInf using a combination of methods widely used in steganography – PVD and LSB substitution. The authors propose a selective algorithm based on the analysis of the Histogram of Oriented Gradients (HOG) to determine the dominant edge direction for each 2×2-block of the container image. In [25], block selection is carried out with a dual purpose: increasing the capacity of the steganographic channel and ensuring high visual quality of the stego-message. However, this is once again done for a specific hybrid steganographic method based on the LSB method and Hamming code (HLAH). The efficiency of the proposed HLAH method is evaluated by measuring the total volume of embedded information, MSE, PSNR, and by analyzing the intensity histogram of the stego-message. In [26], to search for optimal regions for embedding secret information in order to increase the capacity of the steganographic channel while simultaneously ensuring the perceptual reliability of the stego-message, a selective method is proposed based on the Canny and Sobel edge detection methods. This approach is tailored to a specific steganographic method: the AdInf embedding process is carried out by modifying the most significant bit in the edge regions. Recently, selective methods based on the use of Artificial Intelligence (AI) have become very widespread. Thus, in [27], an effective deep learning-based method for selecting DI blocks to embed secret information is proposed, utilizing the frequency domain of the image – the discrete cosine transform. One of the selection objectives is to ensure the high visual quality of the stego-message. Following the preliminary partitioning of the DI into blocks, semantic and structural features are extracted from each block, making it possible to assess the block's suitability for data embedding. Additionally, the Proximal Policy Optimization algorithm is introduced into the block selection process to learn adaptive embedding policies. The use of neural networks also forms the basis of the method proposed in [28] for big data security. Although AI is continuously expanding its scope of application today, AI-based selective methods are not without significant systemic drawbacks, which can prove to be critical for steganography:

- The operation of a neural network constitutes a “black box”, defining only the “input” (the DI container) and the “output” (the set of container blocks). If this selection is, for any reason, unsatisfactory – making targeted changes to improve the network's performance is difficult to implement, and more often unfeasible;
- The efficiency of a neural network depends heavily on the training dataset: when attempting to use a DI that is atypical or outside the scope of the training dataset as a container, the selective method may operate incorrectly without providing any indication or signaling of the error;
- In selective steganography, ensuring the synchronization process is critically important. In practice today, “blind” steganographic methods are most commonly used, which do not require knowledge of the original container to extract the secret message. If the stego-message undergoes even minor attacks against the embedded message during transmission – which occurs quite frequently in practice – the receiver's selection process may identify the wrong blocks instead of those where the AdInf was actually embedded, leading to critical distortion of the extracted AdInf.

It should be noted that for selective steganography, any error in selecting even a single block – given the necessity of synchronization to ensure AdInf decoding – can lead to a catastrophic distortion of the entire hidden message or to an increased probability of detecting the covert

communication. Taking all the above into consideration, the authors of this work are convinced that the use of AI within selective steganography is currently not preferable, and that rigorous mathematical substantiations of the performed selection are required, along with a clear understanding of its outcomes. As noted above, a significant drawback of a selective method is its tailoring to a specific steganographic transformation (if this is the case). With this in mind, it is desirable to develop general (universal) selection principles that would be independent of the specifics of the steganographic algorithm used. Such a method, based on a general approach to analyzing the state of information systems [29–31], was recently proposed in [32]. Here, the selection of DI container blocks is performed to enhance the qualitative and quantitative metrics of the perceptual reliability of a stego-message generated by an arbitrary steganographic algorithm, ensuring its operability under random container conditions without any modifications to the algorithm itself. In that work, the image is mapped to a directed graph corresponding to a binary equivalence relation defined on the set of container blocks, which partitions this set into equivalence classes. The study substantiates the feasibility of using the normalized separation of its maximum singular value (NSMSV) as an integral quantitative characteristic of a block for selection purposes. The proposed algorithm for selecting DI container blocks allowed for a significant increase (by 2–6 dB) in the quantitative metric of DI distortion – PSNR – for most of the images used, compared to a random selection of blocks for AdInf embedding across various steganographic methods. This demonstrates in practice that a universal selection principle can indeed ensure high selection efficiency.

3. Aim and Objectives of the Paper

Hierarchy is one of the most general classification methods used by humans. Hierarchical structures are effectively utilized in modeling real-world processes across many areas of human activity [29].

In light of the above, the aim of this paper is to enhance the efficiency of the steganographic system by improving the process of selecting the DI container blocks most preferable for steganographic transformation, independent of the steganographic method used for AdInf embedding, based on the development and subsequent utilization of a hierarchical image structure.

The efficiency of the steganographic system in this work is evaluated by a quantitative metric of the visual quality of the generated stego-message – Peak Signal-to-Noise Ratio [9].

To achieve this aim, the following objectives are addressed in the study:

1. Development of a hierarchical DI structure, taking into account the domain of its further application;
2. Formulation of the principles for constructing a graph that corresponds to the hierarchical DI structure.

4. Hierarchical Structure of a DI

Hierarchical classification reproduces the primary form of coordination or organization. The main task within a hierarchy is to evaluate the higher levels based on the interaction of various hierarchical levels, rather than on a direct dependence on the elements at these levels. Through hierarchical composition, one essentially avoids the direct comparison of the large and the small [33]. Furthermore, hierarchical models possess a number of significant advantages over other types of models [29,34], which are highly important for solving problems in the field of information security [29]:

- They enable the investigation of the “degree of influence” that priorities at the upper levels have on the priorities of elements at the lower levels;
- They provide detailed information about the structure of the system;

- They are flexible (additions to a well-structured hierarchy do not disrupt its characteristics).

Hierarchical structures play an important role in the modeling process of various objects in the field of information security, including secure information systems [29]. Complex technical systems are generally characterized by a hierarchical organizational principle. Hierarchy allows for the analysis of an object/system simultaneously at different levels of granularity – ranging from the global properties of the entire object/system to the local properties of individual components. This is fundamentally important for selective steganography, as it will ensure flexibility in choosing the AdInf embedding region: given a hierarchical structure of the container, it will naturally define the selection space – indicating at which level and in which specific subregions the hidden information should be placed. Let us rigorously define the concept of a hierarchy [35].

Let “ $\leq$ ” be a binary relation of a non-strict order on some set S [36]. For any relation $x \leq y$, where $x, y \in S$, one can define the relation $x < y$, which means $x \leq y$ and $x \neq y$. It is said that y covers x if $x < y$ and there exists no such $t \in S$ that $x < t < y$.

Let X be a finite partially ordered set [36] with the greatest element $\bar{x}$. The set X is a hierarchy if there exists a partition of X into subsets L_k , $k = \overline{1, h}$, where $L_1 = \{\bar{x}\}$, such that the following conditions are satisfied:

$$(x \in L_k) \Rightarrow (x^- \subset L_{k+1}, k = \overline{1, h-1}), \text{ where } x^- = \{y \mid x \text{ covers } y\}; \quad (1)$$

$$(x \in L_k) \Rightarrow (x^+ \subset L_{k-1}, k = \overline{2, h}), \text{ where } x^+ = \{y \mid y \text{ covers } x\}. \quad (2)$$

Let us consider a DI with an $n \times n$ -matrix F . We partition the DI in a certain manner into non-overlapping blocks $B_k^{(1)}$, $k = \overline{1, m_1}$. Similarly, for each block $B_k^{(1)}$, $k = \overline{1, m_1}$, we construct its partition into non-overlapping blocks $B_k^{(2)}$, $k = \overline{1, m_2}$, and so on. In principle, the process can be stopped at any moment or continued until, at a certain s -th step, the block $B_k^{(s)}$ is defined by a single pixel. On the resulting set R of DI blocks, we define a binary relation ρ (“to consist of”):

$$B_{k_1}^{(s_1)} \rho B_{k_2}^{(s_2)} \Leftrightarrow B_{k_1}^{(s_1)} \subset B_{k_2}^{(s_2)}, \quad (3)$$

which is irreflexive (since the inclusion “ $\subset$ ” in (3) is strict), antisymmetric, and transitive, i.e., a strict order relation. Since not any two blocks of the set R are comparable with respect to the order relation ρ , the set R is partially ordered. Each block $B_k^{(i)} \in R$ obtained at the i -th step of the sequential partitioning procedure can cover only some of the blocks obtained at the $(i+1)$ -th step, while being covered by a unique block obtained at the $(i-1)$ -th step. Thus, for the set R , there exists a partition into subsets L_r , $r = \overline{1, s}$ such that conditions (1) and (2) are satisfied for L_r ; moreover, $L_1 = \{F\}$ and $L_r = \{B_1^{(r)}, B_2^{(r)}, \dots, B_{m_r}^{(r)}\}$, meaning that the set R represents a hierarchy, which is graphically illustrated in Fig. 1.

In modern selective steganography methods, the selection of DI container blocks is generally performed based on a pre-established, stationary partitioning of the image matrix. In this case, however, it is fundamentally impossible to trace how the degree of texture varies within the block itself, even though a block may also contain areas with higher and lower degrees of texture – which, in turn, determine the more and less suitable subregions for AdInf embedding within that block. Let us consider this in detail using the example of the selective method proposed in [32], which substantiates the feasibility of using the NSMSV of a block $svdgap_n(1)$ as a quantitative selection criterion to ensure a (comparatively) high visual quality of the generated stego-message:

$$svdgap_n(1) = \bar{\sigma}_1 - \bar{\sigma}_2, \quad (4)$$

where $\bar{\sigma}_1, \bar{\sigma}_2$ are the normalized singular values of the block, determined in accordance with the formula: $\bar{\sigma}_i = \sigma_i / \|\sigma\|, i=1,2$, where $\|\sigma\|$ is the vector norm of $\sigma = (\sigma_1, \sigma_2, \dots, \sigma_l)^T$, and $\sigma_1, \sigma_2, \dots, \sigma_l$ are the singular values of the $l \times l$ -block. When considering a stationary block structure, we are not immune to selecting a block for which the NSMSV is (relatively) insignificant. However, such a positive (relative) characteristic might be achieved merely due to the presence of a small subregion within the block that has highly pronounced texture, while homogeneous parts – undesirable for use in the steganographic transformation process – are also present. An example of this will be demonstrated below.

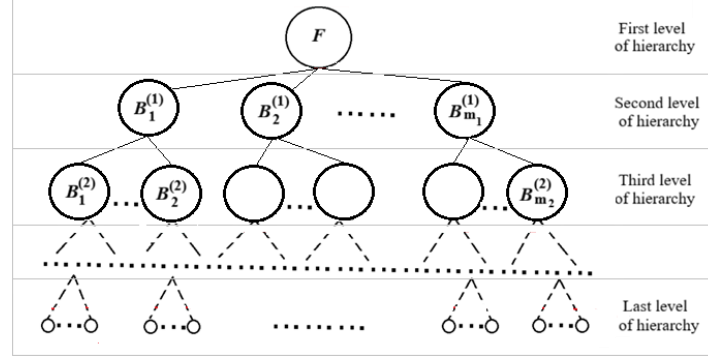


Figure 1: Hierarchical structure of the DI corresponding to the binary relation (3)

The proposed hierarchical DI structure allows one to delve “deep” into the block by advancing to its subsequent levels, and there discard the smaller sub-blocks that represent (relatively) homogeneous regions. Thus, the hierarchical DI structure will enable a deeper analysis of the properties of individual blocks for selecting priority container subregions for AdInf embedding. It allows for the examination of their “internal components” step by step, descending through the levels of the structure down to individual pixels, and, consequently, should provide the opportunity (when utilized) for a higher-quality selection of subregions.

5. Graph Corresponding to the Hierarchical Structure of a DI

We map the constructed hierarchical DI structure to a directed weighted graph $\Gamma(V, E)$ (where V is the set of vertices and E is the set of edges), where the vertices of the graph correspond to the elements (blocks) of the hierarchical structure, and for an edge $\langle B_{k_1}^{(s_1)}, B_{k_2}^{(s_2)} \rangle$ of the graph $\Gamma(V, E)$ to exist, the following condition must be satisfied:

$$\langle B_{k_1}^{(s_1)}, B_{k_2}^{(s_2)} \rangle \in E \Leftrightarrow (s_2 = s_1 + 1) \& (B_{k_1}^{(s_1)} \rho B_{k_2}^{(s_2)}). \quad (5)$$

As the weight coefficient of vertex $\Gamma(V, E)$, the NSMSV (4) is used in this work for definiteness, taking into account [32], although any other parameter characterizing the degree of block texture could also be utilized. Hereinafter, the NSMSV of object A is denoted as $G(A)$ (Fig. 2).

Obviously, the resulting graph is acyclic. It should be noted that $\Gamma(V, E)$ is not the graph of the binary relation (3), since it does not account for the existing connections between elements of non-consecutive levels of the hierarchy; for example, vertex F in the graph of the binary relation would be adjacent to all other vertices of graph $\Gamma(V, E)$, having edges (5) merely as a subset of all edges incident to it. In practice, the level of granularity of the hierarchical structure of the container and, consequently, of graph $\Gamma(V, E)$ used during block selection, will be determined by:

- The capacity of the covert communication channel: The number of selected blocks must be sufficient to embed the AdInf;
- The specifics of the steganographic algorithm used: The minimum block size must allow for AdInf embedding and must contain the required number of parameters used for the embedding process. For example, if AdInf embedding requires singular vectors that correspond to singular values with indices greater than 2 [37], then the blocks must have a size greater than 2;
- The characteristics of the DI container used: If the DI container features large homogeneous regions and a relatively large volume of AdInf needs to be embedded, this will necessitate the use of small-sized blocks for the steganographic transformation.

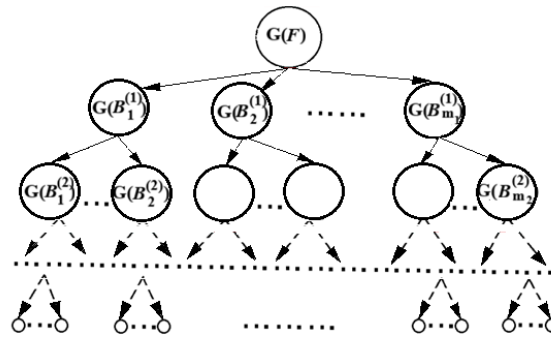


Figure 2: Graph corresponding to the hierarchical structure of a DI

An example of a graph for a specific DI with a size of 160×160 pixels, corresponding to the first three levels of its hierarchical structure to demonstrate the advantages of block selection considering the hierarchical structure of the DI container, is presented in Fig. 3.

The last, fourth 80×80 block (Fig. 3(c)), which has the minimum NSMSV among all blocks of this partitioning level, equal to 0.8314, has the highest priority for use in the steganographic transformation process, since the relative contribution of the high- and mid-frequency components within it is generally the maximum among the four 80×80 blocks. Without further analysis of the DI hierarchy, this entire block could be selected for AdInf embedding. However, a constituent part of this block is a 40×40 sub-block (Fig. 3(d)), for which the NSMSV is so significant (0.9687) that it exceeds the NSMSV of all 40×40 sub-blocks of the 80×80 block with a value of 0.9293, which holds the lowest priority among all 80×80 blocks.

Thus, when considering the quantitative characteristics of only a single level to evaluate the “suitability” of a block for steganographic transformation, a fully objective assessment of its “suitability” may not be achieved. This can affect not only the visual quality of the stego-message but also, consequently, the capacity of the covert channel.

It should be noted that a stationary partitioning of the container matrix into very small blocks (corresponding to the bottom level when using a hierarchical structure) and searching among them for those suitable for AdInf embedding – which, at first glance, might seem to yield a comparable final block selection result – is less advantageous compared to the hierarchical approach due to the following reasons.

First, the stationary approach can significantly increase the computational overhead when implementing small block sizes. A small block size increases the total number of blocks upon partitioning, which in turn can lead to an increase in the computational complexity of such a block-based method. Although remaining polynomial of degree 2, it increases the coefficient of the leading term in the function that relates the number of arithmetic operations to the input data size. Conversely, utilizing a hierarchical structure allows discarding those parts of the DI that are undesirable for steganographic transformation – namely, (relatively) large homogeneous blocks (the

NSMSV for such blocks will be close to unity) – at the very first steps of the selection process. This reduces the selection “field” at its earliest stages and, consequently, lowers the computational complexity of choosing suitable blocks. We refer to this advantage of hierarchical block selection as “controlled computational complexity”.

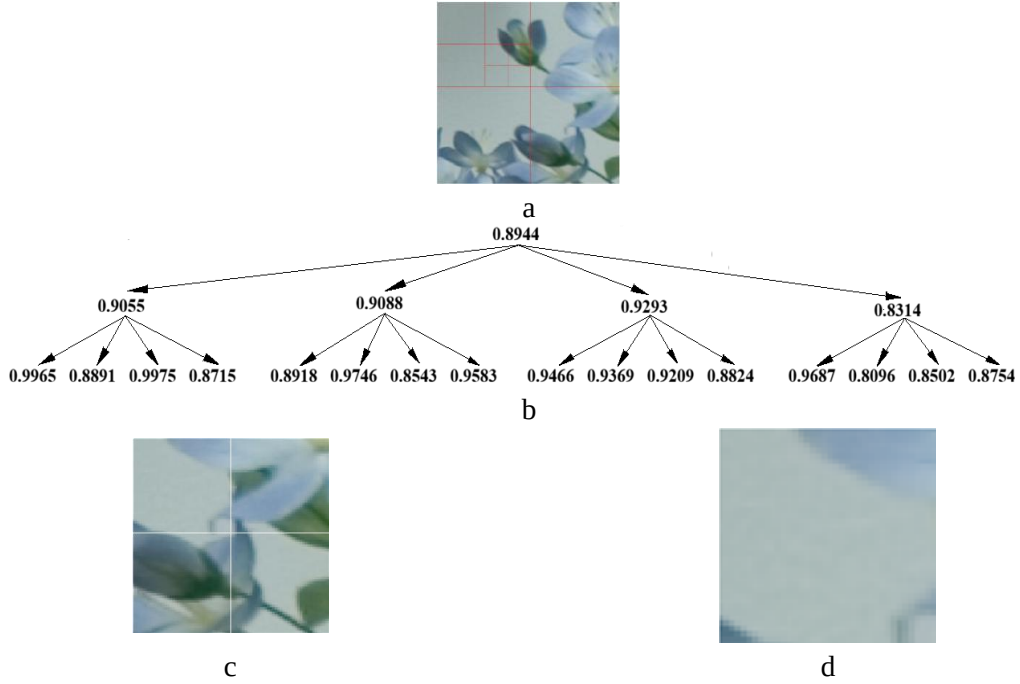


Figure 3: Construction of the graph corresponding to the hierarchical DI structure: a – original DI; b – graph corresponding to the first three levels of the hierarchical DI structure; c – 80×80 DI block with the minimum NSMSV; d – 40×40 sub-block of the block shown in Fig. 3(c), undesirable for steganographic transformation

Notably, controlled computational complexity enables the hierarchical selection process to be terminated at a specific level of the structure without significant detriment to the quality of the resulting stego-message (e.g., under critical time constraints). For stationary partitioning, the selection process cannot be stopped until the quantitative characteristics of all (small) blocks have been analyzed, which formally corresponds to evaluating the bottom level of the container's hierarchical structure without the ability to dynamically discard upper-level blocks due to their unsuitability for steganographic transformation. Second, with a stationary partitioning of the DI container matrix into small blocks, a situation may arise where their analysis becomes uninformative in terms of achieving the objective of the selection process (i.e., the visual quality of the stego-message). This is due to the following: for original DIs captured by physical digital cameras, object contours are most often defined not by a pair of adjacent pixels where the luminance function undergoes a single significant leap, but rather by a group of adjacent pixels. In this case, if small block sizes are used and their boundaries coincide with the edges of the contour, the presence of the contour itself may be lost, which subsequently reduces the capacity of the generated steganographic channel. While this can also occur when using a hierarchical DI structure, the multilevel structural analysis solves this problem: the presence of a contour will be signaled by the block level of the previous hierarchy tier. This higher-level block will then be utilized as a whole for AdInf embedding, whereas its constituent blocks at the next level of the hierarchy will not be processed as separate objects for steganographic transformation. This is critically important for block-based steganographic methods, which constitute the majority of state-of-the-art techniques [38–40].

Third, with a stationary partitioning of the DI into small blocks, large areas with a high degree of texture – which are “ideal” for AdInf embedding – may be lost. This is demonstrated in Fig. 4, where, for instance, an 80×80 block (Fig. 4(a), highlighted by a red contour) possesses a high degree of

texture (which is obvious even from a subjective evaluation), as evidenced by its NSMSV $svdgap_n(1) = 0.8720$. However, if we take 4×4 or 2×2 blocks from this exact same 80×80 container subregion, they fail to signal the texture of this subregion due to their minuscule size, as demonstrated by the histograms of the normalized separation values of the maximum singular value for the blocks within this 80×80 subregion (Fig. 4(b, c)). If such blocks were evaluated under a stationary partitioning approach, most of them would be discarded, leading to a significant reduction in the capacity of the covert communication channel.

Thus, a hierarchical structure that reflects the connections among its elements both “top-down” and “bottom-up” provides the opportunity not only to reduce the number of operations but also to prevent a falsely justified reduction in the capacity of the covert communication channel (wherever possible, by accounting for the properties/normalized separation values of larger blocks at the previous level). When discussing the perceptual security of the generated stego-message, we incorporate a human subjective evaluation into the steganographic system's property assessment framework. This evaluation accounts for the specific characteristics of the human visual system, which to date have not been fully formalized. Moreover, given the psychological factors influencing human assessment, a complete formalization is unlikely ever to be achieved in a strict mathematical sense, as the human psyche involves a vast array of variables, many of which remain hidden today. In this context, we can only speak of a dynamic probabilistic model of human perception.

Considerable effort by contemporary researchers is currently directed toward predicting human visual attention [41–43], which is often accomplished using Salient Object Detection – identifying the object or region in a DI that most strongly attracts human attention. As a rule, such regions are characterized by a high degree of contrast (e.g., a red apple on green grass), a unique texture (a smooth object against a highly textured background, or vice versa), and/or a specific positioning of the object within the boundaries of the depicted scene (e.g., isolation, such as a solitary bird in the sky). The results of these studies must be taken into account in steganography [44]. Given that a Salient Object is typically defined by contour lines – i.e., by significant transitions in pixel luminance values, which from a steganographic perspective hold priority for AdInf embedding – and considering the characteristics of the human visual system, it is advisable not to use the Salient Object for AdInf embedding, since it is highly likely to be under the most intense scrutiny of an observer. This introduces a contradiction regarding the use of object contours (regions of significant luminance changes) for steganographic transformation aimed at ensuring the perceptual security of the stego-message. However, upon closer examination, when utilizing block selection, this contradiction proves not to be critical:

- First, when it comes to a subjective attack by a stegoanalyst aimed at detecting the presence of artifacts in a DI, they pay equal attention to all parts of the image;
- Second, in practice, determining a Salient Object for an arbitrary DI is not a task with a single, unambiguous solution due to the inherent characteristics of the human psyche;
- Third, block selection identifies blocks rather than specific pixels. Even when using the proposed hierarchical DI structure, “descending” to the pixel level will not occur. The degeneration of blocks into individual pixels would severely limit the applicability of the corresponding selective method, given that the vast majority of modern steganographic techniques are block-based. The integral characteristic of a block used during selection (such as the NSMSV) accounts, to a greater or lesser extent, for the behavior of pixels within the neighborhood of each individual pixel;
- Fourth, the identification of Salient Object blocks in a DI is not a significant event for steganographic block selection when using the proposed hierarchical DI structure. This is because, by moving down the structure and continuing to analyze the characteristics of

smaller blocks, it becomes possible to examine the Salient Object from the inside, thereby determining which of its internal parts are suitable or unsuitable for steganographic transformation. If a constituent block B of a Salient Object represents a subregion with a relatively large/small (or zero) contribution of the high-frequency component, then B will/will not be included in the set of blocks recommended for AdInf embedding, regardless of whether it belongs to the Salient Object or not. Similar reasoning applies to DI regions that do not contain a Salient Object. Here, the hierarchical approach (descending deep into the structure) acts as an arbiter that determines a container subregion worthy of steganographic transformation, regardless of whether it belongs to the Salient Object or the “background”;

- Fifth, in [42], when solving problems from psychological vision science research – which is an integral part of studies aimed at ensuring the visual quality of stego-messages – it is substantiated that the analysis of small blocks must be governed by the overall context of the image. In essence, this constitutes taking the DI hierarchy into account. In light of the proposed hierarchical structure, it can be interpreted as accounting for the influence of the covering elements (1) of the block set on the covered elements (2).

All of this indicates that for selective steganography, even when accounting for the subjectivity of the human visual system, instead of dividing the DI into a “Salient Object” and “background” [41–43], it is significantly more advantageous to partition it into hierarchy levels based on its degree of spatial heterogeneity. The advantages of using the hierarchical DI structure for the selection of its blocks are demonstrated in Fig. 5 for an artificially generated 32×32 DI (Fig. 5(a)). Let us assume that this DI is used to embed 7 bits of AdInf using a block-based steganographic method, where one container block is utilized to embed 1 bit. Equation (4) is used as the quantitative criterion for block selection. With a stationary partitioning of the DI into blocks, it is obvious that the number of these blocks must, in any case, be no less than seven. When partitioning into 8×8 blocks, the blocks indicated by gray shading in Fig. 5(c) would be utilized for the steganographic transformation. However, when using a hierarchical structure (Fig. 5(d)) that includes 4×4 blocks at the bottom level, the selection result would be different. Already within the second level of the structure, the 16×16 block with $NSMSV = 0.9981$ would be discarded, as would two 8×8 blocks at the third level, since their $NSMSV$ are close to unity (the discarded blocks in Fig. 5(d) are shaded in lilac). This significantly reduces the number of 4×4 blocks (by 37.5%) analyzed at the bottom level of the hierarchy, compared to their quantity under a stationary partitioning of the DI into 4×4 blocks. It should be noted that the 4×4 blocks selected at the bottom level of the hierarchical structure (shaded in gray in Fig. 5(d)) are by no means all included within the 8×8 blocks resulting from the selection under stationary partitioning of the DI into 8×8 blocks (shaded in yellow in Fig. 5(d)). Furthermore, the second selection option yields a better result when using these blocks in the steganographic transformation process:

- For the Koch and Zhao method [9], the gain in the PSNR metric was 4% (PSNR increased from 38.2 dB for selection with stationary partitioning to 39.7 dB for selection considering the hierarchical structure);
- For the method in [11], the gain was 3% (PSNR increased from 37.5 dB for stationary partitioning to 38.6 dB for the hierarchical structure).

To empirically validate the advantages of using a hierarchical DI structure for block selection, a computational experiment was conducted in which the above-described procedure was applied to 950 DIs. These images varied in genre, texture, dimensions, and storage formats (lossless (TIFF) and lossy (JPEG)), acquired using both professional and consumer cameras, including 52 AI-generated DIs. During the experiment, no instances were recorded in which the PSNR value for the stego-

message obtained via hierarchical block selection was lower than that obtained via direct selection. On average, the gain in the PSNR metric amounted to 2.7%.

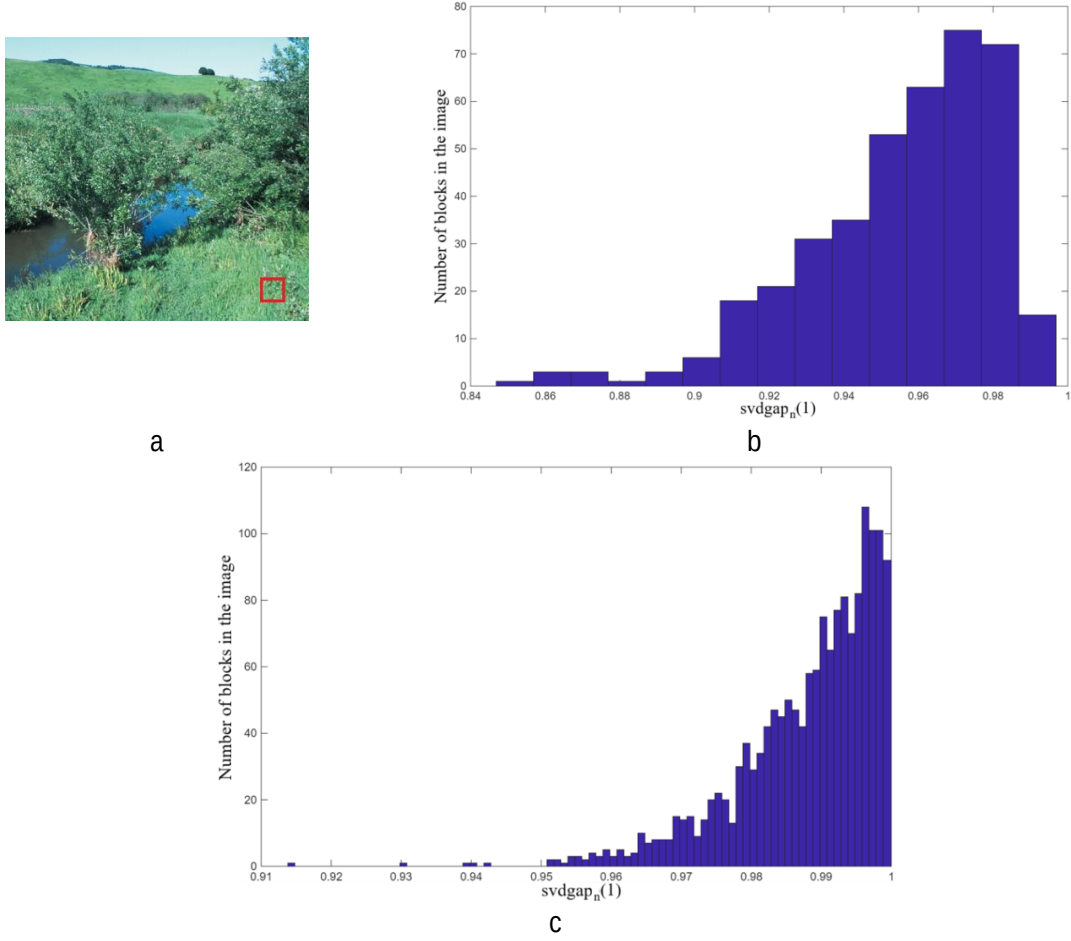


Figure 4: Example of a possible negative block selection outcome in the case of stationary container partitioning: a – DI container with a highlighted 80×80 block featuring a high degree of texture; b – histogram of $svdgap_n(1)$ values for 4×4 blocks within the highlighted region; c – histogram of $svdgap_n(1)$ values for 2×2 blocks within the highlighted region

Thus, we arrive at a confirmation of the practical expediency of the hierarchical method for selecting DI subregions for AdInf embedding, which is based on the proposed hierarchical container structure. The utilization of the hierarchical DI structure in block selection effectively combines coarse (initial) and deep (local) selection into a single process. Notably, discarding blocks at the upper levels of the hierarchical structure when the NSMSV is close to unity is fully justified during block selection. A NSMSV close to unity indicates the absence or extreme insignificance of the high-frequency component, thereby signifying the homogeneity of the block. While discarding a small-sized block (2×2 or 4×4) might lead to overlooking a portion of a contour defined by a cluster of adjacent pixels, for a larger block, a value close to unity serves as a reliable signal of its homogeneity and the clear unsuitability of its use for AdInf embedding. *Remark.* The proposed hierarchical DI-container structure and the corresponding graph – which allow for a “coarse” selection followed by its subsequent “refinement” – serve as a universal tool for achieving any arbitrary selection objective, rather than solely ensuring a (relatively) high visual quality of the resulting stego-message. Indeed, the selection objective is directly reflected by the weight coefficients of the graph vertices: specifically, their semantic meaning and the method used to determine them. For instance, the weight coefficients used in this work are a quantitative indicator of the block's degree of texture, making it possible to ensure a (comparatively) high visual quality of the stego-message. If, however, we consider the volume of protected information [12, 13] as the block's weight coefficient, then the

constructed hierarchical structure can be utilized for block selection aimed at obtaining a stego-message with a (comparatively) high robustness against attacks targeting the embedded message.

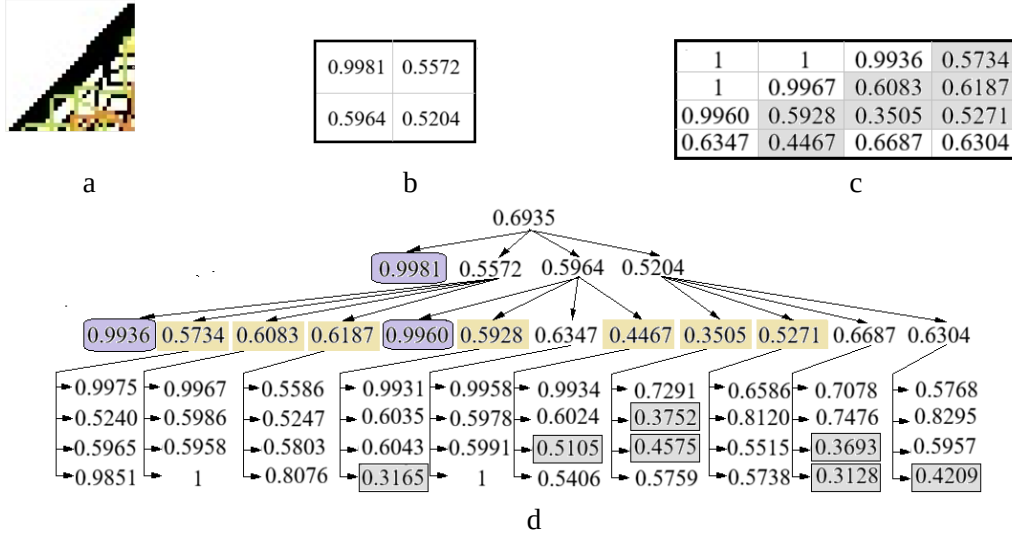


Figure 5: Example of using stationary and hierarchical partitioning for container block selection: a – 32×32 DI container; b – result of partitioning into 16×16 blocks, indicating the NSMSV for each block; c – result of partitioning into 8×8 blocks, indicating the NSMSV for each block, with the blocks selected for steganographic transformation highlighted by gray shading; d – graph corresponding to the hierarchical DI structure

6. Conclusions

To enhance the efficiency of the steganographic system – which is evaluated by the visual quality metric of the generated stego-message – this work proposes an improvement to the DI-container block selection process, during which:

- A hierarchical DI structure is developed based on the strict order binary relation “consists of”, defined on the set R of image blocks, which establishes its partial ordering. The hierarchical DI structure allows for an in-depth analysis of the properties of individual blocks to select priority container subregions for AdInf embedding by examining their internal components;
- Principles are developed for constructing a directed weighted graph corresponding to the hierarchical DI structure. This enables block selection for steganographic transformation by conducting structural analysis both top-down and bottom-up. Consequently, this makes it possible to exclude relatively large blocks – whose involvement in the steganographic transformation is undesirable – at the initial levels of the hierarchical structure, thereby reducing the “search space” and, as a result, the computational costs of the selection process;
- The proposed hierarchical structure of the DI container and the corresponding graph – which allow for a “coarse” selection followed by its subsequent “refinement” – serve as a universal tool for achieving any arbitrary selection objective, which is reflected by the weight coefficients of the graph vertices;
- The use of the hierarchical structure graph for selecting DI container blocks with the specific objective of ensuring a (relatively) high visual quality of the stego-message made it possible to improve the quantitative distortion metrics (PSNR) of the container resulting from steganographic transformation – regardless of its specific type – by 2.7% compared to selection under stationary block partitioning.

The concept of hierarchical selection for DI container blocks has been implemented in a new, efficient selective method developed by the authors of this paper, the details of which are currently in preparation for publication.

Declaration on Generative AI

The authors have not employed any Generative AI tools.

References

- [1] 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.
- [2] 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>
- [3] 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>
- [4] S. Mukherjee, Implementing cybersecurity in the energy sector, 2019. URL: <https://doi.org/10.6084/m9.figshare.9728051>
- [5] 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>
- [6] 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>
- [7] S. Pramanik, M.M. Ghonge, R.V. Ravi (Eds.), *Multidisciplinary Approach to Modern Digital Steganography*, Information Science Reference, 2021.
- [8] M.A. Bamanga, A.K. Babando, M.A. Shehu, Recent Advances in Steganography, in J. Mayer (Ed.), *Steganography – The Art of Hiding Information*, IntechOpen, 2024. doi: 10.5772/intechopen.1004521
- [9] G. Konakhovich, D. Progonov, O. Puzyrenko, *Steganographic Processing and Analysis of Multimedia Data*, Center for Educational Literature, 2018.
- [10] W. Luo et al., A comprehensive survey of digital image steganography and steganalysis, *APSIPA Transactions on Signal and Information Processing* 1 (2024) 1–67. URL: <https://doi.org/10.1561/116.20240038>
- [11] M.A. Melnik, Compression-resistant steganography algorithm, *Information Security* 2 (2012) 99–106.
- [12] I. Bobok, A. Kobozeva, S. Sokalsky, The problem of choosing a steganographic container in conditions of attacks against an embedded message, *Problemele Energeticii Regionale* 4 (2022) 74–88. URL: <https://doi.org/10.52254/1857-0070.2022.4-56.07>.
- [13] I. Bobok, A. Kobozeva, S. Sokalskiy, Improving the steganographic container selection method for enhancing system robustness against embedded message attacks, *Radioelectronics and Communications Systems* 3 (2025) 135–152. URL: <https://doi.org/10.20535/S0021347025030045>
- [14] M.S. Subhedar, Cover selection technique for secure transform domain image steganography, *Iran J Comput Sci* 4 (2021) 241–252. URL: <https://doi.org/10.1007/s42044-020-00077-9>

- [15] M. Azam et al., A systematic review on cover selection methods for steganography: Trend analysis, novel classification and analysis of the elements, *Computer Science Review* 56 (2025) 100726. URL: <https://doi.org/10.1016/j.cosrev.2025.100726>
- [16] I.I. Bobok, S.M. Hryhorenko, A.A. Koboziyeva, K.L. Yavorska, Improving steganosystem efficiency as an integral part of ensuring the routine operation of energy infrastructure facilities, *Problemele Energeticii Regionale* 2 (2026) 78–93. URL: <https://doi.org/10.52254/1857-0070.2026.2-70.07>
- [17] A.A.M. Fadhl, H.O.M. Shareif, M.A.E. Ali, A.M.A. Elmangoush, Adaptive image steganography: A review and research directions, in: *Proceedings of the 2024 IEEE 7th International Conference on Advanced Technologies, Signal and Image Processing (ATSIP)*, Sousse, Tunisia, 2024, pp. 494–499. doi: 10.1109/ATSIP62566.2024.10638907.
- [18] I. Kala, S. Carol, D. Krishna Kumar, V.A. Nehya Ragavan, AI-powered adaptive steganography, in: *Proceedings of the 1st International Conference on Smart System for Integrated Computing and Communication (ICSSICC 2024)*, Coimbatore, India, 2024, pp. 328–340. doi: 10.1007/978-3-031-99939-0_26
- [19] K. Chahine, H. Kim, Neural cover selection for image steganography, in: *Proceedings of the 38th International Conference on Neural Information Processing Systems (NIPS'24)*, Vancouver, Canada, 2024, pp. 70875–70904.
- [20] X. Li, D. Guo, C. Qin, Diversified cover selection for image steganography, *Symmetry* 11 (2023) 2024. URL: <https://doi.org/10.3390/sym15112024>
- [21] J. Han, G. Ye, S. Han, An image steganography algorithm using selective timestep embedding and diffusion model, *Expert Systems with Applications* 310 (2026) 131313. URL: <https://doi.org/10.1016/j.eswa.2026.131313>
- [22] S. Joshi, K.V. Sonawane, Selection of image blocks using genetic algorithm and effective embedding with DCT for steganography, in: *Proceedings of the 9th Annual ACM India Conference (COMPUTE '16)*, New York, USA, 2016, pp. 161–166. doi: 10.1145/2998476.2998495
- [23] O. Hosam, N. Ben Halima, Adaptive block-based pixel value differencing steganography, *Security Comm. Networks* 9 (2016) 5036–5050. URL: <https://doi.org/10.1002/sec.1676>.
- [24] M.A. Hameed, M. Hassaballah, S. Aly, A.I. Awad, An adaptive image steganography method based on histogram of oriented gradient and PVD-LSB techniques, *IEEE Access* 7 (2019) 185189–185204. URL: <https://doi.org/10.1109/ACCESS.2019.2960254>.
- [25] Y. Wang, M. Tang, Z. Wang, High-capacity adaptive steganography based on LSB and Hamming code, *Optik* 213 (2020) 164685. URL: <https://doi.org/10.1016/j.ijleo.2020.164685>
- [26] S.M. Ismail, F.E. AbuAladas, M. Abu Helou, W. Abu-ulbeh, Edge-adaptive high-capacity image steganography using hybrid edge detection and MSB embedding, *Computers* 3 (2026) 141. URL: <https://doi.org/10.3390/computers15030141>
- [27] R. Yang, L. Liu, B. Han, F. Hu, Deep reinforcement learning-based DCT image steganography, *Mathematics* 19 (2025) 3150. URL: <https://doi.org/10.3390/math13193150>
- [28] B.M. Issac et al., Deep learning steganography for big data security using squeeze and excitation with inception architectures, *Sci Rep* 15 (2025) 31193. URL: <https://doi.org/10.1038/s41598-025-16394-7>
- [29] Новая монографія S.V. Milevskyi, Integrated methodology for the detection, analysis, and neutralization of threats in the sphere of national security and defense, NTU “KhPI”, 2026.

- [30] I.I. Bobok, A.A. Kobozieva, 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>
- [31] 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>
- [32] A. Kobozieva, I. Bobok, O. Laptiev, V. Savchenko, Application of graph theory to ensure the reliability of steganographic message perception in the creation of a covert communication channel, in: *Proceedings of the 13th International Conference on Information Control Systems & Technologies (ICST 2025)*, Odesa, Ukraine, 2025, pp. 94–108.
- [33] H.A. Simon, The architecture of complexity, in: *Facets of Systems Science. International Federation for Systems Research International Series on Systems Science and Engineering*, vol. 7., Springer, 1991, pp. 457–476. doi: 10.1007/978-1-4899-0718-9_31
- [34] T.L. Saaty, L.G. Vargas, *Models, Methods, Concepts & Applications of the Analytic Hierarchy Process* (2nd Ed.), Springer, 2022.
- [35] J. Wu, Hierarchy theory: An overview, in: R. Rozzi, S. Pickett, C. Palmer, J. Armesto, J. Callicott (Eds.), *Linking Ecology and Ethics for a Changing World. Ecology and Ethics*, vol 1., Springer, 2013, pp. 281–301. doi: 10.1007/978-94-007-7470-4_24
- [36] G. Haggard, J. Schlipf, S. Whitesides, *Discrete Mathematics for Computer Science*, Brooks Cole, 2005.
- [37] C. Bergman, J. Davidson, Unitary embedding for data hiding with the SVD, 2005. URL: <https://dr.lib.iastate.edu/handle/20.500.12876/54635>
- [38] H.-Y. Wu, L.-H. Chen, Y.-T. Ching, Block-based steganography method using optimal selection to reach high efficiency and capacity for palette images, *Applied Sciences* 21 (2020) 7820. URL: <https://doi.org/10.3390/app10217820>
- [39] H. Rahman, H. Syarif, D. Wahono, N.J. de La Croix, T. Ahmad, A steganographic method based on pixel block differences in grayscale images, in: *Proceedings of the 2023 3rd International Conference on Smart Generation Computing, Communication and Networking (SMART GENCON)*, Bangalore, India, 2023, pp. 1–6. doi: 10.1109/SMARTGENCON60755.2023.10442053.
- [40] A. Patel, D. Vekariya, An efficient image steganography method using block-based indexing and LSB substitution, *Journal of Innovative Image Processing* 2 (2026) 536–557. URL: <https://doi.org/10.36548/jiip.2026.2.006>.
- [41] J. Kim, S. Lee, Deep learning of human visual sensitivity in image quality assessment framework, in: *Proceedings of the 2017 IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, Honolulu, HI, USA, 2017, pp. 1969–1977. doi: 10.1109/CVPR.2017.213.
- [42] N. Liu, N. Zhang, K. Wan, L. Shao, J. Han, Visual saliency transformer, in: *Proceedings of the 2021 IEEE/CVF International Conference on Computer Vision (ICCV)*, Montreal, Canada, 2021, pp. 4702–4712. doi: 10.1109/ICCV48922.2021.00468.
- [43] J. Lou, H. Lin, D. Marshall, D. Saupe, H. Liu, TranSalNet: Towards perceptually relevant visual saliency prediction, *Neurocomputing* 494 (2022) 455–467. URL: <https://doi.org/10.1016/j.neucom.2022.04.080>
- [44] P. Luo, J. Liu, Q. Dang, D. Mu, Robust image steganography in online social networks via neural style transfer, *Mathematics* 4 (2026) 629. URL: <https://doi.org/10.3390/math14040629>