Improving Steganosystem Efficiency as an Integral Part of Ensuring the Routine Operation of Energy Infrastructure Facilities

[1]Bobok I.I., [1]Hryhorenko S.M., [2]Kobozieva A.A., [2]Yavorska K.L.
[1]Odesa Polytechnic National University, Odesa, Ukraine
[2]Odesa National Maritime University, Odesa, Ukraine

Abstract. Steganography currently holds a vital position in information security, reflecting its growing importance within the energy industry. Steganographic methods are employed to ensure data integrity and authentication in Smart Grids; for the authentication of thermograms and diagnostic images obtained during power line monitoring, etc. The effectiveness of a steganographic system fundamentally depends on the properties of the container used, making the task of container selection highly relevant, yet one that has lacked a satisfactory solution until now. The objective of this work is to increase the efficiency of a steganographic system by developing a method for selecting a container from a given set of digital images, ensuring optimal or near-optimal visual quality of the stego-message, regardless of the container format or the steganographic method employed. In this study, steganographic efficiency is defined as a quantitative assessment of the perceptual reliability of the generated stego-message, evaluated using the Structural Similarity Index Measure (SSIM). This objective was achieved by addressing the following tasks: introducing the concept of the local (pixel-wise) texture degree of an image and justifying a selection criterion based on the relative number of pixels with the most frequent local texture degree value. The most significant result of this research is the provision of a mechanism for selecting a container that facilitates the formation of high-visual-quality stego-messages. The importance of the obtained result lies in the fact that the developed selective method ensures an increase in steganographic system efficiency compared to the use of a random container. The maximum recorded increase in efficiency was 31.6%.
Keywords**:** steganographic system, cover image selection, digital image, perceptual imperceptibility.

DOI: https://doi.org/10.52254/1857-0070.2026.2-70.07
UDC: 004.056

Creșterea eficienței sistemului steganografic ca parte componentă a procesului de asigurare a funcționării normale a unui obiect energetic

[1]Bobok I.I., [1]Hryhorenko S.M., [2]Kobozieva A.A., [2]Yavorska K.L.
[1]Universitatea Națională Politehnică din Odesa, Odesa, Ucraina
[2]Universitatea Națională Maritimă din Odesa, Odesa, Ucraina

Abstract. Steganografia ocupă în prezent o poziție vitală în securitatea informațiilor, reflectând importanța sa crescândă în industria energetică. Metodele steganografice sunt utilizate pentru a asigura integritatea datelor și autentificarea în rețelele inteligente; pentru autentificarea termogramelor și a imaginilor de diagnostic obținute în timpul monitorizării liniilor electrice etc. Eficacitatea unui sistem steganografic depinde fundamental de proprietățile recipientului utilizat, ceea ce face ca sarcina de selecție a recipientului să fie extrem de relevantă, una pentru care până în prezent nu a existat o soluție satisfăcătoare. Obiectivul acestei lucrări este de a crește eficiența unui sistem steganografic prin dezvoltarea unei metode de selectare a unui recipient dintr-un set dat de imagini digitale, asigurând o calitate vizuală optimă sau aproape optimă a stego-mesajului, indiferent de formatul recipientului sau de metoda steganografică utilizată. În acest studiu, eficiența steganografică este definită ca o evaluare cantitativă a fiabilității perceptive a stego-mesajului generat, evaluată folosind Măsurarea Indexului de Similaritate Structurală (SSIM). Acest obiectiv a fost atins prin abordarea următoarelor sarcini: introducerea conceptului de grad de textură locală (pe pixeli) al unei imagini și justificarea unui criteriu de selecție bazat pe numărul relativ de pixeli cu cea mai frecventă valoare a gradului de textură locală. Cel mai semnificativ rezultat al acestei cercetări este furnizarea unui mecanism de selectare a unui container care facilitează formarea de stego-mesaje de înaltă calitate vizuală. Importanța rezultatului obținut constă în faptul că metoda selectivă dezvoltată asigură o creștere a eficienței sistemului steganografic în comparație cu utilizarea unui container aleatoriu. Creșterea maximă înregistrată a eficienței a fost de 31.6%.
Keywords: sistem steganografic, selecție a imaginii copertei, imagine digitală, imperceptibilitate perceptivă.

Повышение эффективности стеганосистемы как составной части процесса обеспечения штатного функционирования объекта энергетики

[1]Бобок И.И., [1]Григоренко С.Н., [2]Кобозева А.А., [2]Яворская К.Л.
[1]Национальный университет «Одесская политехника», Одесса, Украина
[2]Одесский национальный морской университет, Одесса, Украина

Аннотация. Развитие информационных технологий привели к внедрению их в процесс функционирования энергетической отрасли, ее широкой цифровизации, следствием чего явились многочисленные киберугрозы, количество и негативные последствия реализации которых возрастают с каждым днем. Важное место в организации защиты информации занимает сегодня стеганография, что нашло свое отражение и в процессе функционирования энергетической отрасли. Стеганометоды используются для обеспечения целостности данных и аутентификации в Smart Grids; для аутентификации термограмм и диагностических снимков, получаемых в ходе мониторинга состояния линий электропередач; для защиты секретной технической документации и т.д. Эффективность стеганосистемы ключевым образом зависит от свойств используемого контейнера, делая задачу его выбора актуальной, однако не имеющей удовлетворительного решения до настоящего момента. *Целью* работы является повышение эффективности стеганосистемы путем разработки метода выбора контейнера из заданного множества цифровых изображений, обеспечивающего наилучшее/близкое к наилучшему визуальному качеству стеганосообщения, независимо от формата контейнера и используемого стеганометода. Под эффективностью стеганосистемы в работе понимается количественная оценка надежности восприятия формируемого стеганосообщения, оцениваемая при помощи Structural Similarity Index Measure. *Поставленная цель была достигнута* путем решения следующих задач: введения понятия степени локальной (пиксельной) текстурности изображения; обоснования выбора критерия селекции контейнеров – относительного количества пикселей изображения с наиболее часто встречающимся значением степени локальной текстурности. *Наиболее важным результатом работы* является обеспечение возможности выбора контейнера, на основе которого формируется стеганосообщение высокого визуального качества. *Значимость полученного результата* заключается в обеспечении за счет использования разработанного селективного метода повышения эффективности стеганосистемы, по сравнению с использованием случайного контейнера. Максимально зафиксированное повышение эффективности составило 31.6%.

Ключевые слова: стеганосистема, выбор контейнера, цифровое изображение, надежность восприятия стеганосообщения.

INTRODUCTION

The energy sector is a critical infrastructure component essential for the functioning of modern society. Any disruptions in its operation, whether intentional or accidental, can lead to severe consequences, potentially reaching catastrophic scales. Rapid advancements in information technology and their integration into energy processes have driven widespread digitalization. However, this shift has also introduced numerous cyber threats, with both the frequency and the impact of these attacks increasing daily [1-4]. A defining characteristic of modern energy complexes is their nature as cyber-physical systems, where digital code directly controls physical assets. Consequently, the deliberate manipulation of transmitted data can force equipment to operate outside of safe parameters, leading to its failure or destruction. In such cases, the impact ranges from substantial economic losses to the physical destruction of critical infrastructure [3].

Under the conditions of modern warfare, any disruption in the operation of the energy system ceases to be a purely technical issue and escalates into a direct threat to national security. Deliberate adversary interference in data exchange can deprive critical infrastructure of power, thereby undermining the state's defense capabilities [5].

Cyberattack-induced disruptions to critical infrastructure—particularly within the energy sector—can trigger a “domino effect”. Due to the pervasive integration of information technology, a control failure at even a single local node, such as a railway signaling system or an electrical substation serving a residential area, can lead to cascading failures across interdependent economic sectors and result in human casualties. In the modern world, the cost of digital vulnerability is increasingly measured not by lost data bytes, but by the physical safety of individuals, particularly in the context of malfunctions or unauthorized interventions at nuclear power plants [6].

Consequently, to ensure the normal operation of the energy sector, it is critically imperative to guarantee the cyber and information security of its constituent components.

Steganography, defined as the science and art of covert communication, currently occupies a

vital position in the field of information security [7]. In the course of modern steganographic transformation, secret information undergoes prelimi0nary encoding. This results in a digital sequence or a digital image (DI) — referred to as Additional Information (AI) — which is then embedded into an inconspicuous object known as the cover. The resulting stego-message is subsequently transmitted over an open communication channel or stored in its processed form. This process is executed by a steganographic system [8], which must satisfy several fundamental requirements: ensuring perceptual imperceptibility of the stego-message (it must remain visually indistinguishable from the original cover); resistance to steganalysis; robustness against attacks targeting the embedded message, etc. Given that attacks on steganographic systems in the modern digital landscape are becoming increasingly sophisticated [9, 10], enhancing system effectiveness across all performance indicators is critically important.

The efficiency of any steganographic system fundamentally depends on the properties of the cover used. This highlights the relevance of the cover selection task, the objectives of which vary: reducing the stego-message's sensitivity to perturbations, improving its visual quality, or increasing the payload capacity of the resulting channel [11, 12]. The methodologies for achieving these goals also differ.

For instance, the method proposed in [13] utilizes the requirement of minimum aggregate perturbation during steganographic transformation as the selection criterion for a DI-cover from a set of candidates. This is ensured by analyzing all possible embedding positions within each candidate image. However, a significant drawback of this approach is its substantial computational complexity, which serves as a major barrier to its practical implementation.

Often, cover selection is tailored to a specific steganographic method [14, 15], which the authors of this study consider a significant limitation. Given the vast diversity and number of existing steganographic methods, a current priority is the development of general principles for cover selection based on a specific objective, ensuring that the selection results remain independent of the specific steganographic algorithm used for AI embedding. Such principles underpin the selective methods proposed in [12, 16]. So, the approach described in [16] is based on a genetic algorithm, where the authors select a DI-cover that provides the best compatibility with a specified secret message. A similar goal is pursued in [12], where the selective method is based on representing the AI as a collection of perturbations within specific (protected) singular triples of the cover matrix that occur during the steganographic transformation.

It should be noted that the outcome of the cover selection process is frequently not the absolute optimal candidate among the contenders relative to the stated objective, but rather one that ensures acceptable or satisfactory performance characteristics for the stego-message [11, 12, 14].

Despite the extensive research in the field of selective steganography, the problem of cover selection remains unresolved to date. It continues to be highly relevant as a significant avenue for enhancing the overall efficiency of steganographic systems.

The growing importance of steganographic information protection has also manifested in the operational processes of the energy sector. The application of steganography within the power industry serves as a practical, modern tool for robust data security.

A specific technology within the energy industry is the Smart Grid [17]. In Smart Grids, which transmit data between meters, substations, and control centers, steganographic methods are employed to ensure data integrity and authentication through fragile digital watermarking (DWM). The core concept generally involves the following: minor perturbations are introduced into telemetry data (such as voltage and current) using specific algorithms to embed a DWM. This process does not interfere with system operations but enables signal authentication. If an adversary attempts to alter the transmitted data, the fragile DWM is destroyed, immediately indicating unauthorized activity within the system.

DWM embedding in this context is performed using various methods. For instance, [18] proposes a steganographic method for securing digital text within Smart Grid communications. The authors' primary objective in embedding the DWM is to ensure the perceptual imperceptibility of the resulting stego-message, which is quantitatively assessed using the Peak Signal-to-Noise Ratio (PSNR), averaging 33.65 dB. Furthermore, the secret message length ranges from 0.2 to 1.24 KB compared to the

prototype. Clearly, this performance metric inevitably depends on the cover text; however, this issue is not explored in that study.

Smart Grids are undergoing continuous evolution. Wi-Fi is widely utilized for data transmission from metering systems, distribution network control and monitoring units, and power grid protection systems. This poses significant security risks for the transmission of confidential data, particularly in the context of cyber warfare, where standard communication channels may be monitored by an adversary. Under such conditions, if a mission-critical command – such as a shutdown or load redistribution – must be sent, it is imperative to do so without the adversary's monitoring system detecting this activity. One approach to addressing this challenge is concealing the transmitted command within a standard data flow (for instance, inside CCTV footage from an electrical substation) or by establishing a dedicated covert channel.

A novel and efficient method for establishing a covert channel is proposed in [19], which utilizes the IEEE 802.11 Enhanced Distributed Channel Access (EDCA) mechanism for data transmission. According to the authors, this represents the first-ever covert channel to utilize three or four independent covert mechanisms to enhance operational efficiency. In their study, the authors emphasize the dependence of the proposed channel's effectiveness on the parameters of the transmitted video sequence (the cover), specifically frame size and frame count. However, they do not reach a definitive conclusion regarding the precise impact of cover properties on the channel's performance.

A multi-layer encryption approach based on chaotic techniques and steganography is proposed in [20] to enhance data protection in Smart Grid communications. The encryption process in the proposed system involves concealing data – encrypted using a digital dictionary and AES algorithm – within an image. The use of a small key and compact dictionary dimensions contributes to the overall efficiency of the encryption mechanism. The study conducted by the authors utilizes several quantitative metrics, including image distortion measures such as PSNR and Mean Squared Error (MSE), to demonstrate that the proposed multi-layer system is a robust and high-speed method for information protection.

Energy facilities (nuclear power plants, hydroelectric plants, substations, etc.) generate vast amounts of visual content, a significant portion of which consists of digital images that can effectively serve as steganographic covers for various tasks. One such task is the authentication of thermograms and diagnostic imagery [21]. Thermal imagers are widely used to monitor the condition of power lines and transformers. An adversary can easily falsify these images – for example, by erasing an overheating zone – to mask an impending accident or sabotage. However, embedding fragile digital watermarking (DWM) into a thermogram ensures that any unauthorized modifications causing DWM destruction will be identified, signaling the unreliability of the data. Furthermore, the thermogram itself can be embedded into a DI or frames of non-specific digital video using steganographic methods. This approach avoids raising suspicion regarding the presence of sensitive information while ensuring the perceptual imperceptibility of the resulting stego-message [22, 23]. The effectiveness of such thermogram protection fundamentally depends on the selection and properties of the cover used. Given that bispectral cameras – which simultaneously capture a conventional photograph and a thermogram – are frequently used in the energy sector, the thermogram (which typically has a lower resolution) is embedded into its corresponding visual counterpart. This simultaneously achieves two goals: concealing vital information from unauthorized observers and ensuring the inseparability of the two informational components, as a thermogram without its visual context loses much of its value.

The monitoring of power lines is frequently conducted using drones, which transmit a vast volume of imagery to the recipient. For each DI captured in this manner, the acquisition metadata – such as the specific drone ID, timestamp, altitude, and other telemetry – is mission-critical. To ensure the inseparability of the DI file from its acquisition data and to minimize the risk of unauthorized modification, this information is embedded into the DI via steganography [24]. Although perceptual imperceptibility in this scenario cannot be enhanced by selecting a different cover (as the image itself represents the primary data), relative improvements in visual quality can still be achieved through the selection of specific sub-regions (blocks) within the existing cover [25].

Since the energy sector is a vital component of a nation's critical infrastructure, technical documentation, power grid blueprints, power

plant protection schemes, and various other documents are classified as sensitive assets requiring stringent access control. At the generation stage, it is expedient to embed a DWM containing essential service information. This measure enables the tracing of the source should any visual data leakage occur. Although the energy sector is not unique in this particular application of steganographic techniques, steganography nonetheless remains an effective tool for safeguarding the information used within the industry.

Consequently, for the energy sector – as for any other component of critical infrastructure – the challenge of enhancing the effectiveness of steganographic data protection remains both vital and highly relevant.

Given that the primary objective of steganography is to conceal the existence of additional information within the utilized information content [7, 8], the fundamental requirement for the steganographic system in this study is ensuring the perceptual imperceptibility of the resulting stego-message.

The aim of this work is to enhance steganographic system effectiveness by developing a method for selecting a cover from a given set of digital images that ensures optimal or near-optimal visual quality of the corresponding stego-message, regardless of the image format or the steganographic method employed.

In this research, the effectiveness of the steganographic system is defined as the quantitative assessment of the perceptual imperceptibility of the generated stego-message, evaluated using the Structural Similarity Index Measure (SSIM) [26].

DEFINING THE COVER SELECTION CRITERION

The goal of cover selection in this work is to ensure relatively high visual quality for the corresponding stego-message. For this purpose, DIs possessing a high texture degree [15, 27] are the most suitable; that is, images that collectively contain relatively large sub-regions with significant variations in pixel brightness values. Consequently, to achieve the research objective, it is necessary to define a numerical parameter for the DI that can most effectively estimate its texture degree. This parameter must enable the identification of an image where the number of significant pixel brightness variations is maximal (or near-maximal), taking into account the subsequent use of this DI for steganographic transformation.

The most effective, and consequently the most widely used classical approach to determining the texture degree of a D) is the gradient-based method [29, 30]. This is logical, as the gradient for a specific pixel in a DI captures the rate of change of its brightness across various directions. The larger the absolute value of the gradient element, the more significant the corresponding brightness jump. Such pixels are preferable for the steganographic transformation process because, in the presence of high brightness variation, minor changes are highly unlikely to be perceived visually. In general, it can be asserted that the larger the jump in brightness values, the lower the probability of visually detecting any modification to these values [31]. However, despite its widespread application, this approach does not guarantee that all existing “jumps” are accounted for. This represents a significant drawback when selecting a DI as a cover: “missing” these jumps can lead to sub-optimal cover selection and, consequently, a reduction in the payload capacity of the covert communication channel, which is undesirable. In light of this, let us examine the foundations of the gradient-based approach in greater detail.

Let $f(x,y)$ be a function whose domain discretization and value quantization have resulted in a digital image represented by a matrix F with elements f_{ij}. For $f(x,y)$, the gradient at point (x,y) is defined as $grad\ f(x,y)=\left(\frac{\partial f}{\partial x}(x,y),\frac{\partial f}{\partial y}(x,y)\right)$. In digital image processing, the term “gradient” is frequently used to refer to the Euclidean norm of the vector:

$$\left\|grad\ f(x,y)\right\|=\left(\left(\frac{\partial f}{\partial x}(x,y)\right)^2+\left(\frac{\partial f}{\partial y}(x,y)\right)^2\right)^{1/2},$$

however, given the large dimensions of modern images, the following is used as a gradient estimate [31]:

$$\nabla f=\left|\frac{\partial f}{\partial x}(x,y)\right|+\left|\frac{\partial f}{\partial y}(x,y)\right|. \qquad (1)$$

In digital image processing, the gradient for a specific pixel f_{ij} can be calculated in various

ways. Let us consider the neighborhood of this pixel with a radius of 1:

$$\begin{pmatrix} f_{i-1,j-1} & f_{i-1,j} & f_{i-1,j+1} \\ f_{i,j-1} & f_{ij} & f_{i,j+1} \\ f_{i+1,j-1} & f_{i+1,j} & f_{i+1,j+1} \end{pmatrix}. \quad (2)$$

Using the first-order divided difference [32] to estimate the derivative of a discrete function at a point, we obtain:

$$\frac{\partial f}{\partial x}(x,y) = f_{i+1,j} - f_{ij},\ \frac{\partial f}{\partial y}(x,y) = f_{i,j+1} - f_{ij}. \quad (3)$$

An alternative estimation variant is also proposed in [31]:

$$\begin{aligned} \frac{\partial f}{\partial x}(x,y) &= f_{i+1,j+1} - f_{ij}, \\ \frac{\partial f}{\partial y}(x,y) &= f_{i+1,j} - f_{i,j+1} \end{aligned} \quad (4)$$

Using (3) and (4) to estimate the gradient (1) results in the upper and left neighborhoods of pixel f_{ij} being entirely disregarded, even though the brightness transition for f_{ij} may occur precisely in those areas. Thus, for the objectives of this study, formulas (3) and (4) clearly fail to provide a comprehensive assessment of the behavior of neighboring pixels for f_{ij}. Consequently, their application would hinder the high efficiency of the corresponding cover selection method, regardless of the steganographic algorithm employed.

The Prewitt and Sobel operators are the most preferred and frequently used in practice for gradient estimation in digital image processing [31].

To obtain the components of the gradient vector, the classical Sobel operator employs 3×3 masks:

$$\begin{pmatrix} -1 & -2 & -1 \\ 0 & 0 & 0 \\ 1 & 2 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 & 1 \\ -2 & 0 & 2 \\ -1 & 0 & 1 \end{pmatrix},$$

while the Prewitt operator (to obtain approximations of the derivative along the OX and OY directions) uses the following:

$$\begin{pmatrix} -1 & -1 & -1 \\ 0 & 0 & 0 \\ 1 & 1 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 & 1 \\ -1 & 0 & 1 \\ -1 & 0 & 1 \end{pmatrix}.$$

It is evident that, considering the research objective, the Sobel operator is preferred over the Prewitt operator for the following reason. In the Sobel masks, those neighboring pixels of f_{ij} that lie directly on the OX and OY axes – the directions along which the partial derivatives are calculated – are explicitly emphasized (weighted). This leads to a more accurate approximation of these derivatives compared to the Prewitt operator and, consequently, a more precise estimation for (1).

Using the Sobel masks, we obtain:

$$\begin{aligned} \frac{\partial f}{\partial x}(f_{ij}) = G_X \approx &-(f_{i-1,j-1} + 2f_{i-1,j} + f_{i-1,j+1}) + \\ &+(f_{i+1,j-1} + 2f_{i+1,j} + f_{i+1,j+1}), \\ \frac{\partial f}{\partial y}(f_{ij}) = G_Y \approx &-(f_{i-1,j-1} + 2f_{i,j-1} + f_{i+1,j-1}) + \\ &+(f_{i-1,j+1} + 2f_{i,j+1} + f_{i+1,j+1}) \end{aligned} \quad (5)$$

For the Sobel operator, the mask size can exceed 3×3; however, increasing the dimensions leads to a decrease in the operator's sensitivity: fine lines and small details may be lost, which is critical for the task of steganographic cover selection. Furthermore, increasing the mask size results in higher computational complexity for the gradient calculation process. Considering that this process is intended to establish the texture degree of a DI to determine its suitability as a cover – and given that there may be numerous candidates for the cover role – any increase in the computational complexity of analyzing a single DI is highly undesirable.

Thus, for establishing the texture degree of a DI using a gradient-based approach at the current stage of research, the Sobel filter with 3×3 masks holds the highest priority. However, for the objectives of this study – where the texture degree is determined for the subsequent selection of a steganographic cover – the Sobel operator exhibits significant drawbacks. Suppose that the neighborhood (2) takes the following form:

$$\begin{pmatrix} a & b & a \\ b & f_{ij} & b \\ a & b & a \end{pmatrix}. \quad (6)$$

Then,

$$G_X = 0, G_Y = 0, grad(f_{ij}) = 0, \nabla f = 0,$$

which in the general case may falsely indicate the absence of brightness transitions in the neighborhood of pixel f_{ij}, even when they are present. Indeed, several situations are possible here:

- $b >> a$; here, f_{ij} may be comparable to b (resulting in a cross-like structure), f_{ij} may be comparable to a (resulting in a "checker-board" structure), or f_{ij} may differ significantly from both a and b;
- $b << a$; for f_{ij}, variations analogous to the previous point are possible;
- a and b differ insignificantly from each other (or have identical values) but differ significantly from f_{ij}.

In each of these situations, one or more sharp jumps in brightness values occur within the neighborhood of f_{ij}. While these variations are essential for determining the overall texture degree of the DI, the Sobel operator fails to detect them.

Remark 1. When the Sobel operator (5) is applied, condition $\|grad\ f(x,y)\| = 0$ or $\nabla f = 0$ constitutes a necessary but not sufficient condition for the local homogeneity of the DI (within the neighborhood of f_{ij}). In other words, it cannot guarantee the absence of brightness transitions in the vicinity of the pixel f_{ij}.

Remark 2. Although the gradient defined for a DI pixel naturally characterizes the behavior of its neighbors by accounting for the rate of brightness change when transitioning from the given pixel to its neighbors, this representation in the form of ∇f is cumulative. For the purpose of identifying a DI that is best suited for embedding a secret message – in terms of maintaining the visual perception of the stego-object – it is crucial to have the ability to evaluate the behavior of each individual neighbor of pixel f_{ij}.

To provide a visual clarification of Remark 2, let us illustrate it with an example involving two 3×3 DI blocks:

$$\begin{pmatrix} 25 & 25 & 25 \\ 25 & 30 & 25 \\ 25 & 25 & 30 \end{pmatrix}, \begin{pmatrix} 24 & 24 & 25 \\ 24 & 25 & 25 \\ 25 & 26 & 26 \end{pmatrix}. \qquad (7)$$

The gradient (1) for each of these, calculated for the central pixel using (5), will be equal to 10. The simultaneous consideration of the aggregate differences between pixels in the given neighborhood leads to an illusory equivalence of the blocks in terms of their texture degree as determined by the gradient. However, it is evident that the first block is clearly preferable for DI embedding, as it possesses a more significant brightness transition.

In view of the foregoing, to assess the texture degree of a DI – characterizing its suitability or unsuitability to serve as a cover – it is necessary to define a quantitative parameter for each pixel that focuses on the presence of brightness jumps and is free from the drawbacks identified above. The sought-after parameter must:

- utilize information from the entire neighborhood of f_{ij} (in contrast to formulas (3) and (4));
- characterize the behavior of the immediate neighbors of pixel f_{ij};
- be capable of detecting existing brightness jumps in situations where the gradient fails to reveal them—specifically in scenarios such as (6) and (7).

The following parameter satisfies all the established requirements and is hereafter referred to as the Local (Pixel-wise) Texture Degree Index (LTDI). It is proposed as an alternative to the gradient for detecting brightness jumps within the neighborhood f_{ij}:

$$G(f_{ij}) = \max_{k,l \in \{-1,0,1\}} |f_{ij} - f_{i+k,j+l}|. \qquad (8)$$

Thus, the LTDI is defined as the maximum of the absolute brightness jumps between pixel f_{ij} and any neighboring pixel within neighborhood (2). The satisfaction of the first two requirements is evident. Let us now examine the behavior of $G(f_{ij})$ under the conditions specified in (6):

$$G(f_{ij}) = \max\{|f_{ij} - a|, |f_{ij} - b|\}. \qquad (9)$$

In this case, $G(f_{ij}) = 0$ if and only if $f_{ij} = a = b$; that is, when the block under consideration is indeed homogeneous.

For blocks of type (7), where one is homogeneous and the other contains more significant brightness transitions, it is evident that parameter (9) will clearly distinguish between them. It assigns a higher value $G(f_{ij})$ to the block that has priority for steganographic

transformation: specifically, $G(f_{ij})=5$ for the first block and $G(f_{ij})=1$ for the second block.

It is evident that the higher the texture degree of a DI, the greater the number of pixels with relatively high LTDI (8) values, and consequently, the higher its priority among candidate cover images. Based on the foregoing, a hypothesis is proposed regarding the truth of the inverse statement: the greater the number of pixels in a DI that possess relatively high LTDI values, the higher the visual quality of the corresponding stego-message will be.

The most suitable mathematical tool for testing the proposed hypothesis is the histogram of $G(f_{ij})$ values for the DI pixels, hereinafter denoted as $\Gamma(G)$. The properties of $\Gamma(G)$ will differ between relatively homogeneous Dis – those containing large regions with minor brightness transitions (e.g., Fig. 1(a)), hereafter referred to as Type I images – and DIs containing a vast number of diverse (fine) details, objects, and contours (e.g., Fig. 1 (b, c)), hereafter referred to as Type II images. For Type I DIs, the mode of $\Gamma(G)$ will consistently be located in the immediate vicinity of zero, and the value at this mode is expected to be relatively high, as illustrated in Fig. 1(d). Indeed, for a homogeneous DI, the brightness transitions for the majority of pixels will be insignificant and comparable to one another; among other characteristics, this is reflected in the unimodality of the histogram.

At first glance, one might expect the mode of $\Gamma(G)$ for Type II images to be significantly shifted to the right relative to zero. However, this is not always the case (cf. Fig. 1(e) and 1(f)), which is attributed to the fact that even highly textured original DIs contain homogeneous regions. For this group of images, the value at the mode of $\Gamma(G)$ cannot be as dominant relative to other histogram values as it is for Type I images. This is due to the presence of numerous contours and brightness transitions that generally vary in magnitude. Furthermore, the existence of areas with small brightness variations in original Type II images often results in the multimodality (polymodality) of $\Gamma(G)$ (Fig. 1(f)). Specifically, multimodality in histogram $\Gamma(G)$ is frequently observed in thermograms. This occurs because thermograms often contain regions of relatively uniform temperature (infrared radiation intensity), which function as homogeneous areas within the image (Fig. 2).

To empirically validate the identified properties of the histograms $\Gamma(G)$, a computational experiment was conducted using the following image sets:

- set $M_{Tif,1}$: 100 lossless digital images (TIF) from the 4cam_auth database [33];
- set $M_{Tif,2}$: 400 lossless digital images (TIF) from the img_Nikon_D70s database [34];
- set $M_{Jpeg,1}$: 100 lossy images (JPEG, QF=75) obtained by resaving the images from $M_{Tif,1}$;
- set $M_{Jpeg,1}$: 400 lossy images (JPEG, QF=75) obtained by resaving the images from $M_{Tif,2}$;
- set M_{Jpeg}: 300 JPEG images from the NRCS database [35].

At this stage of the computational experiment, an LTDI (8) value histogram was constructed for each DI. The following findings were established:

- For Type I images, the mode of $\Gamma(G)$ falls within the range 0…2, and the histogram is invariably unimodal.
- For Type II images, the mode of $\Gamma(G)$ falls within the range 0…23, most frequently taking values between 1…3. In this case, the histogram is often multimodal.
- For images of the same dimensions, the value of $\Gamma(G)$ at its mode for Type II is more than twice as small as that for Type I. Consequently, Type II images contain a larger number of pixels with relatively high LTDI values.
- The aforementioned properties are independent of the DI format (lossless or lossy).
- When comparing corresponding DIs (image pairs from sets $M_{Tif,1}$ and $M_{Jpeg,1}$, $M_{Tif,2}$ and $M_{Jpeg,2}$), it was established that the mode of $\Gamma(G)$ for the lossless format (TIF) is consistently greater than or equal to the mode of $\Gamma(G)$ for the corresponding lossy format (JPEG). This phenomenon serves as a natural quantitative indicator that resaving a DI from a lossless format to a lossy one reduces the relative contribution of the high-frequency component. This leads to a (slight) smoothing of contours, which frequently results in a de-

crease in $G(f_{ij})$ for the pixels that define those contours.

Thus, the results of the computational experiment have fully confirmed the properties of $\Gamma(G)$ that were established theoretically.

One of the requirements for the developed selective method, given that the number of candidate cover images can be substantial, is the low computational complexity involved in analyzing a single DI. In view of this requirement, we shall simplify the LTDI calculation process (8) by considering only the four nearest neighbors of a pixel:

$$\overline{G}(f_{ij}) = \max\begin{pmatrix} |f_{ij} - f_{i,j-1}|, |f_{ij} - f_{i,j+1}|, \\ |f_{ij} - f_{i-1,j}|, |f_{ij} - f_{i+1,j}| \end{pmatrix}. \quad (10)$$

Naturally, by using the value (10) as the LTDI, some information regarding the behavior of the neighbors of pixel f_{ij} will be lost. However, as demonstrated by the computational experiment conducted using the previously defined DI sets, the properties of the histograms for $\overline{G}(f_{ij})$ values (hereinafter $\Gamma(\overline{G})$) and $G(f_{ij})$ for the original DIs are virtually indistinguishable (cf. Fig. 3 and Fig. 1(f)). Furthermore, the number of operations required to determine $\overline{G}(f_{ij})$ is half that required for $G(f_{ij})$. This leads to a significant reduction in the time required for histogram construction and, consequently, for the analysis of an individual DI.

Let us define a histogram characteristic that can serve as an indicator of the DI texture degree, thereby ensuring the visual quality of the stego-message and acting as a robust criterion for container selection.

Taking into account the previously established properties of histograms for Type I and Type II DIs, and to eliminate any potential dependence of the sought-after characteristic on image dimensions, it is proposed to use the relative frequency of pixels whose LTDI matches the mode of the histogram as a quantitative assessment $P(F)$ of the texture degree for an image with an $n \times m$-matrix F:

$$P(F) = \frac{T_{\mathrm{m}}(F)}{mn} \cdot 100\%, \quad (11)$$

where $T_{\mathrm{m}}(F)$ is the histogram value at the mode.

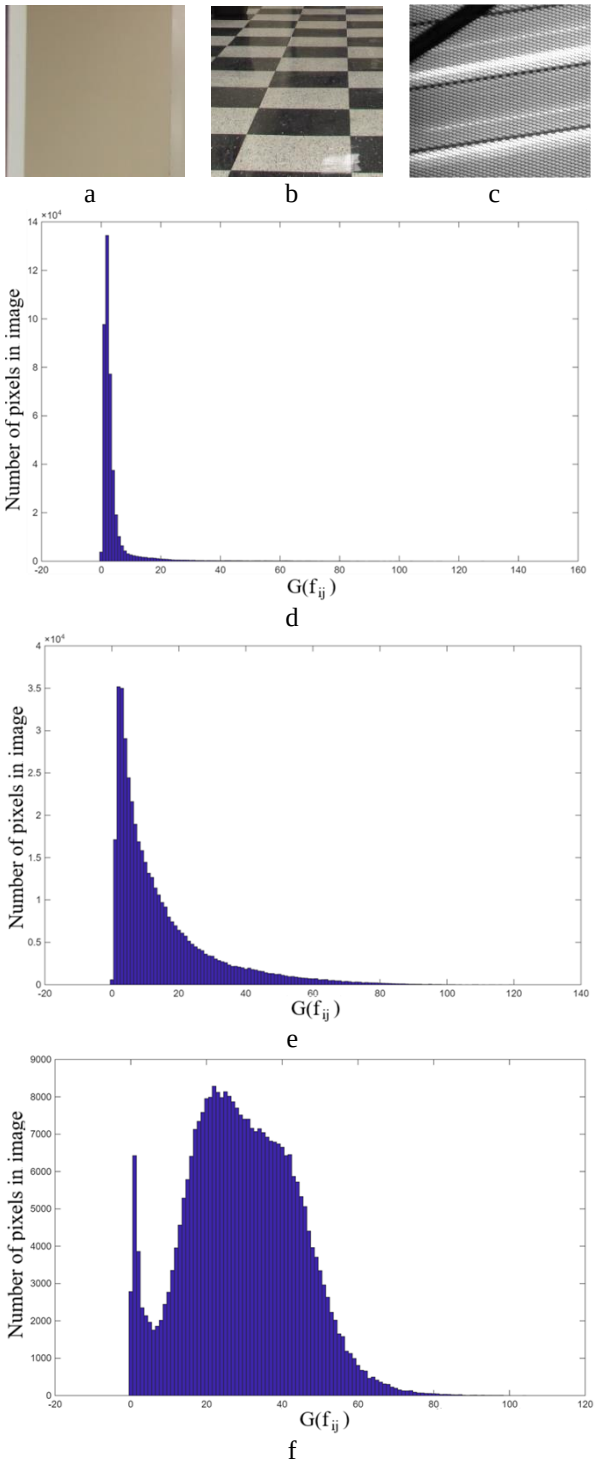
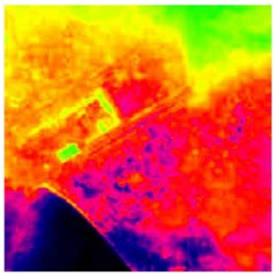
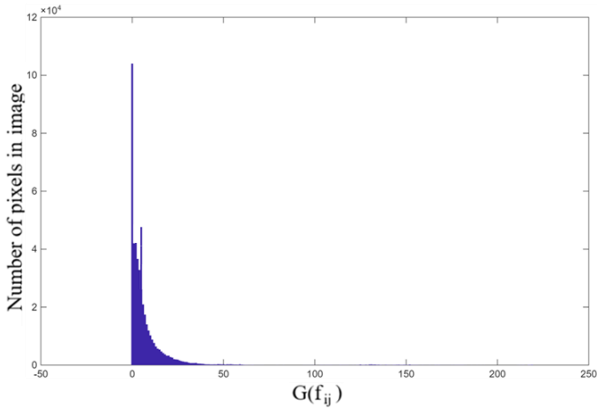


Fig. 1. Examples of $\Gamma(G)$ for DIs: a, b – from set $M_{Tif,1}$; c – from set $M_{Jpeg,2}$; d, e, f –corresponding histograms.



a



b

Fig. 2. An example of the emergence of a polymodal histogram: a – thermogram [36]; b – $\Gamma(G)$.

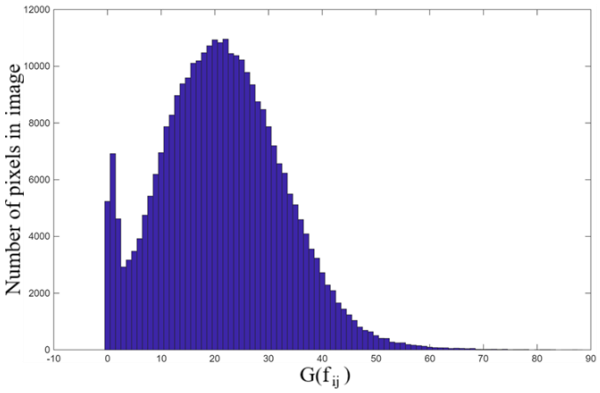


Fig. 3. Histogram $\overline{G}(f_{ij})$ for the DI shown in Fig. 1(c).

The proposed container selection criterion (11) is independent of the DI format (lossless or lossy) and is entirely uncoupled from the steganographic method employed thereafter; it is determined solely by the inherent structure of the DI. Specifically, a lower value of $P(F)$ indicates that a greater number of pixels possess relatively high LTDI values. Consequently, such a DI is assigned a higher priority for use as a steganographic cover object.

METHOD FOR COVER IMAGE SELECTION

Let $M=\{F_1,F_2,...,F_k\}$ be the set of candidate cover images. Based on the previously discussed properties of $\Gamma(G)/\Gamma(\overline{G})$, the fundamental steps of the container selection method are as follows:

Step 1. Select the method for calculating the LTDI.

Step 2. For $\forall F_r \in M$:

2.1. For each pixel f_{ij} of the DI F_r, determine its texture degree index: $\overline{G}(f_{ij})/G(f_{ij})$;

2.2. Construct the histogram $\Gamma(G)/\Gamma(\overline{G})$ of the $G(f_{ij})/\overline{G}(f_{ij})$ values;

2.3. Determine the mode $m_r(\Gamma)$ of the constructed histogram $\Gamma(G)/\Gamma(\overline{G})$;

2.4. Determine the value $T_{\mathrm{m}}(F_r)$ at the mode $m_r(\Gamma)$;

2.5. Determine the value $P(F_r)$ (11).

Step 3. Определить такое ЦИ $F_l \in M$, для которого Identify such DI $F_l \in M$ for which

$$P(F_l)=\min_{F_r \in M} P(F_r). \qquad (12)$$

If F_l is the only digital image in set *M*,

then F_l is the sought-after cover object.

If $F_{l_1},F_{l_2},...,F_{l_t} \in M$ satisfy condition (12),

then among $F_{l_1},F_{l_2},...,F_{l_t}$, identify the digital image $F_{l_h} \in M$ for which

$$m_{l_h}(\Gamma)=\max_{1\le i\le t} m_{l_i}(\Gamma). \qquad (13)$$

If $F_{l_h} \in M$ is the only digital image from $F_{l_1},F_{l_2},...,F_{l_t}$,

then F_{l_h} is the sought-after cover object.

If among $F_{l_1},F_{l_2},...,F_{l_t}$, several images $F_{l_{k_1}},F_{l_{k_2}},...,F_{l_{k_j}}$ satisfy condition (13),

then from $F_{l_{k_1}},F_{l_{k_2}},...,F_{l_{k_j}}$ select the digital image $F_{l_{k_h}}$ whose histogram exhibits a polymodal structure.

If $F_{l_{k_h}}$ is uniquely determined,

then $F_{l_{k_h}}$ is the sought-after cover object.

If $F_{l_{k_h}}$ cannot be uniquely determined or is not defined,
then any digital image from the set $F_{l_{k_1}}, F_{l_{k_2}}, ..., F_{l_{k_j}}$ may be chosen as the sought-after cover object.

The specific form of the computational formula for the LTDI in Step 1 depends on the operational conditions of the covert communication channel. When the time available for transmitting secret information is critically limited, it is natural to use relation (10) for LTDI calculation during container selection. Conversely, if time constraints are not critical and there is a high probability of passive attacks by an adversary, priority should be given to formula (8) for the LTDI.

PERFORMANCE EVALUATION OF THE METHOD

To evaluate the effectiveness of the proposed container selection method, a computational experiment was conducted. Despite the previously established minor differences between the properties of $\Gamma(G)$, $\Gamma(\overline{G})$ histograms, both algorithmic implementations – corresponding to LTDI calculation formulas (8) and (10) – were analyzed to account for different operational scenarios.

The experiment utilized the image sets defined in the previous sections, supplemented by four additional sets to ensure statistical robustness:

- Sets $M_{mix,1}$, $M_{mix,2}$: Derived from a general pool
  $M_{Tif,1} \bigcup M_{Tif,2} \bigcup M_{Jpeg,1} \bigcup M_{Jpeg,2} \bigcup M_{Jpeg}$.
  From this pool, 200 images of various formats and resolutions were randomly selected and divided into two equal groups of 100 images each.
- Sets $M_{AI,1}$ and $M_{AI,2}$: Given the current prevalence of AI-generated content, these sets consist of 100 images each, sourced from the [37] database. Testing on synthetic images is crucial, as they are highly likely to be used as cover objects in modern covert communication channels.

As previously noted, a quantitative assessment of the perceptual fidelity of the generated stego-object is conducted using the Structural Similarity Index Measure (SSIM) [26].

To evaluate the performance of the proposed selection method, the following steganographic algorithms were employed to generate the stego-objects:

- LSB-Matching [38]: One of the most widely used spatial-domain methods. The implementation utilized a payload capacity of 1 bpp. Unlike standard LSB replacement, LSB-matching provides better security by randomly incrementing or decrementing pixel values to match the secret bit's parity.
- Koch and Zhao Method [8]: A frequency-domain technique. Embedding was performed in the Discrete Cosine Transform (DCT) domain by partitioning the container into standard 8×8 blocks [31]. The secret bits were embedded by modifying the DCT coefficients at coordinates (4,5) and (5,4). The quantization parameter for the embedding process was set to 25.
- Maximum Singular Value Modification [39]: A matrix-decomposition method based on Singular Value Decomposition (SVD). This approach is recognized for its high robustness against compression attacks. Embedding was carried out in the SVD domain of each 8×8 block obtained through standard partitioning. The key embedding parameter was set to 200.

For all experiments, the embedded data consisted of a randomly generated binary sequence. The results of the computational experiment are summarized in Table 1 and illustrated in Figure 4.

The results of the computational experiment fully confirm the hypothesis proposed above: the smaller the relative number of pixels for which the LTDI coincides with the most frequent value across the entire image, the greater the number of pixels with relatively high LTDI values, and, consequently, the higher the visual quality of the corresponding stego-object.

Based on the obtained results, the high efficiency of the proposed method can be confirmed. For all sets of candidates composed of original digital images captured by physical cameras, the selected containers consistently provided the maximum possible SSIM visual quality index across the entire set. The only exception occurred in one set containing AI-generated digital images (Fig. 4). These deviations in AI-generated images can be attributed to the inherent differences in their properties – including statistical characteristics – compared to those obtained via physical sensors [40]. However, even in this case, the discrepancy

between the SSIM value of the selected container and the absolute maximum was negligible: 0.09% for the LSB-matching method; 1.27% for the Koch and Zhao method; and 0.11% for the SVD-based method [39]. These results are illustrated in Fig. 4.

The experiment utilized pairs of corresponding digital image sets: $M_{Tif,1}$ and $M_{Jpeg,1}$, $M_{Tif,2}$ and $M_{Jpeg,2}$. It is important to note that within each pair, the optimal container was uniquely identified – specifically, the image that consistently yielded stego-objects of the highest quality (in terms of SSIM), regardless of its format (lossy or lossless). This confirms that the effectiveness of the developed selection method is independent of the candidate images' file formats.

The implementation of the proposed container selection method significantly enhanced the effectiveness of the steganographic system compared to random container selection within the analyzed datasets. To quantify the impact, we evaluated the maximum potential gain in efficiency – defined as the difference in visual quality between the optimally selected container and the container that would have resulted in a stego-object with the minimum SSIM value. These results are summarized in Table 2.

Thus, the container selection method proposed in this work enabled a maximum increase in steganographic system efficiency – in terms of visual perception – by 31.6%.

To ensure a comprehensive evaluation of the effectiveness of the developed selective method, a comparative analysis with analogs was conducted. It should be noted that, in the general case, comparing selective methods based on specific quantitative characteristics of the stego-message obtained from a chosen container is incorrect, as these characteristics depend on the particular set of candidates. The most appropriate criterion for comparing the proposed methods is the indicator of the difference between the target characteristics of the stego-message obtained using the selected container and the characteristics of the best possible stego-message (in terms of target characteristics) within that set of candidates, as done, for example, in [12]. Ideally, of course, the container selection should ensure the highest quality (given the selection goal) of the corresponding stego-message across the entire set of candidates – an absolute result. However, not all selective methods are capable of providing such a choice. For instance, method [14], which does not yield an absolute result, ensures the selection of containers for which stego-messages formed by the LSB method have a high average SSIM value of 0.9935. For comparison: the average SSIM value for stego-messages obtained by the LSB method using containers selected by the method proposed in this work was 0.9972, i.e., 0.4% higher.

For a correct comparative analysis of the efficiency of the proposed method, one of the most effective analogs to date – method [13] – was chosen for the following reasons: both methods target the improvement of the stego-object's visual quality as their selection goal; both methods yield an absolute selection result for all considered candidate sets obtained by physical cameras, regardless of the steganographic method used. However, the method proposed in this work has distinct advantages over [13].

Table 1

Performance Results of the Algorithmic Implementations of the Proposed Method

DI sets	Minimum $P(F)$ value across the set		SSIM value of the selected cover / Maximum SSIM value across the set		
	$\Gamma(G)/\Gamma(\overline{G})$	achieved on the same DI (+) or on a different DI (−)	LSB-Matching (1 bpp)	Koch and Zhao Method	Method [39]
$M_{Tif,1}$	5.8708 / 8.1828	+	0.9945 / 0.9945	0.9945 / 0.9945	0.9894 / 0.9894
$M_{Tif,2}$	3.4407 / 4.7028	+	0.9983 / 0.9983	0.9814 / 0.9814	0.9800 / 0.9800
$M_{Jpeg,1}$	4.8235 / 6.3287	+	0.9946 / 0.9946	0.9355 / 0.9355	0.9265 / 0.9265
$M_{Jpeg,2}$	3.0112 / 3.4939	+	0.9984 / 0.9984	0.9829 / 0.9829	0.9733 / 0.9733

M_{Jpeg}	2.3220 / 3.0990	+	0.9982 / 0.9982	0.9782 / 0.9782	0.9711 / 0.9711
$M_{mix,1}$	2.5728 / 3.6245	+	0.9981 / 0.9981	0.9780 / 0.9780	0.9713 / 0.9713
$M_{mix,2}$	2.7544 / 3.3807	+	0.9981 / 0.9981	0.9757 / 0.9757	0.9665 / 0.9665
$M_{AI,1}$	11.8379 / 13.7528	+	0.9907 / 0.9916	0.8972 / 0.9087	0.8813 / 0.8823
$M_{AI,2}$	11.2630 / 12.8764	+	0.9923 / 0.9923	0.9153 / 0.9153	0.9025 / 0.9025

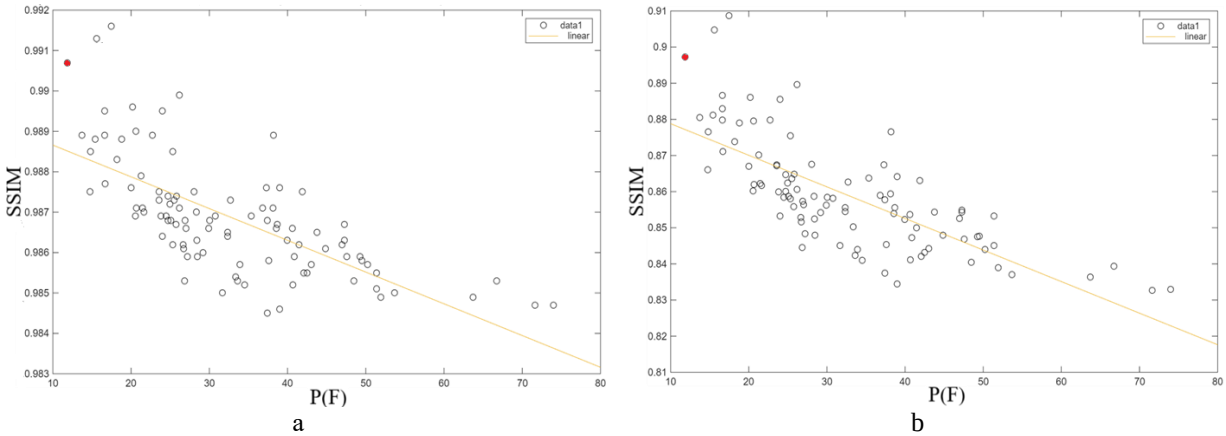


Fig. 4. Dependency of the SSIM index $P(F)$ determined based on $\Gamma(G)$ for set $M_{AI,1}$ for stego-objects generated by: a – LSB-matching with a capacity of 1 bpp; b – Koch and Zhao method.

Table 2

Maximum potential increase in steganographic system efficiency (measured by the SSIM index) when using the proposed container selection method compared to random container selection (%)

DI set	LSB-matching 1 bpp	Koch and Zhao method	Method [39]
$M_{Tif,1}$	1.1	18.0	18.2
$M_{Tif,2}$	2.9	30.7	28.1
$M_{Jpeg,1}$	1.1	13.7	16.5
$M_{Jpeg,2}$	3.0	31.6	29.0
M_{Jpeg}	1.1	12.1	13.4
$M_{mix,1}$	1.6	18.2	19.7
$M_{mix,2}$	1.5	17.4	17.4
$M_{AI,1}$	0.6	7.7	5.9
$M_{AI,2}$	0.8	9.8	10.2

First, the analysis of a single $n\times n$-DI by the proposed method always requires $O(n^2)$ operations for both algorithms (determined by the number of pixels in the DI), whereas the computational complexity of analyzing one DI in [13] can reach $(n^2)!$; for example, if a binary sequence containing n^2 bits is embedded into an $n\times n$-image using the LSB method, where all possible embedding variants into n^2 pixels are exhausted during the selection process.

Second, our proposed method is universal in the sense that the selection result is independent not only of the specific steganographic algorithm but also of the additional information intended to be embedded in the selected container. The container selection within the existing set of candidates is performed once, and the resulting container is then used by any steganographic

method with various additional information, unlike [13], where the selection must be made every time for a specific piece of data.

Admittedly, container selection is not always utilized in the organization of covert communication channels today, as it requires additional computational overhead that is sometimes deemed unacceptable. However, it is precisely container selection that allows for the "smoothing out" of shortcomings in existing methods with limited scopes of application. A prime example is method [39], which may produce visible artifacts when a stego-object is generated based on a randomly selected container. Nonetheless, this method possesses significant advantages: it is highly robust against attacks on the embedded message, even those of considerable strength (e.g., JPEG compression attacks with a quality factor QF < 30). Any modifications aimed at improving the visual quality of such a stego-object (to expand its applicability) – which in practice means seeking a compromise between robustness and visual fidelity – would inevitably alter the method's core mathematical basis, most likely decreasing its resistance to attacks. For such methods, container selection is the only way to ensure their effective practical implementation. In all other cases, container selection consistently ensures that the quality of the steganographic system is never degraded and, in practice, is enhanced in one sense or another.

CONCLUSION

This paper presents a container selection method from a set of candidate digital images designed to ensure the best or near-optimal visual quality of the resulting stego-object, quantitatively measured by the SSIM index.

During the development of the method, the following milestones were achieved:

- The concept of the Local Texture Degree Index (LTDI) of a digital image was defined, and calculation formulas for its estimation were proposed.
- A selection criterion was established based on the properties of LTDI value histograms, specifically the relative number of pixels having an LTDI equal to the mode $\Gamma(G)/\Gamma(\overline{G})$.
- The experimental evaluation led to the following conclusions:
  - Reliability and Universality: The container selected by the proposed method from sets of images captured by physical cameras consistently yielded the highest visual quality across all tested steganographic algorithms.
  - Performance on AI Content: For AI-generated image sets, the selected container provided stego-objects with an SSIM deviation of only 1.27% from the theoretical maximum in the worst-case scenario.
  - Format Independence: The selection process proved to be invariant to the file format (lossy or lossless) of the candidate images.
  - Efficiency Gains: The implementation of the proposed method increased the efficiency of the steganographic system—in terms of perceptual reliability—by a maximum of 31.6% and a minimum of 0.6% compared to random container selection.

Further investigation is evidently required for AI-generated image sets, which currently constitutes the primary focus of the authors' ongoing research.

References

[1] Mukherjee S. Implementing cybersecurity in the energy sector. Available at: https://doi.org/10.6084/m9.figshare.9728051 (accessed 15.05.2024)

[2] Hariri F., Moroz O. Possibilities of geoinformation systems for implementation of the smart grid concept in electrical distribution networks. *Proceedings of the 2023 International Scientific and Practical Conference on Electrical Energy, Electromechanics and Technologies in Agricultural Industrial Complex*. Kharkiv, 2023. P. 101–102.

[3] Tomasek R., Qu Y. Cybersecurity Regulations in the Energy Industry: A Detriment or a Benefit? *European Journal of Electrical Engineering and Computer Science*, 2025, vol. 9, no. 3, pp. 9–15.

[4] Rashid M. et al. A comprehensive review of cybersecurity challenges and resilience strategies in renewable energy integration with battery storage for sustainable smart grids. *Results in Engineering*, 2026, vol. 29, 108557.

[5] Smith B. *Defending Ukraine: early lessons from the cyber war*. Available at: https://blogs.microsoft.com/on-the-issues/2022/06/22/defending-ukraine-early-lessons-from-the-cyber-war/ (accessed 26.12.2024).

[6] Bobok I., Kobozeva A., Maksymov M., Maksymova O. Checking the Integrity of

CCTV Footage in Real Time at Nuclear Facilities. *Nuclear & Radiation Safety*, 2016, no. 2, pp. 68–72.

[7] Hammad O.M., Smaoui I., Fakhfakh A., Hashim M.M. An Overview of Image Steganography Techniques: Historical Development, Methodologies, and Evaluation Criteria. *SHIFRA*, 2024, pp. 74–87.

[8] Konakhovich G., Progonov D., Puzyrenko O. *Steganographic Processing and Analysis of Multimedia Data*. Center for Educational Literature, 2018.

[9] Kobozeva A.A., Bobok I.I., Garbuz A.I. General principles of integrity checking of digital images and application for steganalysis. *Transport and Telecommunication Journal*, 2016, vol. 17, no. 2, pp. 128–137.

[10] Karampidis K., Kavallieratou E., Papadourakis G. A review of image steganalysis techniques for digital forensics. *Journal of Information Security and Applications*, 2018, vol. 40, pp. 217–235.

[11] Azam M.H.N. et al. A systematic review on cover selection methods for steganography: Trend analysis, novel classification and analysis of the elements. *Computer Science Review*, 2025, vol. 56, 100726.

[12] Bobok I., Kobozieva A., Sokalskiy S. Udoskonalennya metodu vyboru steganografichnogo konteineru dlya pidvyschennya stiikostisteganosystemy do atak proty vbudovanogo povidomlennya [Improving the steganographic container selection method for enhancing system robustness against embedded message attacks]. *Radioelectronics and Communications Systems*. 2025. https://doi.org/10.20535/S0021347025030045 (in Ukrainian).

[13] Hajduk V., Levicky D. Cover selection steganography with intra-image scanning. *Proceedings of the 2018 28th International Conference Radioelektronika* (*RADIOELEKTRONIKA*), Prague, Czech Republic, 2018. P. 1–4.

[14] Molato M., Gerardo B. Cover image selection technique for secured LSB-based image steganography. *Proceedings of the 2018 International Conference on Algorithms, Computing and Artificial Intelligence* (*ACAI'18*), Sanya, China, 2018. P. 1–6.

[15] M.S. Subhedar, "Cover selection technique for secure transform domain image steganography," *Iran J Comput Sci*, vol. 4, pp. 241–252, 2021, doi: 10.1007/s42044-020-00077-9v

[16] Shah P.D., Bichkar R.S. Genetic algorithm based approach to select suitable cover image for image steganography. *Proceedings of the 2020 International Conference for Emerging Technology* (*INCET*), Belgaum, India, 2020. P. 1–5.

[17] Douris C. *Balancing Smart Grid Data and Consumer Privacy*. Available at: https://www.lexingtoninstitute.org/wp-content/uploads/2017/07/Lexington_Smart_Grid_Data_Privacy-2017.pdf (accessed 26.12.2024).

[18] Khadam U. et al. Advanced security and privacy technique for digital text in smart grid communications. *Computers & Electrical Engineering*, 2021, vol. 93, 107205.

[19] Natkaniec M., Kępowicz P. StegoEDCA: An Efficient Covert Channel for Smart Grids Based on IEEE 802.11e Standard. *Energies*, 2025, vol. 18, no. 2, 330.

[20] Qasim Q.A., Golshannavaz S. Data protection enhancement in smart grid communication: An efficient multi-layer encrypting approach based on chaotic techniques and steganography. *e-Prime - Advances in Electrical Engineering, Electronics and Energy*, 2024, vol. 10, 100834.

[21] Rathika S., Gayathri R. Performance analysis of data hiding in thermal image using alpha blending technique. *Materials Today: Proceedings*, 2021, vol. 46, part 20, pp. 10164-10168.

[22] Koshy D.T., Vijayananth S. Steganography on thermal images using generation technique. *Proceedings of the 2014 IEEE International Conference on Advanced Communications, Control and Computing Technologies*, Ramanathapuram, India, 2014. P. 214–218.

[23] Gong L., Han Y., Li R. STGAN: A Fusion of Infrared and Visible Images. *Electronics*, 2025, vol. 14, no. 21, 4219.

[24] Alkodre A.B. et al. A Shuffling-Steganography Algorithm to Protect Data of Drone Applications. *Computers, Materials & Continua*, 2024, vol. 81, no. 2, pp. 2727–2751.

[25] Bobok I., Kobozieva A. Normalized separability of the maximum singular number of a digital image block as an indicator of the feasibility of its stegano transformation. In V. Vychuzhanin (Ed.), *Information Control System and Intelligent Technologies: Advances and Applications*. Lviv, 2025. P. 58–75.

[26] Wang Z., Bovik A.C., Sheikh H.R., Simoncelli E.P. Image quality assessment: from error visibility to structural similarity. *IEEE Transactions on Image Processing*, 2004, vol. 13, no. 4, pp. 600–612.

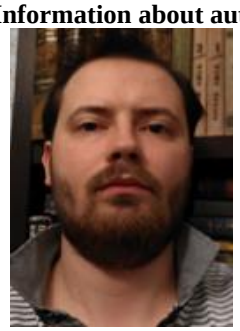
[27] Chen M., He P., Liu J. HLTD-CSA: Cover selection algorithm based on hybrid local texture descriptor for color image steganography. *Journal of Visual Communication and Image Representation*, 2022, vol. 89, 103646.

[28] SEC "ZTZ-Service". *Services on transformers and transformer equipment*. Available at: http://ztz-service.com.ua/en/transformer-services (accessed 23.11.2025).

[29] Hameed M.A., Hassaballah M., Aly S., Awad A.I. An Adaptive Image Steganography Method Based on Histogram of Oriented Gra-

dient and PVD-LSB Techniques. *IEEE Access*, 2019, vol. 7, pp. 185189–185204.
[30] Xie G. et al. A Novel Gradient-guided Post-processing Method for Adaptive Image Steganography. *Signal Processing*, 2023, vol. 203, 108813.
[31] Gonzalez R.C., Woods R.E. *Digital Image Processing*. Pearson: Upper Saddle River, USA, 2018.
[32] Dukkipati R.V. *Numerical Methods*. New Age International Pvt Ltd Publishers, 2010.
[33] Hsu Y., Chang S. Detecting image splicing using geometry invariants and camera characteristics consistency. *2006 IEEE International Conference on Multimedia and Expo*, Toronto, 2006. P. 549–552
[34] Gloe T., Böhme R. The "Dresden Image Database" for benchmarking digital image forensics. *Proceedings of the 2010 ACM Symposium on Applied Computing* (*SAC '10*). New York, 2010. P. 1585–1591.
[35] NRCS Photo Gallery. United States Department of Agriculture. Washington, USA. Available at: https://www.nrcs.usda.gov/ (accessed: 26.07.2012).
[36] Ardila P.A.R. et al. Analysis of gemorphological systems using morphometric techniques in the Pla de Sant Jordi, Mallorca, Illes Baleares. Available at: https://www.researchgate.net/publication/370028545_Analysis_of_gemorphological_systems_using_morphometric_techniques_in_the_Pla_de_Sant_Jordi_Mallorca_Illes_Baleares (accessed 23.11.2025).
[37] Peng Q. et al. Crafting Synthetic Realities: Examining Visual Realism and Misinformation Potential of Photorealistic AI-Generated Images. *Proceedings of the Extended Abstracts of the CHI Conference on Human Factors in Computing Systems* (*CHI EA '25*), Yokohama, Japan, 2025. P. 1–12.
[38] Al-Aidroos N.M., Bahamish H.A. Image steganography based on LSB Matching and image enlargement. *Proceedings of the 2019 1st International Conference of Intelligent Computing and Engineering* (*ICOICE*), Hadhramout, Yemen, 2019. P. 1–6.
[39] Melnik M.A. Compression-resistant steganography algorithm. *Information Security*, 2012, no. 2, 99–106.
[40] Wang S.-Y. et al. CNN-Generated Images Are Surprisingly Easy to Spot… for Now. *Proceedings of the 2020 IEEE/CVF Conference on Computer Vision and Pattern Recognition* (*CVPR*), Seattle, 2020. P. 8692–8701.

Information about authors.



Ivan Igorovych Bobok
Doctor of Technical Science, Associate Professor. Department of Computer Systems and Software Technologies. Odesa Polytechnic National University.
Research interests: Steganography, Information security
ORCID: 0000-0003-4548-0709
Email: onu_metal@ukr.net

Svitlana Mykolaivna Hryhorenko
Candidate of Technical Sciences, Associate Professor. Department of Computer Systems and Software Technologies. Odesa Polytechnic National University. Research interests: Steganography, Information security
ORCID:0009-0006-4551-8243
Email: sngrygorenko@gmail.com

Alla Anatoliivna Kobozieva
Doctor of Technical Science, Professor. Department of Cybersecurity and Information Protection. Odesa National Maritime University.
Research interests: Steganography, Mathematics in information security
ORCID:0000-0001-7888-0499
Email: alla_kobozeva@ukr.net

Ksenia Leonidivna Yavorska
Master's student of the Department of Cybersecurity and Information Protection. Odesa National Maritime University.
Research interests: Steganography, Mathematics in information security
ORCID: 0009-0009-3782-7347
Email: ksenya.foxy05@gmail.com