Theoretical Foundations of a New Approach to Container Selection when Organizing a Steganographic Communication Channel

Ivan Bobok[1], Svitlana Hryhorenko[1], Alla Kobozieva[2] and Oksana Vasylenko[3]
[1]*Department of Computerized Systems and Software Technologies, Odesa Polytechnic National University, Shevchenko Avenue 1, 65044 Odesa, Ukraine*
[2]*Department of Cybersecurity and Information Protection, Odesa National Maritime University, Mechnikova Str. 34, 65029 Odesa, Ukraine*
[3]*Preparatory College of Saxony-Anhalt, Anhalt University of Applied Sciences, Lohmann Str. 23, 06366 Köthen, Germany*
onu_metal@ukr.net, s.m.hryhorenko@op.edu.ua, alla_kobozeva@ukr.net, oksana.vasylenko@hs-anhalt.de

Keywords: Container Selection, Perception Reliability, Structural Similarity Index Measure (SSIM), Singular Value Decomposition.

Abstract: The most promising direction of information protection today is steganography, the main goal of which is to hide the very fact of the existence of information exchange. The choice of container plays a key role in ensuring certain properties of the steganographic system, but the problem of container selection currently has no satisfactory solution. *The aim* of the work is to develop the theoretical foundations of a new approach to a priori selection of a container from a given set of digital candidate images, common in the sense of independence from the steganographic algorithm used, to improve the visual quality of the steganographic message. *The aim is achieved by means of* a well-founded definition of the container selection criterion; choosing a quantitative indicator of the visual quality of the steganographic message. *The most significant results* of the work are the theoretical justification of the feasibility of using the normalized separation of the maximum singular number of the image matrix as a selection criterion. *The significance of the obtained theoretical results* lies in the possibility of their effective practical use for selecting a container from a given set of candidates, which is demonstrated in the work by means of a computational experiment. It is shown that using the selected image as a container allows obtaining the best/close to the best structural similarity index for the corresponding steganographic message (the maximum deviation from the best value within the experiment was 0.3%), regardless of the steganographic algorithm used and the format of the candidate images. Using subjective ranking, it was established that the visual quality of steganographic messages obtained based on selected containers was improved compared to random ones.

1 INTRODUCTION

In today's conditions of rapid development of digital technologies and globalization of information networks, the problem of ensuring the confidentiality of data transmission is becoming critical. According to analytical reports of ENISA and ITU [1], [2], in conditions of rapid expansion of the cyberthreats and improvement of automated traffic monitoring tools, steganography is becoming particularly relevant, the main purpose of which is to hide the very fact of the existence of information exchange [3], [4]. This approach allows to divert/reduce the attention of a potential attacker to the communication channel, which is strategically important for protecting private and corporate data in the information environment.

The effectiveness of a steganographic system is determined by a compromise between its capacity, stability and visual invisibility of the changes made - the reliability of perception of the steganographic message [5]. The key role in achieving this balance is played by the choice of the container [6]-[8], as which the work considers a digital image. The properties of the container determine the degree of potential concealment of embedded data - additional information, which for modern steganography is a digital sequence that is the result of the work of the steganographic system`s precoder. Random choice of container for some steganographic methods can lead

to visual distortions as a result of embedding additional information [9].

2 LITERATURE REVIEW

Considering that failure to ensure the reliability of perception as a result of a subjective attack will instantly lead to the detection of the presence of a hidden (steganographic) communication channel, this requirement most often becomes key when choosing a container in the works of modern Specialists [7], [10]. In [10], the authors note that the goals of improving steganographic systems today are divided into two groups: the first is aimed at maximizing the ability to hide information; the second is to minimize the visual distortion of the container as a result of embedding additional information. The higher the visual quality of the steganographic message, the less attention it attracts to itself, which obviously increases the degree of security of the embedded information.

One approach to automating container selection is proposed in [11]. The authors use evolutionary programming to generate mathematical rules (signatures) that allow selecting a container based on its ability to counteract statistical steganography. The peak signal-to-noise ratio (PSNR) is used to assess visual distortions when obtaining a steganographic message. This difference indicator has a weak correlation with the visual perception of the digital image by a person, does not take into account the Spatial relationships of pixels, considering them as independent. Similar remarks can be attributed to the following works [12]-[14]. In [12], the idea is implemented that the optimal digital image for the role of a container is a digital image in which the process of embedding the additional information leads to minimal disturbances. The proposed method in the course of its work scans all possible positions for embedding a secret message in a container and performs such a scan for all candidate digital images, which leads to its significant computational complexity and is often an insurmountable obstacle to the use of the method in practice. In [13], a method for selecting a container from a set of digital images for a given secret message, which is also considered in the form of digital images, is proposed. The method is divided into two main steps: first, the set of candidates is filtered taking into account the relative entropy and features of their histograms in order to filter out unambiguously unsuitable candidates; second, the local characteristics of the pixel intensity of the blocks of digital images-candidates are analyzed. The proposed method, as its authors claim, demonstrates high visual quality of the steganographic message, but since the difference PSNR indicator is used to evaluate it here, as noted above, the objectivity of the authors' assessment can be questioned. In [14], the container selection problem is considered, for the solution of which a method based on a genetic algorithm is proposed, which ensures good compatibility with the given secret data. But the conclusion about good compatibility is again made using the difference indicators: PSNR and MSE.

To assess the visual quality of a steganographic message, not only difference indicators can be used. An example of a metric that tries (not without success) to take into account the peculiarities of the perception of the human visual system can be considered the structural similarity index (SSIM) [15], and the results of assessing the effectiveness of container selection methods presented within the framework of using this metric in [10], [16] have a higher priority and trust among the authors of this article than the previous ones. Thus, in [16] an approach to container selection is proposed, based on the analysis of the features of the texture of the central image and the human visual system, within which the similarity between the original central image and the corresponding steganographic message is quantitatively assessed. As a result, one central image container is selected that has the maximum similarity with its steganographic message. Despite the authors' attempt to take into account the peculiarities of the human visual system through the use of SSIM, their approach is limited to the analysis of the statistical characteristics of the texture in discrete directions. This leaves out the holistic structural similarity between the container and the steganographic message.

In [10], the problem of visual quality of the steganographic message is considered as a classification problem, where a classifier based on a convolutional neural network (CNN) is used to select a digital image from a set of candidates for the role of a container that can provide high quality - perceptual reliability, which is estimated using SSIM, after the steganographic transformation process (STP). A binary classifier divides the digital images into high - and low-quality classes, based on the SqueezeNet architecture. The CNN was trained in two scenarios: transfer learning and learning from scratch. Although both classifiers, according to the authors, were able to achieve high accuracy, they have fundamental shortcomings. The first of these shortcomings is

common to methods based on deep learning: the process of this training works as a "black box", not giving an answer why this digital image was chosen, as a result of which, in the presence of an unsatisfactory result, it is impossible to get an answer about the reason for this and, as a result, make adjustments. In addition, the result of the learning process critically depends on the training sample. The second drawback concerns the idea of a binary classifier. The binary distribution is very rigid. For most of the digital images, they cannot be unambiguously attributed to textured or homogeneous. As a rule, the digital image has areas with different degrees of texture, which is not taken into account in the case of a binary classifier. If the digital image is defined as having high quality - textured, then as a result of embedding the digital image without taking into account the possible presence of homogeneous subregions in the selected container, the situation of the appearance of artifacts after the STP is likely.

It should be noted that, given the diversity of the image in all its properties, the idea of a clear division of them into classes of suitable and unsuitable for the role of a container is, in the opinion of the authors of this article, unpromising. It is fundamentally wrong to expect a clear division from a selective method, since such a division can only be based on clear thresholds for quantitative estimates of a particular digital image parameter, but the threshold will always be tied to the image database that is being considered (or used for training the network) at the moment. Changing the candidate database will, as a rule, lead to a change in the threshold values, i.e., a change in the quantitative characteristics of the classifier and a decrease in its efficiency.

3 METHODOLOGY

A characteristic feature of many methods available today for selecting a container in order to ensure the visual quality of the corresponding steganographic message is their focus on a specific steganographic algorithm [17], [18]. Such a focus helps to ensure their effective operation, but it severely limits the scope of application, which in conditions of lack of time, which often occur in practice when solving information protection problems, in particular the problem of organizing a covert communication channel, can be critical. It is clear that, taking into account the existing general sufficient conditions for ensuring the reliability of steganographic message perception [19], [20], the problem of selecting a container should have a general solution that is not focused on the specifics of a particular steganographic algorithm.

Thus, today it cannot be stated that the problem of choosing a container to ensure the visual quality of the corresponding steganographic message has a satisfactory solution. Taking this into account,

The aim of the work is to develop the theoretical foundations of an approach to a priori selection of a container from a given set of digital images-candidates, general in the sense of independence from the steganographic algorithm used, to improve the visual quality of the steganographic message.

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

1) Determining a quantitative criterion for container selection in order to ensure a (relatively) high-quality steganographic message in the visual sense;
2) Selection of a quantitative indicator for assessing the visual quality of the steganographic message - an indicator of the effectiveness of the corresponding steganographic system;
3) Study of the dependence of the visual quality of the joint venture on the container selection criterion.

3.1 Determining the Quantitative Criterion for Container Selection

Let F *be* an $n \times n$ matrix of the digital image with elements f_{ij}, $i,j = \overline{1,n}$. For it, we can construct a singular decomposition:

$$F = U\Sigma V^T, \quad (1)$$

where: U, $V$are orthogonal matrices, the columns of which u_i, v_i, $i = \overline{1,n}$ are the left and right singular vectors (SV) *of* F, respectively, $\Sigma = diag(\sigma_1, \sigma_2, \ldots, \sigma_n)$and are the diagonal matrix of singular numbers (SN): $\sigma_1 \geq \sigma_2 \geq \ldots \geq \sigma_n \geq 0$, $\sigma_i \in R$, $i = \overline{1,n}$, R are the set of real numbers. In accordance with the general approach to the analysis of the state of information systems, based on matrix analysis and perturbation theory [19], [21], [22], the STP of a central container with matrix F can be represented in the form $\overline{F} = F + \Delta F$ ($\overline{F}$, Δ F is the steganographic message matrix with elements $\overline{f}_{ij}$, $i,j = \overline{1,n}$, and the container perturbation as a result of the STP), and, as a result, in the form of a set of perturbations of the full set of formal parameters F - SV and SN, which is the result of embedding the digital image. Thus, the singular decomposition and

its parameters play a key role in assessing the state of the resulting steganographic message.

Since the main goal of this work is to select a container that provides relatively high-quality visual steganographic message, while the smallness of the norm $\|\Delta F\|$is often considered as an indicator of ensuring a significant probability of reliable perception of steganographic message [12], among the parameters of the full set it is necessary to select those whose perturbations will adequately reflect the strength of the $\|\Delta F\|$perturbation during STP - insensitive, or resistant, to perturbations. Among the SV matrices of any digital image, there are both stable and unstable ones [19], [21], [22] in accordance with the relation:

$$sin\,2\,\theta_i \le \frac{2\|\Delta F\|_2}{svdgap(i,F)}, \qquad (2)$$

where :$\theta_i$is the rotation angle u_i (v_i) as a result of the turbulent action ΔF, $\|\cdot\|_2$is the spectral matrix norm, $svdgap(i,F) = \min\limits_{i\neq j}\left|\sigma_i - \sigma_j\right|$is the separation of the SN σ_i. All SNs are stable or well-conditioned: $\max\limits_i\left|\sigma_i(F) - \sigma_i\left(\overline{F}\right)\right| \le \|\Delta F\|_2$, where$\sigma_i(F)$, $\sigma_i\left(\overline{F}\right)$ - SN matrices, F, $\overline{F}$respectively.

Of texture of the steganographic message container is desirable [18], [23]: the container should have a large number of contours, small details, etc., that is, a significant relative volume of such subregions where there are significant differences in pixel brightness values, which leads to a relatively significant high-frequency component.

Recently, to organize the separation of the digital image, stored in various forms (with/without loss), the authors justified the feasibility of using the normalized gap of maximum SN (NGMSN) of the corresponding matrix: $svdgap_n(1) = \overline{\sigma}_1 - \overline{\sigma}_2$, the calculation of which corresponds to the general formula for the normalized separation of SN σ_i:

$$svdgap_n(i) = \min\limits_{i\neq j}\left|\overline{\sigma}_j - \overline{\sigma}_i\right|, \qquad (3)$$

where: $\overline{\sigma}_i$, $i = \overline{1,n}$, are defined as: $\overline{\sigma}_i = \frac{\sigma_i}{\|(\sigma_1,\sigma_2,\ldots,\sigma_n)\|}$, $\|(\sigma_1,\sigma_2,\ldots,\sigma_n)\|$- Euclidean norm of the vector $(\sigma_1,\sigma_2,\ldots,\sigma_n)$. The NGMSN is obtained from (3) with $i = 1$taking into account that for the SN of the original digital image:

$$\sigma_1 >> \sigma_2 \ge \ldots \ge \sigma_n \ge 0. \qquad (4)$$

The difference in the values of the NGMSN in [24] was an indicator of the difference in the relative content of the high-frequency component, which for the lossy format is less than the corresponding indicator in the lossless format. Considering such "abilities" of the NGMSN, it is proposed to use it as a criterion for selecting the digital image-containers that provide the visual quality of the steganographic message, which is explained by the following considerations.

There is a close connection between singular decomposition and the structure of the digital image. According to [15], the structure of the digital image is understood as the set of its geometric features (edges, outlines of objects, contours, textures, details), which can be observed at different scales. It should be noted here that it is the violation of the digital image structure that is, as a rule, the most noticeable to the human eye [15]. The singular decomposition (1) of the matrix F can be written in the form of outer products [25]:

$$F = \sum_{i=1}^{n}\sigma_i u_i v_i^T, \qquad (5)$$

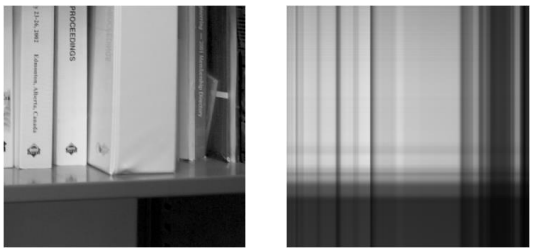
that is, it gives a representation of the digital image as a sum of peer matrices $\sigma_i u_i v_i^T$.

The geometry, the “skeleton” of the digital image is described by the SV [25], [26]. The left/right SV characterize its vertical/horizontal structures: each vector u_i/v_idetermines how the intensity changes along the vertical/horizontal axis, and $u_i v_i^T$creates a peer-to-peer “base” image [26] - the structure of the digital image as a whole, which looks like a set of stripes, grids or contours of a certain direction (Fig. 1). If the components of the vector $v_i$differ slightly, and in $u_i$have significant differences, then the resulting matrix $u_i v_i^T$will consist of horizontal lines, otherwise we will get vertical stripes.

The first SV usually describe the roughest, most important contours of objects, which generally define the scene of the digital image, and the following ones - (small) details, noise. The SN describe the intensity of these structures, i.e. they are weights for these structures. As a result of adding several components $u_i v_i^T$with different weights, $\sigma_i$complex shapes are obtained [26].

Thus, the form (5) clearly indicates the close connection of the singular decomposition of the matrix of the digital image with its structure. If the image has a relatively large NGMSN in comparison with other candidates for the role of the container, this will mean that in such an image the base image dominates more than in others, $\sigma_1 u_1 v_1^T$thereby reducing the relative content of fine details, noise, i.e. the content of the high-frequency component. For the image, which has an insignificant, relative to other candidates, NGMSN, dominance $\sigma_1 u_1 v_1^T$will not be so significant, speaking of the presence of a certain number of parts in the central unit, the presence of a

certain noise, which is a positive sign for using such a central unit as a container, an indicator of which is the NGMSN.



(a) (b)

Figure 1: Relationship between the singular decomposition of the image matrix and its structure: a) - original digital image; b) - peer approximation$\sigma_1 u_1 v_1^T$.

The stability of the structure of the digital image is actually determined by the stability of its SNR, which corresponds to the relation (2). It should be noted that the overall structure of the digital image will mainly depend on the first SV (Fig. 1): the terms in (5) are not equal, the first term carries almost all the energy of the digital image due to (4). If the first SV is disturbed, this will disturb the main axis of the digital image, deforming its structure in such a way that it will be noticed by the observer with a high probability. SV disturbances, which correspond to low-separation SNs, will usually lead to disturbances in small details, texture, which can be ignored by the human visual system. This means, firstly, that, in general, a conclusion about the structure of the digital image can be made by analyzing only the visually dominant structure - $\sigma_1 u_1 v_1^T$, and secondly, absolute dominance is undesirable for $\sigma_1 u_1 v_1^T$the STP: for a container, the better, the relatively smaller the dominance of the first peer approximation will be. A quantitative assessment of the degree of this dominance is the (normalized) separation σ_1. Thus, further, the NGMSN of the corresponding matrix is used as a criterion for selecting the image containers that ensure the visual quality of the steganographic message.

3.2 Choosing a Quantitative Indicator to Assess the Visual Quality of a Steganographic message

The process of container selection is a task that requires consideration of the preservation of complex relationships between the elements of the digital image and its structure.

The use of containers with a high degree of texturity allows for effective masking of the results of step-pan transformation, using the peculiarities of human perception. In this aspect, the use of metrics that can quantify structural distortions of the digital image becomes critically important.

The most common in steganography to date for assessing the reliability of perception of the formed steganographic message remain difference indicators [27], in particular, the mean square error (MSE), the peak signal-to-noise ratio (PSNR), which are quite mathematically simple in their implementation. MSE and PSNR are related to each other:

$$PSNR = 10\,lg\left(\frac{255^2}{MSE}\right),$$

where: $MSE = \frac{1}{mn}\sum_{i=1}^{n}\sum_{j=1}^{m}\left(f_{ij} - \overline{f}_{ij}\right)^2$.

These indicators are not justified for steganography because the assessment of the reliability of perception of the formed steganographic message involves a mandatory expert assessment of a person - visual perception, the specificity of which is not taken into account in these indicators.

The disadvantages of difference indicators are not limited to this. As is well known [26], pixels in the digital image are not independent: the brightness values of neighboring pixels are correlated, they form contours, objects, however, all difference indicators consider each pixel in isolation.

This leads in particular to the fact that the difference indicators do not reflect the difference between the "destruction" of the structure (for example, a break in the nose line on the face) and some uniformly distributed disturbance throughout the digital image, which does not change the overall scene, geometry (mutual arrangement of lines, angles, etc.) and the "content" of objects, i.e. the structure of the digital image, and may go unnoticed. An attempt to smooth out the above-mentioned shortcomings in the quantitative assessment of digital image distortion was made when developing the SSIM metric in [15]:

$$SSIM(X,Y) = \frac{(2\mu_X\mu_Y + C_1)(2\sigma_{XY} + C_2)}{(\mu_X{}^2 + \mu_Y{}^2 + C_1)(\sigma_X{}^2 + \sigma_Y{}^2 + C_2)}, \quad (6)$$

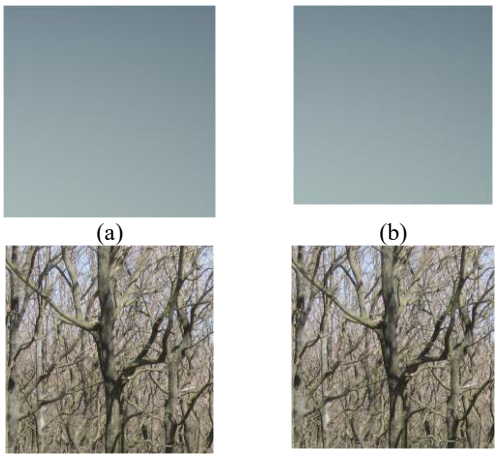
where: *X, Y* - the presented and distorted digital image, respectively ($L \times L$ corresponding windows of the presented and distorted digital image), μ_X, μ_Y - the average brightness values, $\sigma_X{}^2$, $\sigma_Y{}^2$- the variance (contrast index) for (windows) image *X, Y,* respectively, σ_{XY}- the covariance (structural similarity index (windows) image), C_1, C_2- constants introduced by the authors to stabilize the calculations. The closer the index (6) is to unity, the less distortions the human eye should notice according to the authors' idea. Such an orientation towards subjective assessment is achieved for (6) due

to the fact that the authors tried to simultaneously take into account three indicators when constructing the metric: the brightness of the image pixels, contrast and structure.

Gaussian noise with the same parameters was used as a perturbation for both images, resulting in the same value of $PSNR = 33dB$. At the same time, the distortions for the homogeneous digital image are visually noticeable (heterogeneity appeared throughout the image) (Fig. 2b), unlike the textured image (Fig. 2d), which was not demonstrated by the difference distortion indicator. The SSIM metric behaved much better as expected, giving values of 0.8804 and 0.9674, respectively, clearly reflecting the existing connection with the visual perception of the digital image, demonstrating the advantage of the second SI for the role of a container.

The next advantage of the SSIM metric for use in the field of steganography is its ability to provide a distortion map (*SSIM map*) - a matrix of the same size as the studied image *F,* each element of which is a characteristic of the quality of the corresponding pixel *F*: in the distortion map, the value of each element represents the result of a comparative analysis of the values of the fragment (window) around the pixel. Practically, in the distortion map, light zones indicate that the structure of the digital image in these subregions is preserved, while dark zones indicate the destruction of the structure. These characteristics of the SSIM are very important for steganography, in particular, the distortion map makes it possible to see in which zones the STP distorts the (structure) of the digital image container the most/least (Fig. 3).

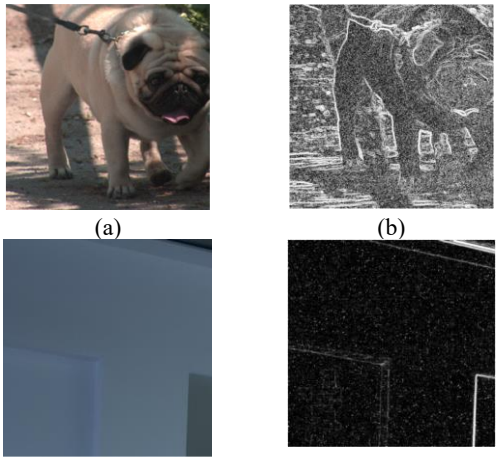
The two examples in Figure 3 are chosen intentionally: for the digital image (Fig. 3d) on the distortion map there are black areas that correspond to the background areas of the container (Fig. 3c) - confirmation that the use of homogeneous areas for the STP can with a high probability lead to a violation of the reliability of the steganographic message perception. On the distortion maps (Fig. 3b, d) the most favorable - light areas corresponding to the contours (which are known to be priority areas for embedding the digital image from the point of view of the reliability of the steganographic message perception). For the image (Fig. 3a) and its other areas are not critically unacceptable for embedding the image (painted in gray (Fig. 3b). This is natural and expected, because this image is textured.



(a) (b) (c) (d)

Figure 2: Illustration of the advantage of the SSIM metric for assessing the visual quality of the image: a), c) - original images; b), d) - digital images, which are the results of superimposing Gaussian noise with zero matrix expectation and *D* =0.0005.

Speaking about the choice of a container in order to improve the quality of visual perception of the steganographic message, it should be noted that the application of the PSNR metric in the conditions of using one of the most widespread to date steganography methods - the least significant bit modification method when implementing LSB-matching [28], is generally uninformative: the PSNR values will be practically the same for all candidates.



(a) (b) (c) (d)

Figure 3: Examples of obtained distortion maps for images containers as a result of applying the LSB method with a hidden channel bandwidth of 1 bit/pixel: a), c) - original central processing units; b), d) - *SSIM maps*.

Thus, SSIM compared to difference measures of the estimation of the distortion of the digital image has significant advantages for application in the field of steganography. Unlike approaches focused on difference measures, SSIM-based analysis allows to identify images and local areas where interference minimally disrupts the correlation between neighboring pixels, the use of which is key to ensuring the resistance of the digital image to subjective attacks.

Despite its advantages, to date, the *SSIM metric* has significantly lost to differential metrics in terms of frequency of use. To ensure objectivity in the choice of metric, let's consider the reasons for ignoring SSIM in most modern works on selective steganography:

- PSNR and MSE are simpler in mathematical sense and computational sense than SSIM. Indeed, for *an n×n* matrix of the digital image, to calculate one term in the sum for MSE, two operations are required, which will give $2n^2$for all terms, and $2n^2 + (n^2 - 1)$to form a double sum, i.e. the total number of operations $K_{MSE}$to calculate MSE will be:

$$K_{MSE} = 2n^2 + (n^2 - 1) + 2 = O(3n^2) = O(n^2). \quad (7)$$

- The computational complexity for calculating PSNR will differ from (7) by adding a small number of operations (three arithmetic operations and one - taking the logarithm), which does not depend on n, will also be defined as $O(3n^2) = O(n^2)$. SSIM for each pixel is calculated in a local window, usually of size L×L (in practice most often $L = 11$). The number of operations for processing one pixel at a given window size depends only on L and is constant taking n into account. The total number of pixels here is n^2. Then the order of computational complexity for calculating SSIM (6) here will also be n^2, as in (7) for MSE, but the coefficient at n^2will be determined L^2 [15], i.e. the computational complexity of calculating SSIM will be: $K_{SSIM} = O(L^2 n^2) = O(n^2)$, and at $L = 11$will be 40 times greater;
- The SSIM indicator characterizes the visual quality of the steganographic message better than the difference indicators, but it is inferior to the difference indicators in terms of quantitative assessment of the stego-message's resistance to steganography. A large number of classical steganography methods are based on the analysis of changes in pixel brightness. MSE, PSNR correlate with changes in signal amplitude, SSIM can be high even if the pixel values have changed significantly (the main thing here is to preserve the structure), which will be a direct indicator of the presence of additional information for a statistical steganography analyzer;
- Scientific "inertia": the use of differential indices in steganography over the past few decades has led to the need to use these indices in recent years to ensure correct comparison with previous methods.

Of the above reasons for the limited use of SSIM from a practical point of view, taking into account the purpose of the work, the first is the main one. However, work on reduction $K_{SSIM}$is being carried out quite actively [29], [30], allowing the use of SSIM even in real time.

Considering the above, SSIM is chosen to assess the visual quality of the resulting steganographic message.

4 RESULTS AND DISCUSSION

The SSIM indicator of container distortion at STP is clearly related to the NGMSN of its matrix. Given that: the structure of the digital image is determined by its peer components $\sigma_i u_i v_i^T$; for embedding the additional information, it is natural to use the existing differences in brightness values, the number of which should be relatively large to ensure a satisfactory bandwidth of the covert channel; it is necessary to avoid changes in $\sigma_1 u_1 v_1^T$; for the STP, absolute dominance is undesirable $\sigma_1 u_1 v_1^T$, the quantitative assessment of the degree of which is the NGMSN, then using a digital image with a relatively small NGMSN as a container should lead to a relatively significant SSIM at STP. That is, theoretically expected here is an inversely proportional relationship between the NGMSN values of the container matrix and the SSIM, which characterizes the container distortion as a result of additional information embedding. This conclusion is general, i.e. does not depend on the specifics of the steganography method used and the digital image format. To confirm this conclusion in practice, a computational experiment was conducted, during which 8 sets of practical power images (100 images in a set) were formed from the bases [31]-[33] (two sets of digital images from each base), which are traditional when working with digital images, as well as two sets of images obtained by non-professional

cameras. Some typical results of the experiment are presented in Figure 4, 5a, where the real largest SSIM value is marked in red, and the one corresponding to the digital image with the smallest NGMSN, if these values do not coincide, in green.

The results are demonstrated on the image sets: M_1 [31] - digital images size 560×560 (Tif format); M_2 [32] - 560×560-images (Jpeg format, QF=75); M_3 - 1000×1000-images (Tif format), obtained with a non-professional camera; M_4 [33] - 1000×1000-images (Jpeg format). Steganography methods considered were the LSB method and the method [9], which does not systematically preserve the reliability of the perception of the steganographic message, but today remains one of the most resistant to compression attacks.

The obtained results, in general, correspond to theoretical expectations: in most cases, there is a correspondence between the largest SSIM value and the smallest value of the container's NGMSN.

If this does not even occur, as, for example, (Fig. 4a, c), then the SSIM value obtained for the smallest NGMSN differs slightly from the maximum possible for the set (the maximum such deviation was recorded in the case of the set M_3, which was 0.3%), since in each case a monotonic decrease in the trend of the function is observed $SSIM = f(\text{NGMSN})$ (Fig. 4, 5a) regardless of either the format of the digital image or the steganography method used when obtaining the steganographic message.

But the strict decrease of the function $SSIM = f(\text{NGMSN})$, which could be expected in accordance with theoretical considerations, is absent. There are several reasons for this. First, none of the quantitative indicators used at all gives an accurate mathematical estimate of the characteristic of the digital image for which it is used: NGMSN - for the contribution of the high-frequency component; SSIM - for the visual quality of the perception of the digital image by a person, but within the limits of the problem considered in the work, such estimates cannot be quantitatively accurate at all. Indeed, it is fundamentally impossible to assess the contribution of the high-frequency component in the digital image absolutely accurately even in the frequency domain, since there is no exact distribution of frequency coefficients into high-, medium- and low-frequency ones. And any agreement here regarding where to "draw the line" between the medium- and high-frequency coefficients cannot be general in principle, taking into account the difference in the size of the image, the diversity of the digital image in any of its characteristics, in particular, texture. Secondly, SSIM depends on the brightness, contrast, and structural similarity of the image, and the NGMSN is mainly focused on the structure component. But when embedding the additional information, changes occur in both the brightness and contrast of the digital image. Thirdly, the process of (slight) blurring of the digital image leads to an increase in the NGMSN [24], but SSIM can remain practically unchanged if the structure of the digital image is not destroyed. This is very clearly visible on the corresponding images, which, displaying the same scene, differ only in the storage format (with/without loss). It is precisely due to the above reasons that there is a possibility of obtaining not the largest possible SSIM value for the set of images for the image with the smallest NGMSN, as well as a "scatter" at close arguments (NGMSN values) of points on the graphs (SSIM values) in Figure 4, 5a.

Special attention in the experimental part of the study was paid to the CGs generated using artificial intelligence, as their use as containers is spreading every day. It is obvious that such CGs have a different statistical structure, a detailed study of which is devoted to the authors' article, which is currently being prepared for publication, but the nature of the relationship between SSIM and NGMSN remain the same (Fig. 5b), where artificially generated digital images from the database [34] are used.

Thus, the existing relationship between SSIM and NGMSN is theoretically justified and practically confirmed: the trend of the function $SSIM = f(\text{NGMSN})$decreases with the increase in NGMSN, which indicates the prospects of using NGMSN as a criterion for a priori container selection to improve the visual quality of the steganographic message and is confirmed by the results of the computational experiment (Fig. 4 and 5) and the results of subjective ranking, typical of which are shown in Figure 6. Here, the set M_3 was deliberately taken, where the largest deviation from the maximum possible SSIM set in the digital image was obtained, which had the smallest NGMSN. As can be seen, even when the obtained steganographic message based on the selected container does not have the maximum SSIM value, the quality of perception of such a steganographic message is better than under the same conditions of the obtained steganographic message based on a randomly selected container in M_3, where there are obvious artifacts.

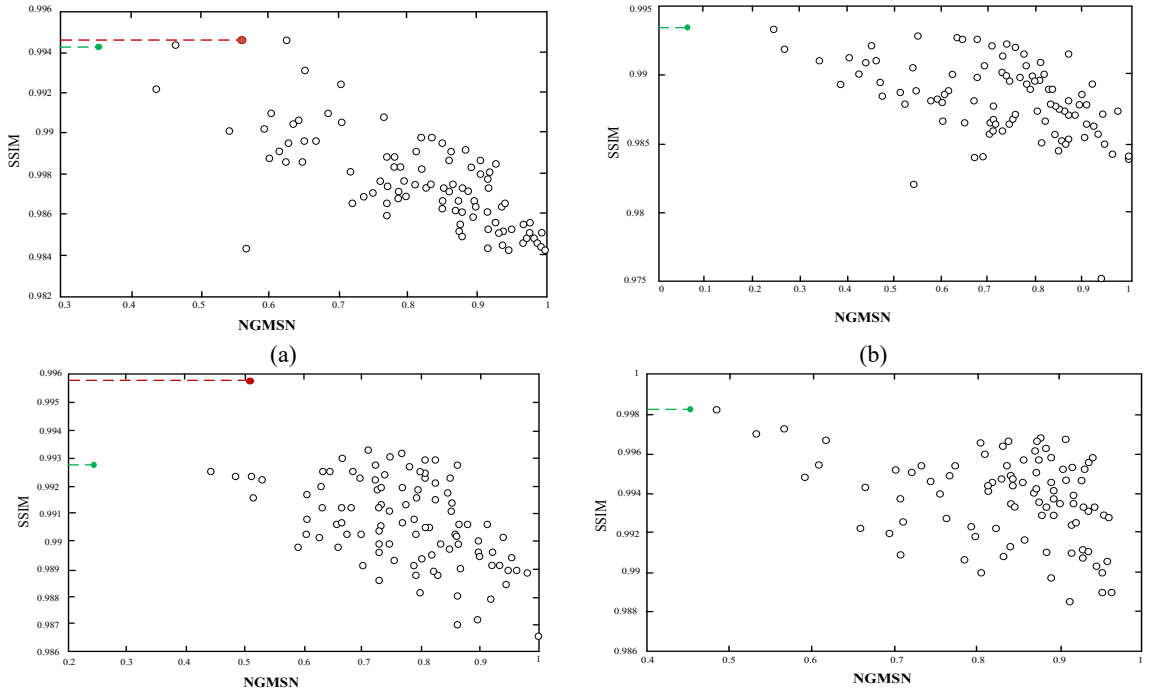


Figure 4: Dependence of the SSIM indicator, which characterizes the visual distortion of the container as a result of steganography by the LSB method with a hidden channel bandwidth of 1 bit/pixel, on the NGMSN of the container matrix for the digital image from the set: a) - M_1; b) - M_2; c) - M_3; d) - M_4.

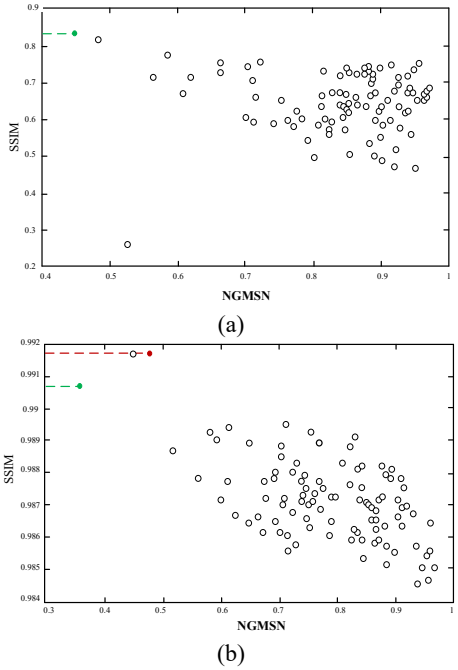


Figure 5: Dependence of SSIM on the container's NGMSN: a) - STP by the method [9], in which all blocks were used, for the digital image with M_4; b) - STP by the LSB method with a hidden channel bandwidth of 1 bit/pixel for artificially generated central processing units.

For practical application of the obtained theoretical results - construction of the corresponding selective method, it is necessary to reduce the degree of "dispersion" of SSIM values at close values of the NGMSN. This can be done using a weighting coefficient, which is determined in a certain way for the correction of the NGMSN, which is the direction of further work of the authors.

(a) (b)

Figure 6: Steganographic messages formed by the steganography method [9] when using all blocks based on a container from the set M_3: a) - with the smallest NGMSN; b) - randomly selected.

5 CONCLUSIONS

The work solves an important scientific problem of developing theoretical foundations of an approach to selecting a container from a given set of digital images candidates, general in the sense of independence from the steganographic algorithm used, format (with/without loss) to improve the visual quality of the steganographic message. In the course of developing the specified theoretical foundations, the following results were obtained:

1) The feasibility of using the NGMSN container matrix as a criterion for selecting it is theoretically justified. Priority is given to the digital image with the lowest NGMSN values;
2) The feasibility of using the SSIM metric for quantifying visual distortions of a container as a result of steganographic transformation is substantiated;
3) The correlation of the selected selection criterion with the structural stability of the digital image matrix and, as a result, the mutual relationship with the visual distortion indicator of the SSIM container is substantiated.

Studies of the practical dependence of the visual quality of the steganographic message on the container's NGMSN showed that using the digital image with the lowest NGMSN among the candidates allows obtaining the best/close to the best SSIM indicator (the maximum deviation from the best value within the experiment was 0.3%), regardless of the steganographic algorithm used and the format of the candidates. Using subjective ranking, it was established that the visual quality of the steganographic message obtained on the basis of selected containers with the lowest NGMSN, compared to random ones, was improved.

REFERENCES

[1] ENISA, ENISA Threat Landscape 2024, European Union Agency for Cybersecurity, 2024, [Online]. Available: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024.

[2] International Telecommunication Union (ITU), Global Cybersecurity Index 2024, 5th ed., Geneva, 2024.

[3] A. Mishra et al., "Recent Advances in Image Steganography and Steganalysis: A Comprehensive Review," Archives of Computational Methods in Engineering, 2024, [Online]. Available: https://doi.org/10.1007/s11831-023-10041-w.

[4] H. Raj and G. Bhaumik, "A comprehensive survey of image steganography: From traditional vision techniques to deep learning paradigms - Trends, challenges, and applications," Computer Science Review, vol. 60, p. 100892, 2026, [Online]. Available: https://doi.org/10.1016/j.cosrev.2026.100892.

[5] A. K. Sahu and G. Swain, "Digital Image Steganography: A Survey on Recent Developments," Journal of King Saudi University - Computer and Information Sciences, vol. 35, 2023, [Online]. Available: https://doi.org/10.1016/j.jksuci.2023.101672.

[6] I. Bobok, A. Kobozieva, and S. Sokalsky, "The Problem of Choosing a Steganographic Container in the Conditions of Attacks against an Embedded Message," Problems Energetics Regionale, no. 4(56), pp. 74-88, 2022, [Online]. Available: https://journal.ie.asm.md/ru/contents/electronni-jurnal-456-2022.

[7] F. Ridzuan et al., "Cover Selection in Steganography: A Systematic Literature Review," Journal of Advanced Research in Applied Sciences and Engineering Technology, vol. 52, no. 2, pp. 107-129, 2025, [Online]. Available: https://doi.org/10.37934/araset.52.2.107129.

[8] I. Bobok et al., "Improving Steganosystem Efficiency as an Integral Part of Ensuring the Routine Operation of Energy Infrastructure Facilities," Problems Energetics Regionale, no. 2(70), pp. 78-93, 2026, [Online]. Available: https://journal.ie.asm.md/ru/contents/electronni-jurnal-270-2026.

[9] M. A. Melnyk, "Steganographic algorithm, resistant to compression," Information Security, no. 2(8), pp. 99-106, 2012.

[10] N. Hamid et al., "Enhancing visual quality of Spatial image steganography using SqueezeNet deep learning network," Multimedia Tools and Applications, vol. 80, no. 28, pp. 36093-36109, 2021, [Online]. Available: https://doi.org/10.1007/s11042-021-11315-y.

[11] H. Sajedi and M. Jamzad, "Evolutionary rule generation for signature-based cover selection steganography," Neural Netw. World, vol. 20, pp. 297-316, 2009, [Online]. Available: https://scholar.google.com/scholar?q=H.+Sajedi%2C+M.+Jamzad%2C+Evolutionary+rule+generation+for+signature-based+cover+selection+steganography%2C+Neural+Netw+World%2C+20+%282009%29+297-316.

[12] V. Hajduk and D. Levický, "Cover Selection Steganography with Intra-Image Scanning," in Proceedings of Radioelektronika, 2018, pp. 1-4, [Online]. Available: https://doi.org/10.1109/RADIOELEK.2018.8376370.

[13] Abed et al., "Efficient cover image selection based on spatial block analysis and DCT embedding," EURASIP Journal on Image and Video Processing, vol. 2019, no. 87, 2019, [Online]. Available: https://doi.org/10.1186/s13640-019-0486-8.

[14] P. D. Shah et al., "Genetic Algorithm based Approach this Select Suitable Cover Image for Image Steganography," in 2020 International Conference for Emerging Technology (INCET), 2020, [Online]. Available: https://doi.org/10.1109/INCET49848.2020.9154032.

[15] Z. Wang, A. C. Bovik, H. R. Sheikh, and E. P. Simoncelli, "Image Quality Assessment: From Error Visibility this Structural Similarity," IEEE

Transactions on Image Processing, vol. 13, no. 4, 2004, [Online]. Available: https://www.cns.nyu.edu/pub/lcv/wang03-preprint.pdf.

[16] S. Nazari and M. S. Moin, "Cover selection steganography via run length matrix and human visual system," pp. 131-138, 2013, doi: 10.7508/jist.2013.02.007.

[17] M. R. D. Molato et al., "Cover Image Selection Technique for Secured LSB-based Image Steganography," in ACAI '18: Proceedings of the 2018 International Conference on Algorithms, Computing and Artificial Intelligence, article no. 17, pp. 1-6, [Online]. Available: https://doi.org/10.1145/3302425.3302456.

[18] M. S. Subhedar, "Cover selection technique for secure transform domain image steganography," Iran Journal of Computer Science, vol. 4, pp. 241-252, 2021, [Online]. Available: https://link.springer.com/article/10.1007/s42044-020-00077-9.

[19] M. M. Brailovskyi et al., Analysis of cyber security of information systems: monograph, Kyiv: FOP Yamchynskyi O. V., 2021.

[20] A. Kobozieva and A. Sokolov, "The Sufficient Condition for Ensuring the Reliability of Perception of the Steganography Message in the Walsh-Hadamard Transform Domain," Problems Energetics Regionale, no. 2(54), 2022, [Online]. Available: https://doi.org/10.52254/1857-0070.2022.2-54.08.

[21] I. Bobok and A. Kobozieva, "Development of the Theoretical Approach this Analyzing the State of Information Protection Systems Based on Matrix Theory," Problems Energetics Regionale, no. 3(63), pp. 29-43, 2024, [Online]. Available: https://journal.ie.asm.md/ru/contents/electronni-jurnal-363-2024.

[22] I. Bobok and A. Kobozieva, "Theoretical Foundations of Digital Content Integrity Expertise," Problems Energetics Regionale, no. 1(65), pp. 105-120, 2025, [Online]. Available: https://journal.ie.asm.md/ru/contents/electronni-jurnal-165-2025.

[23] M. Chen et al., "HLTD-CSA: Cover selection algorithm based on hybrid local texture descriptor for color image steganography," Journal of Visual Communication and Image Representation, vol. 89, pp. 451-464, 2022, [Online]. Available: https://doi.org/10.1016/j.jvcir.2022.103646.

[24] A. A. Kobozeva, I. I. Bobok, and N. I. Kushnirenko, "Method for Distinguishing the Digital Images in Different Formats," Problems Energetics Regionale, no. 1(53), pp. 109-124, 2022, [Online]. Available: https://journal.ie.asm.md/ru/contents/electronni-jurnal-153-2022.

[25] J. Demmel, Applied Numerical Linear Algebra, SIAM, 1997.

[26] R. C. Gonzalez and R. E. Woods, Digital Image Processing, Hoboken: Prentice Hall, 2007.

[27] G. F. Konakhovich, D. O. Progonov, and O. Yu. Puzyrenko, Computer Steganography Processing and Analysis of Multimedia Data, Kyiv, 2018.

[28] N. M. Al-Aidroos et al., "Image Steganography Based on LSB Matching and Image Enlargement," in 2019 First International Conference of Intelligent Computing and Engineering (ICOICE), 2019, [Online]. Available: https://doi.org/10.1109/ICOICE48418.2019.9035172.

[29] G.-H. Chen et al., "Gradient-Based Structural Similarity for Image Quality Assessment," in 2006 International Conference on Image Processing, 2006, [Online]. Available: https://doi.org/10.1109/ICIP.2006.313132.

[30] M. Rouhani et al., "A watermarking method based on optimizing SSIM index by using PSO in DCT domain," in 14 International CSI Conference (CSICC2009), 2009, [Online]. Available: https://doi.org/10.1109/CSICC.2009.5349616.

[31] Y. Hsu and S. Chang, "Detecting image splicing using geometry invariants and camera characteristics consistency," in 2006 IEEE International Conference on Multimedia and Expo, Toronto, pp. 549-552, 2006.

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

[33] NRCS Photo Gallery, [Online]. Available: https://www.nrcs.usda.gov/wps/portal/nrcs/main/national/newsroom/multimedia/.

[34] Q. Peng et al., "AI-Generated Image Dataset," 2025, [Online]. Available: https://doi.org/10.7910/DVN/MGJPBL.