Compression-Resistant Steganographic System as an Effective Software System for Information Protection

Alla Kobozieva[1,*,†], Ivan Bobok[2,†] and Viktor Speranskyy[2,†]

[1] *Odesa National Maritime University, 34 Mechnikova str., 65029 Odesa, Ukraine*
[2] *Odesa Polytechnic National University, 1 Shevchenko av., 65044 Odesa, Ukraine*

Abstract

Information protection today, in the period of rapid development of information technologies and widespread digitalization of the information space, has become one of the main tasks in ensuring the continuous functioning of information systems across all spheres of human activity. One of the most effective modern software systems of information protection is a steganographic system, which must meet several requirements. This work considers digital images as containers, with the main requirements for the steganographic system being resistance to compression attacks while simultaneously ensuring reliable perception of the resulting steganographic message. The problem of satisfying these two requirements for the steganographic systems lacks a definitive solution today and remains extremely relevant, particularly under conditions of compression with low quality factors. The aim of the work is to provide compression stability of the steganographic system, including those with small quality factors, while systematically ensuring the reliability of perception of the formed steganographic message by improving the steganographic method based on the general approach to the analysis of the state of information systems. The aim is achieved by studying the properties of the function of the dependence of the value of the singular number relative error of the image matrix on its number. The most important theoretical result of the work is the substantiation of the existence of the "region of small relative error" for singular numbers, regardless of the specific nature of the perturbation. This region contains singular numbers of the image matrix for which the relative error is comparable to zero. A formal sufficient condition of steganographic algorithm stability against compression attack is obtained. The most significant practical result of the work is the development of an algorithmic realization of the steganographic method improved on the basis of the obtained sufficient condition of stability, the decoding efficiency of which exceeds the existing analogs and is comparable with the efficiency of the prototype. At the same time, the quantitative indicator of reliability of perception of the formed steganographic message, which is the peak "signal-to-noise" ratio, is improved by 13%.

Keywords

steganographic system, compression attack, digital image, singular number

1. Introduction

Information protection today, in the period of rapid development of information technologies and widespread digitalization of information space, becomes one of the main tasks of ensuring the continuous functioning of any information system in private business, public economic sector, military, legal, social, scientific, critical infrastructure of the state [1-3].

A steganographic system is one of the most effective modern software systems for information protection, with its main task being to hide the very fact of a secret message's presence in information content [4]. In the steganographic process, the result of preliminary encoding of secret information – additional hidden information (AHI) – is embedded into an inconspicuous object

Workshop "Intelligent information technologies" UkrProg-IIT`2025 co-located with 15th International Scientific and Practical Programming Conference UkrPROG'2025, May 13-14, 2025, Kyiv, Ukraine
* Corresponding author.
† These authors contributed equally.
alla_kobozeva@ukr.net (A. Kobozieva); onu_metal@ukr.net (I. Bobok); speranskyy@op.edu.ua (V. Speranskyy)
0000-0001-7888-0499 (A. Kobozieva); 0000-0003-4548-0709 (I. Bobok); 0000-0002-8042-1790 (V. Speranskyy)

(container), which is most often represented as a binary sequence $p_1, p_2, ..., p_t$, $p_i \in \{0,1\}$, $i = \overline{1,t}$, which results in a steganographic message. Digital images (DI), which are considered in this paper, are the most widely used containers today.

There are a number of requirements for a modern steganographic system, including [4]:

- ensuring the reliability of perception of the steganographic message (SM): the image-steganographic message should not differ visually from the container;
- resistance to attacks on the embedded message. Such attacks disturb the SM and, consequently, if the steganographic system is vulnerable to disturbances, can lead to distortion or destruction of the embedded AHI; [5]
- resistance to steganographic analysis [6];
- ensuring significant bandwidth of the organized steganographic communication channel [7];
- insignificant computational complexity of the steganographic algorithms used, etc.

The first two requirements are among the most current in practice. In fact, if artifacts appear on SM when AHI is dipped into the container, such a steganographic system is inoperable, because it obviously does not provide the main principle of steganographic data transmission – hiding the fact of secret message presence.

The necessity of providing resistance against attacks on embedded messages — including the imposition of various noises on the steganographic message (SM), filtering, compression, and geometric attacks — is explained by the widespread use of these attacks and the ease and speed with which they can be implemented. This ease of implementation can be attributed to the existence, development, relative ease of use, and high quality of various existing software tools and graphic editors (e.g., Photoshop, Gimp), which do not require significant professional skills or qualifications from the intruder. The most common attack against embedded messages is the compression attack for two main reasons. First, given the substantial volume of digital information that currently circulates in the information space, it is generally stored and transmitted in compressed form. Consequently, the sender seeks to preserve the steganographic messages transmitted through an open channel while avoiding the potential attention they might draw. This preservation, for instance, can be accomplished by employing the JPEG format, which typically results in a loss of data. Achieving this objective necessitates the implementation of a robust steganographic system capable of withstanding compression. Secondly, due to the prevalence of lossy formats for digital information (DI), the consequences of such an attack by an intruder may not be immediately apparent to the intended recipient. For the above reasons, the main attention in this paper is paid to ensuring the steganographic system resistance to compression attack.

2. State of the problem

For any steganographic method that is resistant against compression, it is essential to ensure the reliability of the perception of the generated steganographic message. This is typically quantified using difference indices in steganography, such as the peak signal-to-noise ratio (PSNR) [8]. Generally, higher PSNR values indicate a lower probability of SM perception reliability violation after AHI implementation. In practice, steganographic messages with PSNR > 40 dB are considered to be of good visual quality [8]. However, it should be noted that not all steganographic methods are equally effective in ensuring this condition. In particular, there are methods that do not systematically provide this condition, especially in the context of compression robustness with a small quality factor. This occurs because ensuring these two requirements separately involves contradictory actions: utilizing the low-frequency component of the container during AHI immersion to achieve SM compression resistance, while using the high-frequency component to ensure the absence of artifacts from steganographic transformation.

In [9], a JPEG-compression-resistant steganographic algorithm was developed. This algorithm is based on changing the values of the maximum wavelet coefficients of the blocks of the container matrix. However, this algorithm is designed for the implementation of digital watermarks, a domain in which the requirement of reliability of perception is not as critical as in the organization of covert communication. A significant probability of artifacts on SM remains, which limits its possibility for use in the organization of covert communication channels. Nevertheless, its resilience to compression attacks with small QFs, as well as the methods outlined in [10,11], renders it a compelling subject for a comparative analysis of the effectiveness of the algorithm developed in this paper.

In [12], the use of visually significant DC factors of subimages of the container image in the steganographic transformation process was proposed to improve the robustness of the steganographic message against compression. Each of the four resulting subimages V_1, V_2, V_3, V_4 is the result of its scaling. The reliability of SM perception in the proposed algorithm is ensured by the authors due to $V_i \approx V_j$ for $i \neq j$, which can be explained by the correlation of brightness values of nearby pixels. However, the results of the computational experiment presented in [12], where an insignificant number of DIs were involved, do not provide an objective picture of the reliability of SM perception, which, based on the logic of the AHI implementation process, can be violated in sub-blocks containing pronounced image contours, which is not noted by the authors.

In [13], the authors propose a compression-resistant steganographic algorithm predicated on a fractal model operating within the discrete wavelet transform domain. The proposed scheme involves the embedding of a binary image, regarded as a digital watermark with fractal parameters, within the wavelet domain of the container. The fractal compression technique is then employed to precode the digital watermark. The efficacy of this approach is evident in its ability to achieve complete error-free decoding at QF ≥ 60, while maintaining efficiency in the range of 30 ≤ QF <60.

In [14], a compression-resistant steganographic method is proposed. This method consists of two main processes: determining the immersion point in each block of the DI container with the best possibility of resisting high ratio compression; and immersing the DI in discrete cosine transform factors. To determine the immersion point, the DI container is subjected to JPEG compression with quality ratios ranging from 1 to 100, which is evidently a computationally intensive process. For each block, the number of zeros in the compression of each element is computed. The index is 1 if the corresponding DDC factor is 0. This process is repeated for each quality factor from 1 to 100. The index for the block, the minimum value of which will determine the dipping point, is determined by the sum of indicators of the number of zeros in compression for all coordinates of the block and for all quality factors. This point corresponds to the low-frequency factors, which calls into question the reliability of perception of the formed SM.

In [15], a steganographic algorithm robust to JPEG compression is proposed with quality factor values often used in practice: QF ∈ {65, 75, 85}. Compression attacks of significant strength are not considered at all, as in [16-18].

In [16], the challenge of providing compression-resistant steganography is addressed due to the pervasive use of social media platforms for image posting and the significant potential of leveraging the communication channels offered by various social networks for covert communication. The authors observe that the majority of existing steganographic schemes are not designed to store SMs in the JPEG format. They propose a covert communication method that is robust to such channels. The DI adjustment in the AHI implementation is executed in a manner that ensures the compressed version of the DI corresponds to the SM. This approach enables the authors to ensure absolute accuracy in decoding AHI, albeit only at QF ≥ 75, as the operation of the proposed scheme obviously loses efficiency at lower values of QF.

In [18], a steganographic algorithm for a DI container is proposed. To ensure its resistance to compression attacks, the container elements are selected using the sign of the discrete cosine transform coefficients. This ensures that the sign does not change as a result of DI compression. The incorporation of AHI into the container results in only a marginal distortion. The authors

position the proposed algorithm as one that can effectively resist attacks common in social networks such as Facebook, Twitter, and WeChat.

Consequently, the systematic assurance of perceptual reliability for steganographic methods resistant against compression attacks is a relevant task.

One of the most resistant against compression attacks, including compression with small quality factors, is the algorithm proposed in [19]. The theoretical basis of this algorithm is the general approach to analyzing the state of information systems (GAASIS) based on perturbation theory and matrix analysis. AHI immersion occurs within the singular value decomposition region of 8×8-blocks, into which the container matrix is pre-partitioned. The PSNR value fluctuates within the range of 33-37 dB during the steganographic transformation of all blocks in the container, corresponding to a bandwidth of 1/64 bits/pixel for the hidden communication channel. This necessitates the urgent improvement of AHI, with the objective of enhancing the reliability of SM perception by increasing the PSNR value. Theoretical results obtained by the authors earlier in [20,21] provide opportunities for such improvement.

The aim of this work is to provide compression stability for the steganographic systems, even with small quality factors, while systematically ensuring reliable perception of the formed steganographic message through improvements of the steganographic method proposed in [19].

3. Methods, results and discussion

Let F be an $n\times n$-matrix of the DI container. According to GAASIS, we can represent the result of any steganographic transformation as a perturbation of the container matrix: $\overline{F} = F + \Delta F$, where is $\overline{F}, \Delta F$ the $n\times n$-matrix of the steganographic message and disturbance, which is a formal representation of the change in the container as a result of the steganographic transform, respectively. This representation will occur regardless of which region of the container (spatial, frequency or another transform area) it occurs in. Let

$$F = U\Sigma V^T \tag{1}$$

is the normal singular expansion F [22], determined unambiguously, where U, V are orthogonal matrices whose columns $u_i, v_i, i = \overline{1,n}$ are left and right singular vectors (SV), respectively, while the left SVs are lexicographically positive, $\Sigma = diag\left(\sigma_1(F),\ldots,\sigma_n(F)\right)$, $\sigma_1(F) \geq \ldots \geq \sigma_n(F) \geq 0$ are the singular numbers (SN) F, $\left(\sigma_i, u_i, v_i\right)$ are singular triples F, $i = \overline{1,n}$. According to GAASIS, both the steganographic transformation and the effects of additional disturbances on the SM can be represented as a set of singular number (SN) and singular vector (SV) perturbations of the container matrix, regardless of the specific steganographic method and disturbance used.

In [20,21], GAASIS was further developed, during which it was established that, starting from a certain number i_0, the function $y(\sigma_i, \Delta F) = \Delta\sigma_i$ of the dependence of the perturbation $\Delta\sigma_i$ of the singular number $\sigma_i(F)$ of the DI matrix on its number as a result of the disturbance ΔF, where $\Delta\sigma_i = \left|\sigma_i(F) - \sigma_i(F + \Delta F)\right|$, becomes monotonically decreasing (in terms of trend), defining the stabilization region of SN for the original DI. This property does not hold for non-original digital images. The established properties of the perturbations of the DI matrix SN, specifying their sensitivity to active attacks, provide an opportunity to improve various information protection systems, including the steganographic systems.

The theoretical results obtained in [20, 21] can be effectively used to improve steganographic methods in which AHI immersion occurs additively. However, it is imperative to acknowledge that ensuring the feasibility of AHI decoding under attacks targeting the embedded message necessitates the maintenance of a disturbance magnitude that exceeds the disturbance-attack magnitude on the SM. In the absence of this condition, the integrity of the AHI may be irreparably compromised. However, it should be noted that the steganographic transformation is often based

on relative changes in the formal parameters that define the container [19]. To enhance the efficacy of these steganographic methods, further investigation is necessary to elucidate the nature of relative SN errors:

$$\delta(\sigma_i) = \frac{\Delta\sigma_i}{\sigma_i(F+\Delta F)} \cdot 100\% \quad (2)$$

arising as a result of disturbance. It is necessary to identify SNs whose relative changes will be minimal/small. Although all SNs are well-conditioned or relatively insensitive to disturbance, according to the relationship [23]:

$$\max_i \left|\sigma_i(F) - \sigma_i(F+\Delta F)\right| \le \|\Delta F\|_2 \quad (3)$$

where $\|\cdot\|_2$ is the norm of the spectral matrix, there will still be some among them for which the degree of sensitivity will be greater/less.

When applying disturbance to a digital image, let us consider the function representing the dependence of the relative error of $\delta(\sigma_i)$ SN on its number: $z(\sigma_i, \Delta F) = \delta(\sigma_i)$. A visual representation of all the properties of the function is its plot. For the plot of $z(\sigma_i, \Delta F)$ in the left part of the singular spectrum, there will necessarily be a "section" of SN that has a relative error comparable to zero. This will be the case regardless of which disturbance is used (Fig.1). Indeed, for the original DI, the character of SN decrease has a pronounced specifics [24]: at first, the decrease occurs at a significant rate (for the largest SNs), and then the rate of this decrease begins to decrease, tending to zero at ($i \to n$ Fig. 2(a)), making SNs comparable in value to each other and to zero at a certain moment. As shown in [20,21], for the group of the largest SNs, their absolute errors are comparable to the average values of such errors across the entire singular spectrum. And for the largest SNs, their errors may be comparable to the minimum ones (Fig. 1). Given the good causality of SN (3), the change in their values will be adequate to the disturbance force ΔF quantified by $\|\Delta F\|_2$, ensuring that the largest SN on the left side of the spectrum will remain the largest after perturbation, and the behavior of the singular spectrum of the perturbed DI will remain qualitatively similar to that of the original (Fig. 2 (b)). Such behavior $\Delta\sigma_i$ depending on the SN i number leads to the fact that, regardless of the nature of disturbance, there is a certain set of SNs for DI on the left side of the spectrum (maximum SNs), for which the relative error will be comparable to zero. Such a set will be referred to as the area of small relative error (ASRE). The container modification region (AMC) does not contain those SNs that are included in the stabilization region, preceding it (Fig. 1). This is expected since the SN stabilization region of any original DI begins with the i numbers for which the value $\Delta\sigma_i$ is the maximum or close to the maximum among all absolute errors in the singular spectrum [20,21].

It should be noted that there is no systematic correspondence in the nature of the behavior $y(\sigma_i, \Delta F) = \Delta\sigma_i$ of the functions and $z(\sigma_i, \Delta F) = \delta(\sigma_i)$, which would not depend on the specifics of disturbance. Indeed, it is impossible to determine the nature of monotonicity $z(\sigma_i, \Delta F)$ (classical or in the sense of a trend) in any part of the singular spectrum: conditional monotonicity can be broken both in the left (even in AMC) and in the right parts of the singular spectrum (Fig. 1(b)) and across the entire spectrum (Fig. 1(c)). The nature of monotonicity (trend) $z(\sigma_i, \Delta F)$ can change for the same region of the singular spectrum depending on the disturbance (comparison, for example, of Fig.1(b) and Fig.1(c) in the interval $400 \le i \le 600$). This is expected, since the value of (2) of the relative error $\delta(\sigma_i)$ depends on two parameters: the absolute error and the perturbed SN value itself, each of which is determined for the already perturbed DI. $z(\sigma_i, \Delta F)$ At the present stage of the study, in general, it is not possible to determine in the $z(\sigma_i, \Delta F)$ area corresponding to the stabilization area $y(\sigma_i, \Delta F)$.

Singular triples $\left(\sigma_i, u_i, v_i\right)$ that correspond to the smallest SN F play a significant role in solving the problem of ensuring the reliability of SM perception, since they correspond mainly to the high-frequency component of DI. However, as can be seen from Fig. 1, the behavior of their relative errors is very different for different disturbances: the relative error can take very large values (Fig. 1 (a)), can be comparable to zero (Fig. 1(b)), or occupy an intermediate one value (Fig. 1(c)). This is due to the fact that the values of the smallest SNs themselves are comparable to each other and comparable to 0, as already mentioned above, which leads to a small separation of these SNs, determined according to the formula [23]: $svdgap\left(i,F\right)=\min\limits_{i\neq j}\left|\sigma_i-\sigma_j\right|$ for SNs σ_i. The consequence of this, taking into account (3), is a very slight change in these SNs: after disturbance, the smallest SNs of the spectrum will remain comparable to zero. In this case, their absolute error will also be comparable to zero $\Delta\sigma_i$. Thus, when calculating $\delta\left(\sigma_i\right)$ for such SNs in accordance with (2), in the general case, we come to an uncertainty of the type $\frac{0}{0}$, the disclosure of which, as is known, can give different variants, which is observed in practice (Fig. 1).

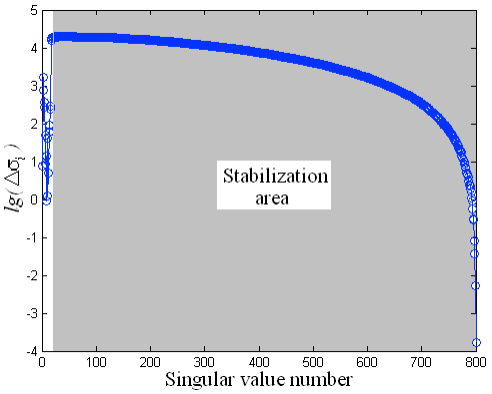
As a result of the conducted studies on the properties of the function $z\left(\sigma_i,\Delta F\right)$, it can be stated that when applying perturbations (attacks against the embedded message) in the DI, the SNs of ASRE will suffer the least in terms of relative error. When considering the embedded AHI in the container according to GAASIS as a set of perturbations of the SN of its matrix, taking into account the obtained results, it becomes obvious that the part of the AHI, whose embedding leads to perturbation of the SN from ASRE, will be least affected by the attack against the embedded message. If the result of the steganographic transformation is only these SN, the resulting SM will be resistant against disturbance. Consequently, the following conclusions can be drawn:

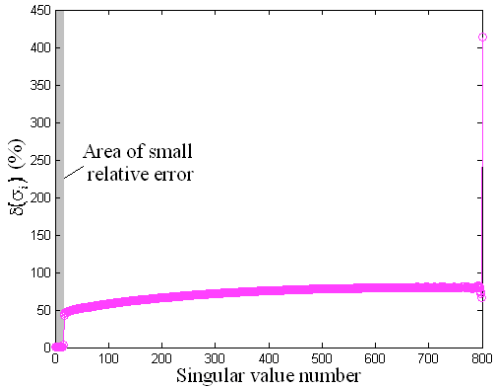
A sufficient condition for the robustness of SM to attacks against the embedded message. In order to ensure the stability of the steganographic transformation against attacks targeting the embedded message, particularly against the compression attack, it is sufficient to implement the AHI so that its formal result is the set of perturbations of SNs from ASRE.

Most of the current (existing and developed) steganographic methods are block methods [4,5,19]. They embedd/decode AHI using blocks of the container matrix/SM obtained as a result of its standard partitioning [25]. There are several reasons for this, including: the possibility of better ensuring the SM's compression stability; providing relatively low computational complexity (for $n\times n$-matrices DI, the computational complexity of any block algorithm will be determined by the number of blocks received, i.e. the number of $O\left(n^2\right)$ operations); the ability to naturally parallelize both the AHI implementation and extraction process, resulting in a reduction in DI processing time, which is especially important due to the increasing use of streaming containers (digital video) in real time. In this article, the first of these options is the most significant in order to make a choice in favor of block processing of a container in steganographic transformation. Block organization is inherent in the most widespread compression algorithms for DI today – JPEG and JPEG2000. It is obvious that taking into account the peculiarities of the DI block processing process during compression will make it possible to better protect the uploaded information from the consequences of compression when carrying out the block injection of AHI with the same partitioning of the container matrix as used by the JPEG and JPEG2000 algorithms.

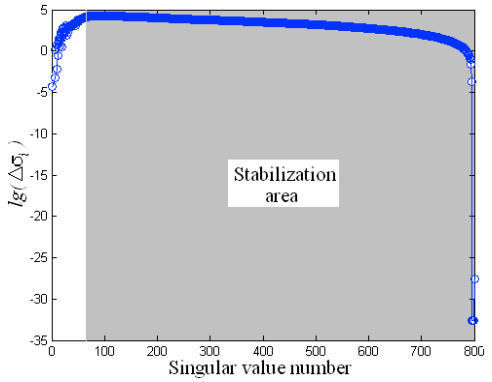
The presence of ASRE for SN has been established for DI matrices in general. Consider the DI blocks resulting from its standard splitting. The justification for the existence of ASRE for the SN of the original DI was in no way limited by its size, so it will obviously take place for blocks as well, although the value of ASRE in terms of the number of SNs included in it will be smaller, which is confirmed by a computational experiment, the typical results of which are demonstrated in Fig. 3 for a specific DI under the conditions of a compression attack – saving SM to JPEG format (QF = 75). It should be noted that for the smallest SNs, the relative error will always be large. This is due to the following reason. In DI compression, the minimum SN of the blocks, for which

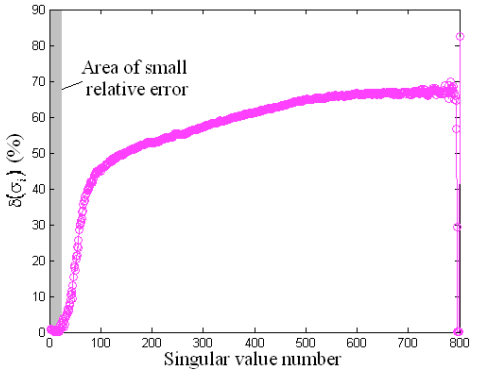
singular triples correspond mainly to the high-frequency component of the blocks, are zeroed out, becoming comparable to zero as a result of DI recovery after compression [26].



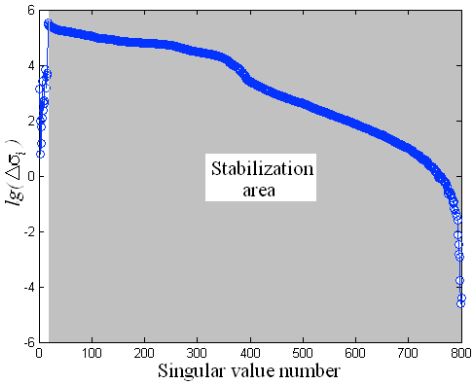


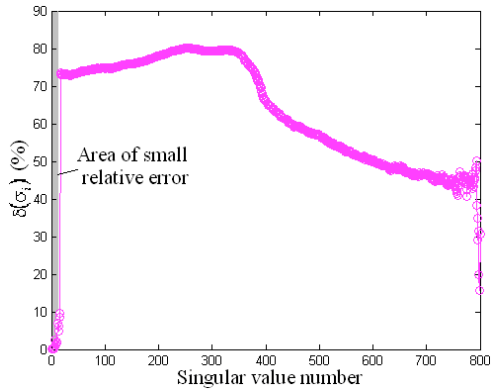
a



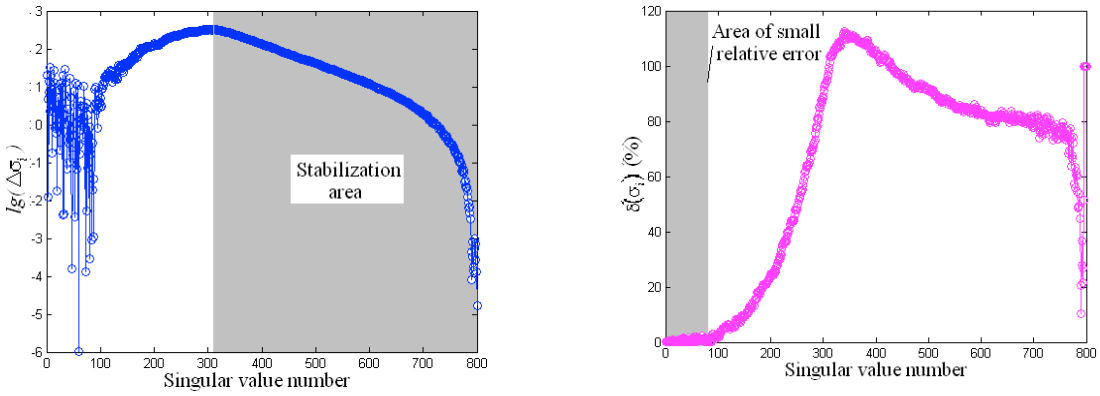


b



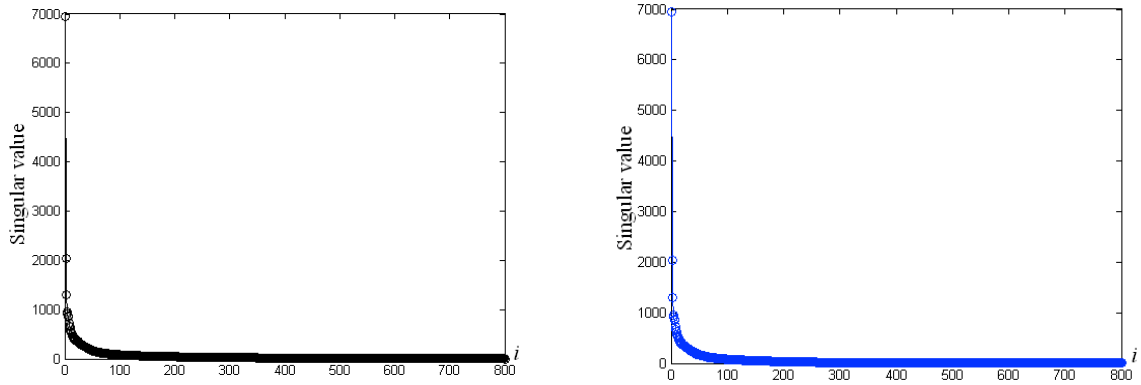


c



d

Figure 1: Dependence plots of the absolute and relative errors of SN on their number for specific DI at different disturbances: a – superposition of Gaussian noise with zero payback and d = 0.0001; b – superposition of multiplicative noise with a variance of d = 0.001; c – "salt & pepper" noise overlay with d = 0.001; d – compression with quality factor QF = 75



a b

Figure 2: Typical type of dependence of SN values on their number for: a – original DI; b – perturbed DI

The presence of ASRE, which contains not only σ_1, at any of the considered block sizes, gives grounds for improving algorithm that is one of the most resistant against the compression attack today [19]. This algorithm, being a block algorithm, is based on the change σ_1 in the block when the AHI bit is immersed in such a way as to achieve a certain relative ratio between the values of σ_1, σ_2, while the choice of σ_1 for adjustment is the key point of the algorithm and is due to the fact that the author [19] does not see alternatives among the set of SN blocks to ensure resistance to a compression attack. But such a method of steganographic transformation, as noted above, is not guaranteed against violating the reliability of perception of the corresponding steganographic message, since the singular triplet $\left(\sigma_1, u_1, v_1\right)$ carries information mainly about the low-frequency component (block) of the image, changes in which are very likely to lead to visible artifacts on the steganographic message. An illustration of this is given in Fig. 4, where one of the regions of the perturbed DI with the artifacts that have arisen is limited by a red line for clarity. A relative change of only 10% in the maximum SN resulted in noticeable visual changes in the image, especially in areas with small differences in brightness values (background).

As can be seen from the results of the presented studies, not only σ_1, but also several SN blocks from ASRE, following after σ_1, have significant resistance to perturbing influences as quantified by the relative error, σ_1 and whose stability will be comparable to the stability σ_1. Moreover,

during the computational experiment, where the DI was used in its entirety, there were non-isolated cases when the relative error of the first SN was not was the smallest (Fig. 1(b)). In view of all of the above, when modifying the method proposed in [19], it is proposed to use not the pair σ_1, σ_2, but the pair σ_m, σ_{m+1} from ASRE, where $m > 1$.

The main steps of the proposed steganographic method for a DI container with a matrix F and an AHI immersed in it $p_1, p_2, ..., p_t$, $p_i \in \{0,1\}$, $i = \overline{1,t}$ which is a modification [19], are as follows.

Implementation of AHI.

Step 1. The matrix F of the DI container is divided in a standard way into non-overlapping $l \times l$-blocks, the arbitrary of which is denoted by B.

Step 2 (*AHI Implementation*).

In each successive block B of the matrix F used to implement AHI, defined according to the secret key, 1 bit p_i of AHI is immersed:

2.1. Determine the SN of the block B, $\sigma_1 \geq \sigma_2 \geq ... \geq \sigma_l \geq 0$;

2.2. Select σ_m, σ_{m+1}, $m > 1$, from ASRE.

2.3. Embedding AHI is carried out by mutual adjustment σ_m, σ_{m+1}. Result is: $\overline{\sigma}_m, \overline{\sigma}_{m+1}$, since $p_i \in \{0,1\}$ – the number of different adjustment options σ_m, σ_{m+1} corresponds to the cardinality of the set $\{0,1\}$, i.e. is equal to two.

2.4. The block of B steganographic message corresponding to the block $\overline{B}$ is formed by replacing SN σ_m, σ_{m+1} with $\overline{\sigma}_m, \overline{\sigma}_{m+1}$.

Step 3 (*Formation of a steganographic message*).

The matrix $\overline{F}$ of steganographic message is constructed by replacing each block B of the container involved in the AHI immersion with a corresponding block $\overline{B}$. The process is complete.

Under the conditions of a supposed compression attack on a steganographic message, its matrix will be perturbed and further denoted $\overline{\overline{F}}$: $\overline{F} \neq \overline{\overline{F}}$.

AHI decoding.

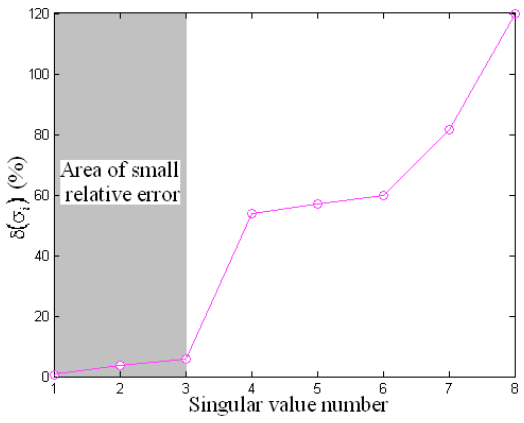
Step 1. The matrix $\overline{\overline{F}}$ of the perturbed SM is divided into blocks $\overline{\overline{B}}$ of size $l \times l$ in a standard way.

Step 2 (*AHI decoding*).

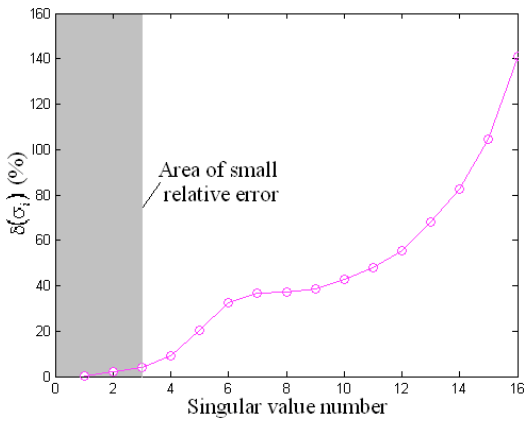
From each block $\overline{\overline{B}}$ of the matrix $\overline{\overline{F}}$ containing the AHI, determined according to the secret key, 1 bit $\overline{\overline{p}}_i$ of AHI is extracted:

2.1. Determine the SN of the block $\overline{\overline{B}}$, $\overline{\overline{\sigma}}_1 \geq \overline{\overline{\sigma}}_2 \geq ... \geq \overline{\overline{\sigma}}_l \geq 0$;

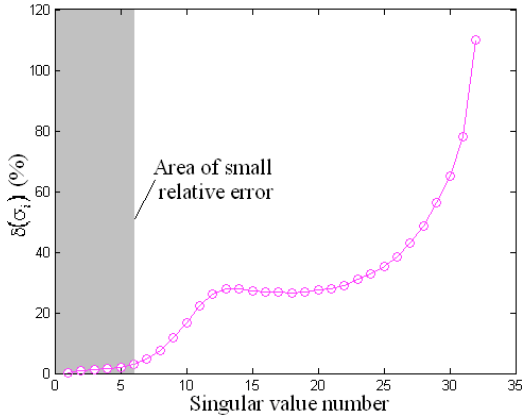
2.2. Determine the ratio between the values of $\overline{\overline{\sigma}}_m, \overline{\overline{\sigma}}_{m+1}$, according to which to extract $\overline{\overline{p}}_i$.



a



b



c

Figure 3: Dependence of the $l \times l$-block mean values of a particular DI $\delta(\sigma_i)$ on the SN number under the conditions of a compression attack (JPEG, QF = 75): a – l = 8; b – l = 16; c – l = 32

a b

Figure 4: Illustration of the effects of changing the maximum SN for the visual perception of DI: a – original DI; b – perturbed DI

The formal representation of the DI container here is a single matrix F. This fully corresponds to the DI in grayscale, but in no way limits the scope of the method to only such images. If a color image is considered as a container, then F is the matrix of one of the three color components, most often blue (RGB scheme), or the luminance matrix Y in the YUV scheme. Note that for a colored DI, stored in the RGB scheme, there is no fundamental limit to the number of color components used to implement AHI in them using the proposed method.

In the algorithmic implementation of the proposed method, the following parameter values were used: l =8 (since the most common algorithm for lossy DI compression today is JPEG, which works with individual DI blocks of size 8×8, it is better to take into account all the features of such compression that allows this particular block size); $m = 2$ (σ_2, σ_3 fall into ASRE at any of the considered block sizes).

In the steps 2.1 of the AHI embedding and extraction process, the SN of the block was computed using the singular value decomposition (1) of its matrix. However, the "classical" singular value decomposition [23] can also be employed in this context. This approach is generally ambiguous due to its lack of the lexicographic positivity requirement on the left SVs, a feature that distinguishes it from the normal singular value decomposition [22]. It should be noted that singular values are not a factor in this particular algorithm.

The steps 2.3 for embedding and 2.2 for extracting the AHI bit were implemented as follows. For embedding $p_i \in \{0,1\}$ into block B by adjusting the values, σ_2, σ_3 two variants of the remainder r

were provided when divided the values $[\sigma_2 - \sigma_3]$ by $\overline{K}$, where $[\cdot]$ the integer part of the argument, $\overline{K}$ is an analogue of the threshold value of the SN perturbation variation in [19], determined experimentally taking into account the requirement to ensure the reliability of SM perception, $\overline{K} = 150, [\sigma_2 - \sigma_3] \equiv r \left(\mathrm{mod}\, \overline{K} \right)$:

$$r = \begin{cases} \overline{K}/4, \text{ if } p_i = 0, \\ 3\overline{K}/4, \text{ if } p_i = 1. \end{cases}$$

For extraction of $\overline{\overline{p}}_i$ the two different options for the remainder $\overline{\overline{r}}$ of division by $\overline{K}$ the values $[\sigma_2 - \sigma_3]$ provide $\overline{\overline{p}}_i \in \{0,1\}$:

$$\overline{\overline{p}}_i = \begin{cases} 0, \text{ if } \overline{\overline{r}} < K/2, \\ 1, \text{ if } \overline{\overline{r}} \geq K/2. \end{cases}$$

To assess the effectiveness of the proposed algorithm, the computational experiment was carried out. The following containers were used: 500 DI from the database [27], 500 DI from the database [28], 100 DI obtained by non-professional video cameras. The test results are presented in Table 1, where compression-resistant steganographic methods were used for comparative analysis: S_1 [29], S_2 [10], S_3 [11], S_4 [9], S_5 [30], S_6 [31], S_7 [32], S_8 [12], S_9 [13], S_{10} [15], S_{11} [16], S_{12} TCM [17], S_{13} DMCSS [18], S_{14} [19], which is the prototype for the one proposed in this work.

The effectiveness of steganographic methods in the work is estimated in a standard way: using the correlation coefficient NC for AHI: $NC = \frac{1}{t} \cdot \sum_{i=1}^{t} p_i' \times \overline{\overline{p}}_i'$, where $p_1, p_2, ..., p_t$; $\overline{\overline{p}}_1, \overline{\overline{p}}_2, ..., \overline{\overline{p}}_t$, $p_i, \overline{\overline{p}}_i \in \{0,1\}$, $i = \overline{1,t}$, is respectively embedded and decoded AHI from a steganographic message; $p_i' = 1, \overline{\overline{p}}_i' = 1$, if $p_i = 1, \overline{\overline{p}}_i = 1$, and $p_i' = -1, \overline{\overline{p}}_i' = -1$ if $p_i = 0, \overline{\overline{p}}_i = 0$, i.e. $p_i' \times \overline{\overline{p}}_i' \in \{1,-1\}$.

Table 1

Value NC for different steganographic algorithms in a compression attack with the different values of the quality factors QF

Method	QF												
	10	20	25	30	40	50	60	65	70	75	80	85	90
S_1				0.15		0.28			0.57				1
S_2	0.15	0.34		0.52		0.52			0.63				0.8
S_3	0.17	0.61		0.59		0.89			0.97				1
S_4	0.34	0.67		0.82		0.96			0.97				0.99
S_5			0.63		0.8	0.89							
S_6			0.8		0.83	0.92							
S_7		0.85				0.87					0.9		
S_8		0.84				0.93					0.97		

S_9	0.42	0.56		0.8	0.95	0.95	1		1		1		1
S_{10}								0.98		0.99		1	
S_{11}										1		1	
S_{12}										0.92		0.92	
S_{13}										1		1	
S_{14}	0.87	0.93	0.94	0.95	0.96	0.98	0.98		0.98	0.98	0.98		0.98
Proposed	*0.84*	*0.91*	*0.92*	*0.93*	*0.95*	*0.96*	*0.96*	*0.96*	*0.96*	*0.97*	*0.97*	*0.97*	*0.97*

As can be seen from the results obtained, the algorithmic implementation of the proposed method is slightly inferior in efficiency to its prototype [19], however, unlike it, the average value of PSNR = 41.3 dB, which in comparison with the best PSNR = 37 dB in the prototype gives an improvement of 13%. At the same time, the efficiency of the proposed algorithm significantly exceeds the efficiency of other analogues in the conditions of a low-QF compression attack: for example, for QF = 10, the best of the analogues, excluding the prototype, is S_9, has an efficiency half as much. It should be noted that most modern methods, which are positioned as resistant against a compression attack, are not able to work effectively in conditions of attack with insignificant quality factors, as can be seen from Table 1. Although such attacks in practice are not only possible, but are often used since compression of DI with even a small factor may not lead to appearing of visible artifacts (Figure 5), but it can destroy the built-in AHI.

a b c

Figure 5: Visualization of the results of saving DI to JPEG format with low quality factors QF: a – original DI in lossless format (TIFF); b – DI after compression with QF = 20, c – DI after compression with QF = 10

4. Conclusions

The paper addresses a significant scientific and practical task of ensuring steganographic system stability against compression attacks while systematically ensuring reliable perception of the resulting steganographic message.

While solving the problem, the detailed study of the function representing the dependence of the relative error of singular numbers in the digital image matrix on their respective index numbers resulting from perturbing influences was conducted. The study encompassed the following:

- the existence of an Area of Small Relative Error (ASRE) for singular numbers has been established and substantiated, regardless of the specific disturbances applied. ASRE contains singular numbers of image matrices for which the relative error is negligible;
- a formal sufficient condition for the stability of steganographic algorithms against compression attacks is obtained.

The steganographic method proposed in [19] is improved on the basis of the obtained theoretical results. The algorithmic implementation of this enhancement, aimed at improving AHI decoding efficiency under compression attacks, demonstrates performance comparable to the prototype while significantly surpassing other analogous methods with QF < 50, most of which were not designed to function effectively under attacks with low quality factors. At the same time, the developed algorithm improves the quantitative index of reliability of perception of the formed steganographic message by 13% in comparison with [19]: PSNR = 41.3 dB.

Thus, the developed algorithmic implementation of the improved steganographic method provides steganographic messages with perception reliability quantified by PSNR > 40 dB. Concurrently, the high efficiency of AHI decoding under compression attack conditions, including those with insignificant quality factors, is maintained. This ensures a high probability that no artifacts appear after AHI embedding.

Declaration on Generative AI

The authors have not employed any Generative AI tools.

References

[1] S. Saeed et al., Digital transformation in energy sector: Cybersecurity challenges and implications, Information 15 (2024) 764. URL: https://doi.org/10.3390/info15120764

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

[3] Z. Xu et al., Optimizing data privacy and security measures for critical infrastructures via IoT based ADP2S technique, Scientific Reports 15 (2015) 9703. URL: https://doi.org/10.1038/s41598-025-94824-2

[4] D. Srinivasan, K. Manojkumar, A. Syed, H. Nutakki, A comprehensive review on advancements and applications of steganography, 2024. URL: https://doi.org/10.13140/RG.2.2.13568.44807

[5] A.A. Kobozeva, A.V. Sokolov, Robust steganographic method with code-controlled information embedding, Problemele Energeticii Regionale 4 (2021) 115–130. URL: https://doi.org/10.52254/1857-0070.2021.4-52.11

[6] A.A. Kobozeva, I.I. Bobok, L.E. Batiene, Steganoanalytical method based on the analysis of singular values of digital image matrix blocks, Problemele Energeticii Regionale 3 (2018) 156–168. URL: https://dx.doi.org/10.5281/zenodo.2222384

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

[8] A.S. Ansari, M.S. Mohammadi, M.T. Parvez, A comparative study of recent steganography techniques for multiple image formats, International Journal of Computer Network and Information Security 11 (2019) 11–25. URL: https://doi.org/10.5815/ijcnis.2019.01.02

[9] W.-H. Lin et al., A blind watermarking method using maximum wavelet coefficient quantization, Expert Systems with Applications 36 (2009) 11509–11516. URL: https://doi.org/10.1016/j.eswa.2009.03.060

[10] E. Li, H. Liang, X. Niu, Blind image watermarking scheme based on wavelet tree quantization robust to geometric attacks, in Proceedings of the 2006 6th World Congress on Intelligent Control and Automation, Dalian, China, 2006, pp. 10256–10260. doi: 10.1109/WCICA.2006.1714009.
[11] B.K. Lien, W.H. Lin, A watermarking method based on maximum distance wavelet tree quantization, in: Proceedings of the 19th Conference on Computer Vision, Graphics and Image Processing, 2006, pp. 269–276.
[12] I. Nasir, Y. Weng, J. Jiang, S. Ipson, Subsampling-based image watermarking in compressed DCT domain, in: Proceedings of 10th IASTED International Conference on Signal and Image Processing (SIP 2008), Kailua-Kona, Hawaii, USA, 2008, pp. 339–344.
[13] S. Shahraeini, M. Yaghoobi, A robust digital image watermarking approach against JPEG compression attack on hybrid fractal-wavelet, in: Proceedings of the International Conference on Computer Communication and Management (ICCCM '11), Wuhan, China, 2011, pp. 616–622.
[14] C.-H. Fan, H.-Y. Huang, W.-H. Hsu, A robust watermarking technique resistant JPEG compression, Journal of Information Science and Engineering 27 (2011) 163–180.
[15] Y. Wu, W. Shang, J. Chen, J., Anti-JPEG compression steganography based on the high tense region locating method, Computers, Materials & Continua 59 (2019) 199–214. URL: https://doi.org/10.32604/cmc.2019.05194
[16] J. Tao, S. Li, X. Zhang, Z. Wang, Towards robust image steganography, IEEE Transactions on Circuits and Systems for Video Technology 29 (2019) 594–600. URL: https://doi.org/10.1109/TCSVT.2018.2881118
[17] Z. Zhao, Q. Guan, H. Zhang, X. Zhao, Improving the robustness of adaptive steganographic algorithms based on transport channel matching, IEEE Transactions on Information Forensics and Security 14 (2019) 1843–1856. URL: https://doi.org/10.1109/TIFS.2018.2885438.
[18] S. Wang, N. Zheng, M. Xu, A compression resistant steganography based on differential Manchester code, Symmetry 13 (2021) 165. URL: https://doi.org/10.3390/sym13020165
[19] M.A. Melnik, Compression-resistant steganography algorithm, Information Security 2 (2012) 99–106.
[20] I.I. Bobok, A.A. Kobozeva, Development of the theoretical approach based on matrix theory for analyzing the state of information security systems, Problemele Energeticii Regionale 3 (2024) 29–43. URL: https://doi.org/10.52254/1857-0070.2024.3-63.03
[21] I.I. Bobok, A.A. Kobozieva, Theoretical foundations of digital content integrity expertise, Problemele Energeticii Regionale 1 (2025) 105–120. URL: https://doi.org/10.52254/1857-0070.2025.1-65.08
[22] C. Bergman, J. Davidson, Unitary embedding for data hiding with the SVD, 2005. URL: https://dr.lib.iastate.edu/handle/20.500.12876/54635
[23] J.W. Demmel, Applied Numerical Linear Algebra, SIAM, 1997.
[24] I. Bobok, A. Kobozieva, S. Sokalsky, The problem of choosing a steganographic container in conditions of attacks against an embedded message, Problemele Energeticii Regionale 4 (2022) 74–88. URL: https://doi.org/10.52254/1857-0070.2022.4-56.07
[25] R. Gonzalez, R. Woods, Digital Image Processing (4th Ed), Pearson, 2018.
[26] A.A. Kobozeva, I.I. Bobok, N.I. Kushnirenko, Method for distinguishing the digital images in different formats, Problemele Energeticii Regionale 1 (2022) 109–124. URL: https://doi.org/10.52254/1857-0070.2022.1-53.09
[27] T. Gloe, R. Böhme, The 'Dresden Image Database' for benchmarking digital image forensics, in: Proceedings of the 2010 ACM Symposium on Applied Computing (SAC '10). Association for Computing Machinery, New York, USA, 2010, pp. 1584–1590. doi: 10.1145/1774088.1774427
[28] NRCS Photo Gallery. United States Department of Agriculture. Washington, USA. URL: https://www.nrcs.usda.gov

[29] S.-H. Wang, Y.-P. Lin, Wavelet tree quantization for copyright protection watermarking, IEEE Transactions on Image Processing 13 (2004) 154–165. URL: http://dx.doi.org/10.1109/TIP.2004.823822.

[30] C. Li, H. Song, A novel watermarking scheme for image authentication in DWT domain, in: Proceedings of the 2009 3rd International Conference on Anti-counterfeiting, Security, and Identification in Communication, Hong Kong, China, 2009, pp. 160–162, doi: 10.1109/ICASID.2009.5276922.

[31] P. Liu, Z. Ding, A blind image watermarking scheme based on wavelet tree quantization, in: Proceedings of the 2009 Second International Symposium on Electronic Commerce and Security, Nanchang, China, 2009, pp. 218–222. doi: 10.1109/ISECS.2009.219.

[32] W. Lu, H. Lu, F.-L. Chung, Robust digital image watermarking based on subsampling, Applied Mathematics and Computation 181 (2006) 886–893. URL: https://doi.org/10.1016/j.amc.2006.02.012