УДК 004.056.55
DOI: 10.31673/2409-7292.2025.030518

Honcharov M. O., Nariezhnii O. P., Malakhov S.

ANALYSIS OF PREREQUISITES FOR ENSURING RESOURCE CONSENSUS WHEN PERFORMING STEGANOGRAPHIC DATA INSERTION PROCEDURES

In the conditions of sustainable growth in the complexity and multi-vector nature of modern cyber threats, digital steganography continues to play an important role in ensuring data confidentiality [1-4] in information systems (IS) that operate in conditions of resource limitations. The relevance of this direction emphasizes the need to create energy-efficient steganographic algorithms that combine content resistance to hacking and low computational complexity. Experiments confirmed the assumption that the procedure of preliminary content smoothing improves the starting conditions for the formation of series of basic blocks (BB) of source images (in this case, content), minimizing the number of procedures at the stage of their encoding with conversion. The introduction of these procedures reduces the consequences of fluctuation «noise» in low-information areas of images and improves the computational complexity indicator of the processing algorithm. Following the test trials results, preliminary assessments of their performance were obtained: - in terms of execution time, PSNR indicator, and the number of BBs formed. The ability to flexibly configure preprocessing parameters [1,5] allows the smoothing process to be adapted to different types of data (statistical properties of content), ensuring a controlled level of visual distortion in the conditions of existing resource limitations of the hardware platforms used. In practical terms, such consequences are extremely useful, especially in conditions of multitasking and/or a scarcity of residual battery capacity in gadgets. This ensures high flexibility and efficiency of the steganography process, even in the conditions of limited resources of the base device and/or system. The modeling performed allows to speak about good prospects for further implementation of the considered data processing mechanisms into the structure of specialized steganographic algorithms included in the group of mobile applications. The results obtained contribute to the further improvement of the concept of low-resource steganography and form perspective directions for further research.

Keywords: steganography, run-lengths encoding, images, basic block, encapsulation, computational complexity; resource consensus.

Introduction

Modern digital technologies open up wide possibilities for data processing and analysis, creating new ways and forms of communication and information exchange [3-4]. However, the rapid development of information technology leads to the emergence of new and growth of already known security threats: - unauthorized access to information; modification and falsification of data; changing user permissions and/or equipment settings, etc. This trend emphasizes the need for continuous improvement and development of new technologies and tools for ensuring information security – IS. In such a genesis of events, digital steganography [5-6] remains an important security tool [1-2] that preserves data confidentiality when using modern information and communication systems (ICS). Unlike cryptographic methods of information protection, steganography additionally conceals the fact of the existence of the process of exchanging/storing important information (hereinafter referred to as content). This process is carried out by embedding secret data in conditional «digital containers» - information carriers (photographic images, audio or video data) [1,7]. It is the imperceptibility of the steganographic insertion that makes digital steganography an important tool for ensuring information security in modern ICS [1]. The development and improvement of steganographic methods that ensure high resistance to content detection, computational efficiency, and hardware cross-platform compatibility is a topical task. In this sense, the key issue is achieving the desired balance between three components: 1 – preserving the necessary visual and statistical properties of the carrier container; 2 – computational complexity (resource intensity) steganographic insertion procedures; 3 – minimal (controlled) distortion of the hidden content [1, 2, 6].

In practical context, steganography covers a wide range of applications: from protecting confidential information in corporate ICS to ensuring data security in mobile devices of private users [4, 8]. Modern steganographic algorithms take into consideration the statistical characteristics of digital media and the properties of information exchange protocols, as well as the physiological characteristics of human senses (sight and hearing). A balanced consideration of these properties forms the boundary conditions for ensuring the «imperceptible of changes» to the container-carrier [2, 3, 8]. Given the variety of potential hardware platforms, from powerful servers to mobile devices,

algorithms of steganographic insertion must be optimized to work in conditions of sporadic scarcity of available computing resources [7, 8]. In this direction of effort, particular attention is paid to improving methods that allow the effective use of the statistical properties of content and containers, thereby minimizing the risks of «successful» work on the part of the steganalyst [1]. Based on the experience of specialized specialists [1-4, 7, 8], this work is aimed at further developing the direction of low-resource steganography by improving key stages of data processing, which is expected to contribute to increasing their practical applicability [5, 6, 9].

The aim of the work is to estimate the computational complexity of input content preprocessing procedures and determine the proportion of their impact on the overall resource intensity of the data encapsulation process. In accordance with the selected concept of the steganographic insertion algorithm [5-6], three variants of special preprocessing (hereinafter referred to as smoothing) of low-information areas of test images were simulated. Following the results of test trials, preliminary estimates of their performance were obtained: in execution time, PSNR indicator, and the number of basic blocks (BB) formed. The formation of an array of BBs is a basic condition for further improvement of the energy efficiency indicator of special transformations within the studied concept of a hybrid steganographic algorithm [1-2, 5-7]. This ensures improved data multiplexing combinatorics and improved content resistance to unauthorized extraction attempts [6, 9-10].

The study was conducted by simulating three processing variants [5-6] for different types (based on the criterion of the probability of brightness difference between neighboring elements) of digital halftone images. Within the modeling, variations were conducted: - the sizes of the blocks into which the original image was divided and the parameter «brightness difference value» between neighboring pixels of the test image assemblies (Dataset). A statistical analysis of the results obtained was performed, taking into consideration the number of basic operations (arithmetic, logical, comparisons) for each block of the selected dimension, and the overall procedural complexity for each of the modeled preprocessing (preprocessing) variants was evaluated. Quantitative assessment of controlled indicators was carried out by measuring: - the execution time of defined procedures; - evaluation of the quality of test images by the PSNR metric (after their preprocessing); - counting the number of formed BBs and the length of series of corresponding BBs. Within the scope of this work, all results are given for a test group of images of the «Landscape» type, with their characteristic statistical characteristics of possible texture differences.

Description of the structure of the investigated algorithm and its functional modules

The proposed concept of a multi-level data multiplex of a hybrid steganographic algorithm [5] allows it to be positioned as an autonomous low-resource solution for ensuring data protection as part of various mobile platforms. The process of embedding and extracting information is carried out using a composite data extractor key [6], which provides parameters multiplexing of steganographic insertion of immediately at several levels of protection. Violation of key integrity leads to data loss or distortion, which increases data security. Modern requirements for steganographic systems take into consideration the existing resources limitations of hardware platforms. That makes it important to have algorithms that provide a compromise between concealment quality, detection resistance, and computational efficiency. Adaptive optimization, which takes into consideration local image characteristics, allows for achieving scalability and energy efficiency, particularly through lightweight computational schemes or hardware acceleration.

The structure of the investigated algorithm consists of four main functional modules that sequentially implement all stages of data processing [5]:

1. Preliminary preparation of source data. At this stage, the image structure is analyzed to identify low-information areas that need to be smoothed. The use of smoothing algorithms allows to eliminate noise, optimize brightness distribution, and create favorable conditions for the formation of series of BBs. This reduces the computational complexity of subsequent procedures and contributes to the preservation of the visual characteristics of the container used.

2. Forming series of BBs of images. The previously «smoothed» image is divided into blocks of the required size and grouped according to a specified scanning scheme [10-11]. Then, the resulting array of image blocks is classified into series by analyzing their similarity [12] according to specified criteria [5-6]. The classification results are presented in the form of an array of series of BBs. Such segmentation of the source data allows creating groups of blocks with similar characteristics of brightness, texture, and other parameters (e.g., orientation [11]), which creates «favorable» conditions for further processing procedures.

3. Processing of the BBs of formed series. For the first block of each series of BBs, a discrete cosine transform (DCT) is performed, with subsequent selection and quantization for the most significant coefficients [2,8], which provides the necessary starting conditions (*reduction of the amount of output data without loss of essential information*) for the subsequent insertion of steganographic content.

4. Data encapsulation and multiplexing. Significant DCT coefficients [12] of each of the BBs are embedded in the corresponding blocks (transformants) of containers. It is important that the dimension of container blocks may differ from the dimension of BBs. The procedure of multiplexing (shifting) BBs before encapsulating the significant DCT coefficients into the container structure provides protection of the content from attempts at unauthorized extraction. Simultaneous work with series length parameters, the type of series scanning, and the spatial orientation of BBs [6,11,13] provides wide opportunities for enhancing the content's resistance to attacks. In principle, all these procedures are not computationally complex.

The application of preprocessing procedures for source data is a key stage in ensuring the effectiveness of the steganographic algorithm. These procedures create optimal initial conditions for the implementation of DCT and subsequent encapsulation of data into the structure of container blocks. Preliminary modification of the source data structure (smoothing of low-information areas) contributes to more efficient formation of series of BBs and improves the combinatorics of content concealment to the container data structure. In combination, this increases the resistance of content to detection and attempts at unauthorized extraction [11, 13]. An important feature of this approach is the reduction of computational complexity by reducing redundant calculations in subsequent stages, as well as reducing visual distortions, which ensures the preservation of container quality [5].

The proposed concept for implementing the algorithm positions it as an autonomous solution for protecting graphic data, in particular on mobile platforms with limited resources. The effectiveness of its use is ensured by the following advantages: - low hardware resource requirements, which allows the algorithm to be used on devices with limited computing capabilities; - high processing speed, which is critical for real-time mobile applications, in particular mobile apps; - adaptability to different types of source data, which ensures effective processing of images of various character and allows achieving the necessary processing consensus in an interconnected system of factors: «container – content – free resource». Within the scope of this work, the results of modeling the first functional module of the developed steganographic algorithm, which is responsible for implementing the procedures for preprocessing the source data are considered.

Smoothing variants and computational complexity estimation

The three approaches to processing low-information areas of source images were investigated during the simulations. An analysis of the consequences of changing value of brightness difference between neighboring elements «^{Pz}» and size of «smoothing matrices» - ^{N} [5] was executed. As mentioned above, the main purpose of preliminary preparation of source data is to transform the structure of input images in order to: - reduce the computational complexity of the processing algorithm and complicate the procedures for analysis and unauthorized extraction of concealed content [1, 6]. This preparation involves reducing the number of visually imperceptible brightness differences of the elements of the source images, i.e., conducting a background smoothing procedure on low-information areas of the images. The developed smoothing variants optimize the initial conditions for improving the quality of encapsulation, improving the formation of series of BBs and

© Honcharov M. O., Nariezhnii O. P., Malakhov S. (2025) Analysis of prerequisites for ensuring resource consensus when performing steganographic data insertion procedures. Сучасний захист інформації, 3(63), 37–47. https://doi.org/10.31673/2409-7292.2025.030518

the combinatorics of multiplexing series of BBs [5]. Below is a detailed description and estimate of their computational complexity. The estimation of the computational complexity of the three variants of smoothing low-information areas of images should be realized based on the analysis of the number of basic operations performed during the processing of each image block and the total number of such blocks. Let the input image have a size of $M \times M$ pixels, and the size of the block for processing is $N \times N$ elements. The number of blocks formed as a result of image segmentation is approximately $(M/N)^2$. The overall complexity of the algorithm is determined as the product of the number of blocks by the number of operations within a one block. For example, if processing one block requires $O(N^2)$ operations, the total complexity for the entire image will be $O(M^2)$. It is important to note that actual performance depends not only on asymptotic complexity, but also on constant factors, such as the type of operations and hardware characteristics.

It should be noted that the dimension of the smoothing matrix (N) is a key parameter that affects the visibility of artifacts of the smoothing procedure and the «starting» conditions for further use of the run-lengths encoding method [9, 12]. A block size that is too small (3×3 or 5×5) can process images at high speed, but retains «noise» in low-information areas of the image. On the other hand, too large a block size (e.g., $N = 11$) increases computational costs and can cause noticeable visual artifacts (in the case of an incorrect choice of P_z value). By varying the dimension of the smoothing mask and the type of container, the desired compromise between the acceptable degree of container distortion and the number of computational operations is achieved. This subsequently provides the desired combinatorics of the data multiplex levels used [6, 13]. The optimal choice of N depends on the specific task, the type of image used, the image size M, and the available hardware resources, so the complexity analysis must be accompanied by experimental evaluation [1].

Zero variant. This variant has exclusively «laboratory sense», as it does not implement any smoothing. This is only necessary to compare the characteristics of other preprocessing variants according to the selected set of criteria: 1 - characteristics of the generated array of BBs series; 2 - computational complexity; 3 - the resulting «new» disparity of data arrays in the «content-container» system. In this case, the image is divided into blocks of a specified size without performing preliminary any preparation of the source data. In other words, operations to smooth or change pixel values are not performed, and the subsequent stages of the algorithm use the source image as it is.

The computational complexity of this variant is $O(M^2)$, which corresponds only to the operations of reading the image and dividing it into blocks, since the processing of blocks occurs in a constant number of operations or is not performed at all. In terms of resource usage, the zero variant is the most economical. However, its application is limited, since the lack of smoothing may not provide sufficient block homogeneity necessary to create optimal initial conditions. This, in turn, complicates the formation of series of BBs and the improvement of the combinatorics of the multiplex series. For example, in the presence of noise or sharp brightness transitions in the image, the zero variant will not allow effective data concealment, since the initial conditions for steganographic insertion remain insufficiently controlled.

First variant. The image is divided into blocks of size $N \times N$. For each block, the difference between the brightness of the central pixel and the brightness of its peripheral pixels is evaluated. If this difference is less than the pre-set coarsening threshold P_z, the value of the peripheral pixel is replaced by the value of the central pixel. If the difference exceeds the threshold, the value of the peripheral pixel remains unchanged. Thus, smoothing is performed by replacing the pixel values in the block based on the central element. The computational complexity of processing one block is $O(N^2)$, since for each block $(N^2 - 1)$ comparisons are performed between the central pixel and the peripheral elements. The total number of blocks in an image of size $M \times M$ is equal to $(M/N)^2$.

The total computational complexity of the first variant is calculated as $O(M^2 / N^2) \times O(N^2)$, which simplifies to $O(M^2)$. Pixel replacement operations do not affect the asymptotic complexity,

since they are performed within the block processing in $O(N^2)$. This variant is acceptable in terms of resource costs, since the dependence on the block size is negated when processing the entire image, which provides a basic level of smoothing which can be sufficient for images with low noise levels, creating homogeneous areas. However, for images with significant brightness variations, the method may be less effective, because the smoothing is based only on the central pixel, which does not always reflect the overall characteristics of the block.

Second variant. The image is divided into blocks of size $N \times N$. For each block, the difference between the brightness of the central pixel and the brightness of all other (peripheral) pixels in the block is evaluated. If at least one peripheral pixel exceeds the total brightness of the central pixel by more than a set coarsening threshold P_z, all pixel values in the block are replaced with the average brightness value of all elements in that block (not the central value!). If no peripheral pixel exceeds the threshold, the block remains unchanged. In other words, smoothing is performed by replacing the pixel values in a block based on the average value that takes into consideration all elements of the block. The computational complexity of processing one block is $O(N^2)$, since for each block $(N^2 - 1)$ comparisons are performed between the central pixel and the peripheral elements, and in the case of replacement, the average value of all N^2 elements is calculated, which also requires $O(N^2)$ operations. The total number of blocks in an $M \times M$ image is $(M/N)^2$.

The computational complexity of the second variant is calculated in total as $O(M^2/N^2) \times O(N^2)$, which simplifies to $O(M^2)$. The operations of calculating the average value do not affect the asymptotic complexity, since they are performed within the block processing in $O(N^2)$. Although the asymptotic complexity coincides with the first variant, the actual execution time may be slightly longer due to the additional operations of calculating the average value. The second variant is more effective because replacing with the average value takes into consideration all pixels in the block, which provides more homogeneous areas compared to the first variant, which is based only on the central pixel. This contributes to better brightness equalization and increases the efficiency of the steganographic insertion, reducing the visibility of artifacts. However, calculating the average value adds constant costs, which can be significant for large blocks or on low-performance devices.

Third variant. The image is divided into blocks of a specified size $N \times N$. In each block, the difference between the brightness of all possible pairs of pixels is calculated, which corresponds to a pairwise comparison of all N^2 elements. If at least one difference exceeds the specified coarsening threshold P_z, the block remains unchanged, since this may indicate the presence/formation of a contour. If no difference exceeds the threshold, all pixel values in the block are replaced with the average brightness value of all elements in that block. The computational complexity of processing one block is $O(N^4)$, since pairwise comparisons of all N^2 elements are performed, and the number of such pairs is equal to $C(N^2, 2) = N^2(N^2 - 1)/2$. In the case of replacement, calculating the average value of all N^2 elements requires $O(N^2)$ operations, but this complexity is less significant compared to $O(N^4)$. The total number of blocks in an $M \times M$ size image is equal to $(M/N)^2$.

The complexity of the algorithm is calculated as $O(M^2/N^2) \times O(N^4)$, which simplifies to $O(M^2 \times N^2)$. This complexity indicates a quadratic dependence on both the image size and the block size, making the variant impractical for large values of N or for processing large images on systems with limited computing power. For example, for an image of 1056×1056 pixels ($M = 1056$) and a block size of 11×11 ($N = 11$), the total complexity will be proportional to $1056^2 \times 11^2 \approx 134$ million operations, and for a block size of 3×3 ($N = 3$), it will be $1056^2 \times 3^2 \approx 10$ million operations, which is significantly less than $N = 11$ and significantly exceeds the complexity of other variants. The latter variant provides the deepest analysis of block homogeneity, which can be useful for high-precision steganographic methods where the most detailed accuracy in selecting image blocks is required. However, the high computational complexity makes the algorithm impractical for most applications

with large parameter values, which makes it impossible to use it effectively in real scenarios, especially on devices with limited computing power or when processing large images or blocks.

Generalization of modeling results

Briefly consider the results of estimating the complexity of smoothing procedures, including analysis of time characteristics, the influence of block size and smoothing parameters on image quality (PSNR), and the computational efficiency of the procedures used.

The time characteristics for different processing variants are shown in Table 1. The results of five one-time complete cycles of smoothing procedures [5] and their average execution time are presented. In this example, the dimension of the smoothing matrices is used 3×3 or 5×5 el., which allows demonstrating the influence of the block dimension on the computational complexity and quality of image content smoothing.

Table 1.

Execution time for different variants of source content processing [s]

№ of attempts to perform the operation	**Var. №0** *(NO processing)*		**Var. №1**		**Var. №2**		**Var. №3**	
	Block dimensions (N×N)							
	3×3	**11×11**	**3×3**	**11×11**	**3×3**	**11×11**	**3×3**	**11×11**
1	*0.075*	*0.061*	*0.459*	*0.53*	*0.567*	*0.655*	*2.528*	*6.502*
2	*0.082*	*0.053*	*0.46*	*0.518*	*0.575*	*0.659*	*2.392*	*6.534*
3	*0.091*	*0.051*	*0.42*	*0.54*	*0.516*	*0.638*	*2.332*	*6.521*
4	*0.076*	*0.063*	*0.473*	*0.499*	*0.588*	*0.616*	*2.248*	*6.565*
5	*0.084*	*0.065*	*0.45*	*0.494*	*0.527*	*0.648*	*2.324*	*6.631*
Average execution time	***0.0816***	***0.0586***	***0.4524***	***0.5162***	***0.5546***	***0.6432***	***2.3668***	***6.5506***

Fig. 1 presents the results of the influence of different smoothing variants for images of the «Landscape» type when different parameters of the processing algorithm. To evaluate the quality of visual distortions of content, the peak signal-to-noise ratio (PSNR) was used. The change in *PSNR* value illustrates the dependence of the resulting image quality on the block size (in this case, smoothing matrices) and the P_z value for different smoothing/processing variants. This allows to objectively evaluate the effect and consequences of using each of the studied processing methods [5, 9, 13]. It should be emphasized that for variant «0» it is impossible to calculate PSNR, since the result is the original image without any changes. The graphs of the number of BBs in Fig. 2 (a-b) confirm this trend that when using large values of N and P_z, all variants show a decrease in the number of BBs. The results demonstrate the feasibility of using a variable approach to smoothing with the ability to adjust preprocessing parameters depending on the image type and requirements for low-performance devices. Fig. 2 (c-d) presents histograms of PSNR values depending on the smoothing variant used [5]. The simulation results confirm the importance of correctly selecting the current processing parameters, which ensures the required level of BB repeatability and preservation of important details in the image. This is important for both content conditions and containers - images. In this case, the higher the degree of smoothing (i.e., the greater the average length of the series that are formed), the better the derived «starting» conditions for working within the «content ↔ container» entity system. Such an improvement provides the conditions for achieving the final target: ensuring a low-resource steganographic insertion mode.

The obtained data allows to estimate the effectiveness of processing methods, determine optimal parameters, and achieve a balance between image quality and computational complexity of the algorithm for further data encapsulation. Increasing the dimension of BB and the P_z parameter

© Honcharov M. O., Nariezhnii O. P., Malakhov S. (2025) Analysis of prerequisites for ensuring resource consensus when performing steganographic data insertion procedures. Сучасний захист інформації, 3(63), 37–47. https://doi.org/10.31673/2409-7292.2025.030518

reduces the number of BBs series, which narrows the base of possible permutations for the current series parameters and increases the visibility of artifacts. BBs of higher dimension are less prone to an increase in the number of formed series than when using blocks of low dimension [5].

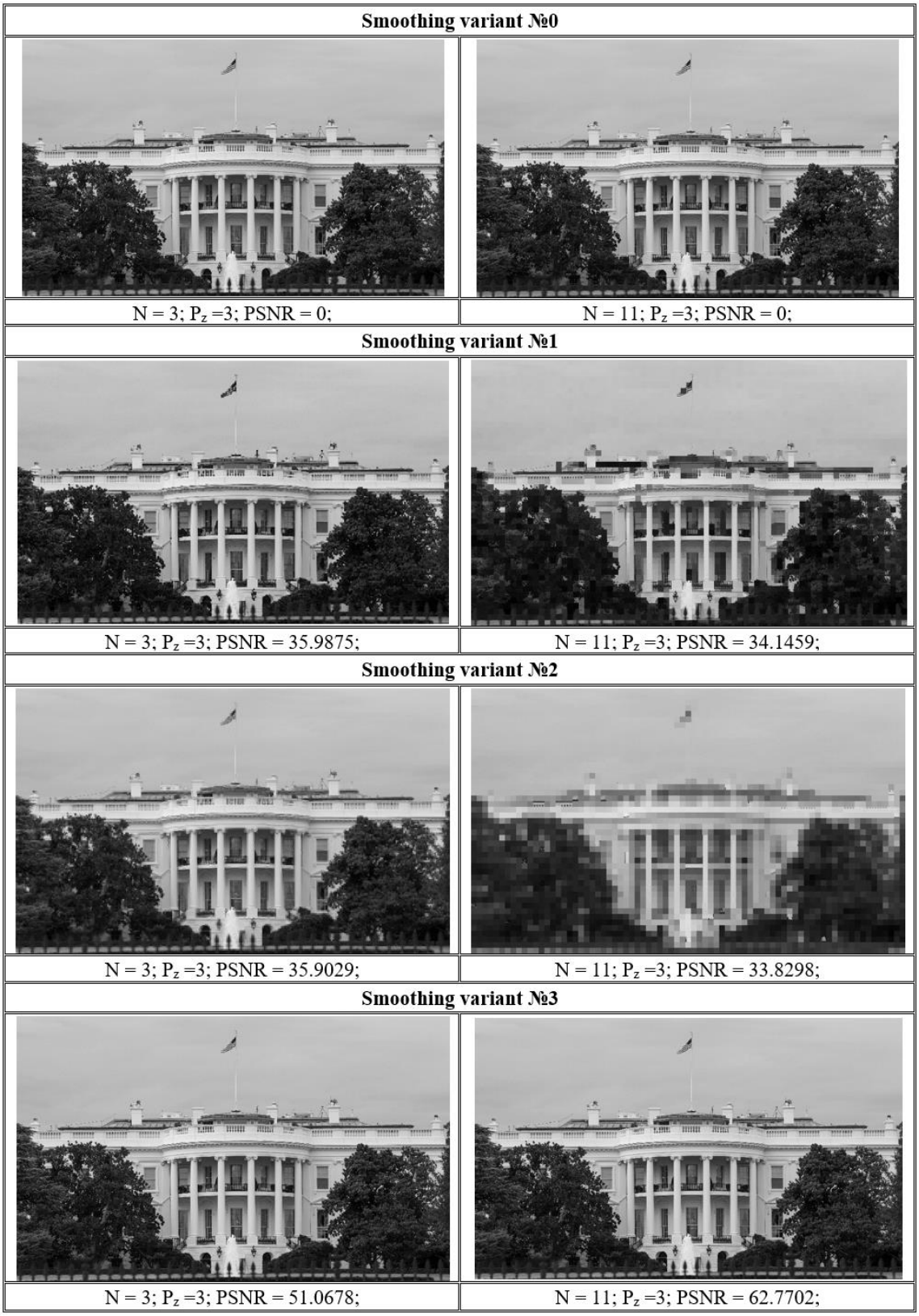

Fig. 1. Test image (Var. №0) and results of three Variants of its preprocessing for different sizes of the «smoothing mask» (*at* $P_z = 3$).

The dimensions of smoothing matrices from 3 to 5 elements, images blocks with a dimension of 4 to 9 el., and coarsening threshold values « P_z » from 3 to 14 brightness gradations are the most optimal processing parameters. This range of settings provides the necessary balance between the quality of reproduced images (both content and container), the number of BBs formed, and the computational complexity of processing procedures.

Fig. 2. Number of BBs and PSNR values for different preprocessing Variants of the test image, type «Landscape» (see Fig. 1).

© Honcharov M. O., Nariezhnii O. P., Malakhov S. (2025) Analysis of prerequisites for ensuring resource consensus when performing steganographic data insertion procedures. Сучасний захист інформації, 3(63), 37–47. https://doi.org/10.31673/2409-7292.2025.030518

The simulation results confirmed that the selected smoothing parameters contribute to the high adaptability of the algorithm to different degrees of image detail [5]. This allows the method to be effectively scaled to process not only portrait images, but also other types of visual content. Such flexibility opens up broad prospects for further research and improvement of modern approaches to image processing, taking into consideration their statistical properties [12] and local characteristics of individual blocks (fragments). This allows to develop more effective procedures for analyzing and using the properties of various visual content [5-6, 12].

Conclusions

1. The use of various variants of preprocessing of the source images of the content provides the necessary conditions for the formation of an array of series of BBs. This improves the ratio of statistical properties of container/content data and strengthens data encapsulation combinatorics [5-6,13]. The number of formed series of BBs depends on a number of parameters that ensure the adaptation of the algorithm to current resource constraints and the features of the processed data. These parameters should include the following [5-6, 10-11]: - image type (content and container); - dimension of the «smoothing mask» (in the example of Fig. 1, these are 3×3 and 11×11 el.); - coarsening threshold « P_z »; - block size at the stage of performing DCT; - the scan scheme used and, as a variant, the orientation of the BBs. Correct selection of the appropriate parameters allows the algorithm to be adapted to different action scenarios and working conditions.

2. Reducing the total number of images blocks that require performing direct and inverse transformations allows to reduce processing time and balance the computational complexity of the algorithm. This contributes to improving its work efficiency and supports consensus between the resource intensity of data processing procedures, the level of current hardware limitations (memory, processor, final residual battery capacity of the gadget, bandwidth of the communication channel used) and the desired level of content stability [10, 11, 13].

3. An assessment of the computational complexity of input data preprocessing procedures showed that the first and second variants for processing neighboring matrices [5-6] have practically the same asymptotic complexity. They demonstrate quadratic computational complexity $O(M^2)$, which makes them the optimal choice for operating conditions characterized by limited available (including free) hardware resources. Their application provides a sufficient level of stability at moderate computational costs. The zero variant (without smoothing) does not generate any homogeneity of the output data, i.e., it is only interesting from the point of view of the possibility of comparing the results obtained under the condition of implementing any preprocessing procedures. The last, third variant (with complexity $O(M^2 \times N^2)$) showed the highest smoothing quality. However, it is impractical for large images (or blocks) due to its high resource intensity, which significantly limits its practical use in real conditions of steganographic insertion.

4. Varying the size of the smoothing mask and the type of image-container allows a compromise to be reached between the permissible level of distortion and the number of BBs formed [5, 9]. This ensures improvement of data multiplexing combinatorics and content resistance to unauthorized extraction attempts [6, 11, 13].

5. The ability to change the current parameters of containers-carriers, depending on the statistical characteristics of the image-content and/or the current resource limitations of the hardware platform (for example, the battery charge level of a mobile device), allows to operative optimize the overall processing algorithm. This ensures high flexibility and efficiency of the steganographic insertion process, even under conditions of limited resources of the base device/system. This makes the researched algorithm concept suitable for the conditions of energy-efficient software applications, for example: - streaming video content extraction with integrated steganographic mark or guaranteed data concealment in conditions of scarcity of computing power of the used ICS, etc.

6. For a group of images of the «Landscape» type (Fig. 1), the choice of parameters for their preprocessing is not as critical as in the case of images of the «Portrait» or «Mnemonic» types [5, 9, 12]. In this case, the texture features of the vast majority of areas of the processed images are saturated

© Honcharov M. O., Nariezhnii O. P., Malakhov S. (2025) Analysis of prerequisites for ensuring resource consensus when performing steganographic data insertion procedures. Сучасний захист інформації, 3(63), 37–47. https://doi.org/10.31673/2409-7292.2025.030518

with various details and are characterized by high values of the probability of brightness differential between neighboring elements (pixels) and data blocks. On the one hand, this noticeably narrows the possibilities for visually «imperceptible» generation of series of BBs and worsens the time indicators of processing. However, on the other hand, the use of such data improves the conditions for encapsulating content directly into the structure of the current BBs. This reduces the visibility of artifacts and increases resistance to revealing the fact of steganographic insertion. In this case, the optimal values for the dimension of the BBs matrices are from 4 to 8 elements, and the coarsening threshold « P_z » is from 3 to 14 brightness gradations (at 256 levels of shades gray). Such settings ensure a balance between preserving the visually unchanged quality of the processed images and the efficiency of the process of forming series of BBs. This complicates the work of a steganalyst and improves the process of hiding information, provided that the criteria of current resource intensity and/or processing time spent are not dominant.

7. The novelty of the conducted research lies in the improvement of the stages and content of the procedures for processing source data (content) within the realization of the concept of «low-resource» adaptive steganographic insertion [5-6, 9]. The considered variants of preprocessing the source images provide for creating the necessary preconditions for reducing the overall computational complexity of the algorithm and «improving the conditions» for encapsulating steganographic content. The term «improvement of conditions» should be understood as the process of changing the output statistical relationships in the «content ↔ container» system to more favorable ones from the point of view of the final goal, namely: - ensuring the mode of low-resource steganographic insertion. The practical significance of the performed modeling lies in the possibility of further implementation of the considered procedures into the structure of specialized steganographic algorithms that are capable of functioning under the conditions of significant resource constraints of modern ICS. The theoretical significance of the research lies in deepening the understanding of the essence of the influence of local characteristics of the source data on: - the process of forming series of BBs; - the combinatoriality of content multiplexing procedures as a mechanism for countering attempts at unauthorized data extraction. As prospects for further research, it should be noted: - automation of procedures for selecting optimal data processing parameters for different states of elements in the conditional system «content - container – resource»; - optimization of the structure of the data extractor key, which supports the conceptual paradigm of «low-resource» steganography.

References

1. Конахович, Г., Прогонов, Д., & Пузиренко, О. (2018). Комп'ютерна стеганографічна обробка й аналіз мультимедійних даних : підручник. Київ: Центр навчальної літератури.

2. Fridrich, J. (2009). Steganography in Digital Media: Principles, Algorithms, and Applications. Cambridge: Cambridge University Press.

3. Yahya, A. (2019). Steganography techniques for digital images. Springer International Publishing.

4. Hassaballah, M. (2020). Digital Media Steganography: Principles, Algorithms, and Advances. Academic Press.

5. Гончаров, М. О., & Малахов, С. В. (2021, 21–23 квітня). Моделювання процедур підготовки даних стеганоалгоритма з багаторівневим мультиплексуванням контенту. Комп'ютерне моделювання в наукоємних технологіях (КНМТ-2021): матеріали 7-ї міжнар. наук.-техн. конф. Харків: ХНУ ім. В. Н. Каразіна, 118–122. URL: http://surl.li/axsna.

6. Honcharov, M., & Malakhov, S. (2024). MODELING ATTEMPTS OF UNAUTHORIZED EXTRACTION OF STEGANOCONTENT UNDER DIFFERENT COMBINATIONS OF DATA KEY-EXTRACTOR. Collection of Scientific Papers «ΛΌГОΣ», (March 1, 2024; Paris, France), 234-245. DOI: 10.36074/logos-01.03.2024.053.

7. Shih, F. Y. (2020). Digital watermarking and steganography. Boca Raton: CRC Press.

8. Fuad, M., & Ernawan, F. (2020). Video steganography based on DCT psychovisual and object motion. Bulletin of Electrical Engineering and Informatics, 9(3), 1015–1023. DOI: 10.11591/eei.v9i3.1859

9. Гончаров, Н., Лесная, Ю., & Малахов, С. (2022). Адаптация принципа кодирования длин серий для противодействия попыткам неавторизованной экстракции стеганоконтента. Grail of Science, (17), 241-247. DOI: 10.36074/grail-of-science.22.07.2022.042.

10. Honcharov, M., & Malakhov, S. (2023). Adaptive modification of the output array of basic blocks series as a mechanism to counteract unauthorized extraction of the staganocontent. Science and technology today, 8(22), 336-352. DOI:10.52058/2786-6025-2023-8(22)-336-352.

11. Малахов, С., Колованова, Є., & Гончаров, М. (2023). ОСОБЛИВОСТІ НЕСАНКЦІОНОВАНОЇ ЕКСТРАКЦІЇ СТЕГАНОКОНТЕНТУ ПРИ ЗМІНАХ ПРОСТОРОВОГО ПОЗИЦІЮВАННЯ ОПОРНИХ БЛОКІВ КОНТЕНТУ. Collection of Scientific Papers «ΛΌГОΣ», (May 26, 2023; Boston, USA), 152–157. DOI: 10.36074/logos-26.05.2023.041

12. Pratt, W. K. (1978). Digital Image Processing. John Wiley & Sons.

13. Honcharov, M., Pavlova, L., & Lesnaya, Y. (2022). Modeling steganocontent extraction attempts with different lengths stack sampling series of images blocks. Computer Science and Cybersecurity, (2), 22-27. DOI: 10.26565/2519-2310-2022-2-02

Надійшла 20.06.2025