symmetry

MDPI

Article

Steganographic Method in Selected Areas of the Stego-Carrier in the Spatial Domain

Predrag Milosav [1,*], Milan Milosavljević [1,2] and Zoran Banjac [1]

[1] Vlatacom Institute, 11000 Belgrade, Serbia; mmilosavljevic@singidunum.ac.rs (M.M.); zoran.banjac@vlatacom.com (Z.B.)
[2] Faculty of Technical Sciences, Singidunum University, 11000 Belgrade, Serbia
* Correspondence: predrag.milosav@vlatacom.com

Abstract: The main goal of this paper is the proposal of a key-based steganographic system in which the ratio of capacity and image quality metrics that represents the stego object while reducing the detectability of hidden content was improved. The main contribution of the proposed steganographic system is a new algorithm for selecting stego areas. The area selection algorithm is based on clustering the pixels of the cover object into a predetermined number of clusters. The goal of this selection of areas (clusters) is to group as many homogeneous parts of the image as possible in order to cover these areas with as few rectangular shapes as possible. Since the data on the defined rectangles represent the key of the system, the capacity of the additional secret channel is minimized in this way. On the obtained stego-carriers, an embedding of test random content is performed in order to estimate its detectability. By combining the proposed area selection method with the Minimal Decimal Difference steganographic method, a system was created with an optimal trade-off between detectability of secret content, quality and capacity of the carrier, and the length of the stego-key. Finally, a comparison of the obtained results with relevant adaptive steganographic methods is presented. The proposed concept obtains its verification in one practical system for secure file transfer of controlled cryptographic strength.

Keywords: image processing; spatial steganography; stego-area; adaptive steganography; K-means; least significant bit (LSB); minimum decimal difference (MDD); histogram; MSE; RMSE; SNR; PSNR; SSIM; steganalysis

Citation: Milosav, P.; Milosavljević, M.; Banjac, Z. Steganographic Method in Selected Areas of the Stego-Carrier in the Spatial Domain. *Symmetry* **2023**, *15*, 1015. https://doi.org/10.3390/sym15051015

Academic Editors: Jian-Qiang Wang and Christos Volos

Received: 20 March 2023
Revised: 13 April 2023
Accepted: 28 April 2023
Published: 2 May 2023

1. Introduction

In accordance with the progress of computer and communication technologies, signal processing and machine learning, the continuous progress of traffic analysis systems is evident. Such systems, installed at large telecommunications hubs, process a huge amount of traffic every day, creating the possibility of illegal violation of the privacy of communications [1]. By increasing the power of such systems, there is a need to develop new steganographic techniques, improving their robustness and resistance to stego-analysis and stego-attack tools. The development of new techniques that lead to the improvement in the mentioned characteristics of stego-objects implies the use of more complex algorithms, and the higher processing power required for this type of processing is the price to be paid. Improving the quality (expressed through numerical values) of stego-objects by a combination of different methods and techniques, quantified through different stego-carrier parameters, is one of the main goals in this context. In addition, one of the goals of developing new methods and techniques is to reduce the accuracy of recognizing the existence of secret content in a stego-object.

In order for a technique to be considered steganographic, four elements are required [2]:

1. Cover object (carrier): the source object used as a carrier to hide information.
2. Message: the secret information that we want to hide.
3. Stego-object: the result of imprinting a message or secret information into the initial cover-object (carrier).
4. Stego-Method: the algorithm used to embed and extract messages into and from the stego-object.

For the purposes of this paper, the following terms will be defined: the stego-area is a part (area) of the cover object (carrier) in which the steganography process is performed. It should be emphasized that the proposed method is key-based steganography, where the key is the information of the positions of the stego area as well as the number of bits that are affected in each of the areas. Unlike keyless steganographic methods, in our case it is necessary to provide an additional secure channel through which the key is transmitted to the receiving side. The choice for key-based steganography is primarily motivated by the demand for a higher level of security that this class of steganographic systems provides compared to keyless steganographic systems [2]. Carrier capacity means the amount of hidden information that a stego-object can transmit. It is expressed in absolute amounts in bytes or relatively in percentages in relation to the size of the stego-object itself. The term "metric" means a set of numerical values that evaluates the quality of a stego-object. In addition to the two mentioned characteristics of the steganographic algorithm, the third and perhaps the most important characteristic is the property of imperceptibility (detectability) of the change in the statistical characteristics of the carrier, which shows how difficult it is to determine the existence of hidden content. Finally, the constant problems related to steganographic techniques are the tradeoff between the capacity of the stego-carrier, the quality and robustness of the stego-object, as well as the processing power required to execute a specific algorithm. In this paper, a solution to the problem of balancing the three aforementioned characteristics of the steganographic process is proposed.

Section 2 provides an overview of relevant works dealing with adaptive steganography. Section 3 describes the proposed system based on the selection of areas in the spatial domain. Section 4 presents an algorithm for selecting areas in a cover object. Section 5 will describe the implemented steganographic algorithm and criteria for evaluation of the quality of the output stego-objects. Experimental results are given in Section 6, while their analysis is presented in Section 7. In the conclusion, final considerations and possible further directions of research are given.

2. Review of the Papers Relevant to This Work

The term adaptive steganography means combining a wider set of different techniques such as image processing, use of different codes, statistical analysis, mutual combination of different steganographic methods, etc. Until now, various authors have been involved in the development of adaptive steganography methods. Review papers [3,4] provide an excellent classification of different types of steganography and the possibility of combining different methods, while the list of references in the cited papers provides a serious basis for work and further scientific research. While some authors worked on combining different types of steganographic methods to improve the performance of stego-objects, others dealt with a priori processing of cover objects before actually imprinting the secret content. An example of adaptive steganography created as a result of combining several different methods is described in the paper [5], as well as an improved version presented in [6]. In the paper [7], Gandharba Swain proposes his method and shows a certain advantage in the quality of stego objects compared to the authors of [5]. Additionally, as a representative of this type of adaptive steganography, it is important to mention the work of the authors of [8]. In order to conceal a secret message, it is possible to use the entire carrier or only some of its areas, which are called stego-areas, selected on the basis of defined criteria.

Some authors use different methods to select parts of the cover object. So, for example, the authors of the paper [9] used edge detection on the cover object, while Abid Yahya in [10] provided comparative characteristics of adaptive steganographic methods (in certain areas of the carrier) using Scale-Invariant Feature Transform (SIFT) and Speeded-Up Robust Features (SURF) algorithms for selecting specific carrier areas. In [11], clustering was proposed, but within previously defined contours, conceiving this method as key-based. The previous works were selected because at the end of this paper, a comparative analysis of the obtained results with those obtained in [5,7,9] will be performed.

As stated in the Introduction, the proposed algorithm requires additional information on the receiving (Rx) side to detect the selected stego-regions, which implies an increase in security due to the unavailability of this information to the attacker. The advantages of this technique are reflected in increasing the security of the steganographic system at the expense of reducing the capacity of the carrier, and a certain increase in the complexity of the system itself. The increase in security is reflected in the fact that the carrier processing algorithm will choose a different combination of stego-areas for different carriers. Therefore, the stego-attacker (Eva) has an additional problem in the analysis of different carriers, with the expectation that the performed stego analysis (RS analysis [12,13]) of the received stego-objects will show a low level of possibility of revealing the existence of secret content. The increase in the complexity of the system compared to the classic process of steganography is reflected in:

- Processing/preparation of carriers in order to determine the stego-areas that will be used;
- Steganography process in defined areas on the Tx side;
- Providing a way to transfer information about stego-areas on the receiving side (independent channel) in order to later process the received stego-object appropriately;
- The process of extracting secret content from selected areas on the receiving end.

3. Description of the Proposed System

The idea is based on the development of an algorithm that uses input images in png format (stego-carriers, cover objects) as well as a set of parameters that are used to adjust the algorithm for calculating stego-areas and to adjust certain steganographic procedures. The algorithm, at the highest level, is designed to contain two modules that are sequentially connected: the input module performs image processing and forwards information about stego-areas to another module that performs the process of steganography on cover objects, in the stego-region. Since steganography can be considered as a procedure that is applied after the encryption procedure of the secret message, the content that is imprinted in the carrier has the properties of random binary content (Figure 1, RNG block). The output of the algorithm is stego-objects and reports on stego-areas, the percentage of used stego-carrier pixels and carrier capacity depending on the applied stego-methods. The reason for choosing the png input format is the ability to use carrier and stego-object files in raw format, without additional compression. In this sense, percentages of changed pixels can be displayed directly; their size can be expressed in bytes as well as all the statistics that will be calculated and discussed later. The block diagram of the system is shown in Figure 1.

The calculation of metrics over the generated stego-objects, the analysis of the obtained results, combined with the report created during the processing of the carrier in the proposed algorithm, aims to establish a correlation between the characteristics of the cover object, the input set of parameters and the desired performance of the stego-object.

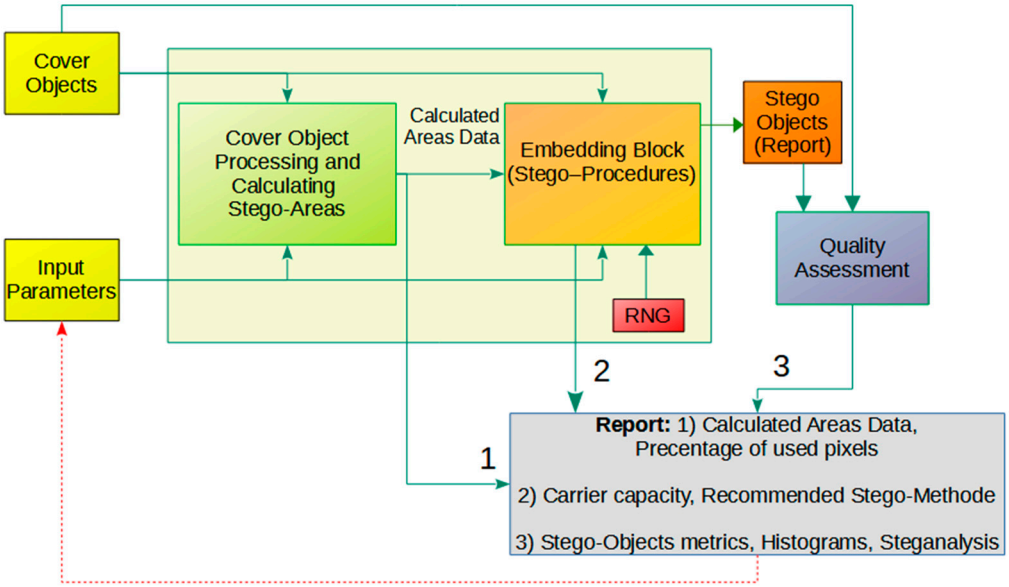

Figure 1. The block diagram of the system.

4. Algorithm for Calculating Stego-Areas

Figure 2 shows a detailed block diagram of the system. The colors of individual parts of the algorithm correspond to the colors shown in Figure 1. In this section, the focus is on the part of the system that deals with calculation of the stego-areas, and those parts of the system are shown in green on the block diagram.

An iterative K-means algorithm is performed over the decimal values of the pixels of the input file in png format, on all three channels (RGB), which results in the clustering of all pixels into N clusters, where N is the input parameter of the algorithm (the number of dominant colors). The iterative K-means algorithm is performed in the following way:

Step 1: Determining the mean value of all pixels (A0);

Step 2: Division of all pixels into two new clusters (C1 and C2) by the K-means algorithm and calculation of new mean values (A1 and A2), which we consider to be the dominant colors, for the newly formed clusters;

Step 3: If the input value is N > 2, an analysis is made of each of the clusters C1 and C2; thus, it is estimated in which cluster there are greater deviations from the mean values of A1 and A2. Suppose that a cluster C2 is selected that has larger pixel deviations than the mean of A2. The K-means algorithm is performed again on the selected cluster C2; then, two new clusters are created that complement the cluster C2. We will call the new clusters C21 and C22 and the new mean values A21 and A22 are calculated. Now, we have a total of three clusters C1, C21 and C22 as well as their three mean values A1, A21 and A22, which we consider the dominant colors;

Step 4: If N > 3, we look at the three existing clusters C1, C21 and C22 and, in the same way as in step 3, we choose which of the existing clusters will be divided into two new ones, while calculating the new mean values. As a result, we obtain four clusters with four mean values.

For larger values of the input parameter N, the algorithm is performed iteratively as explained in steps 3 and 4. Figure 3 shows the original image, and further shows the distribution of pixels of the original image in the 3D (RGB) space, where the size of each sphere is directly proportional to the number of pixels of a particular shade and the way in which the pixels are divided into two clusters. Finally, when we return from the 3D domain of pixel distribution to the image domain, all pixels belonging to cluster 1 are represented by dominant blue color, while all pixels belonging to cluster 2 are represented by dominant green color.

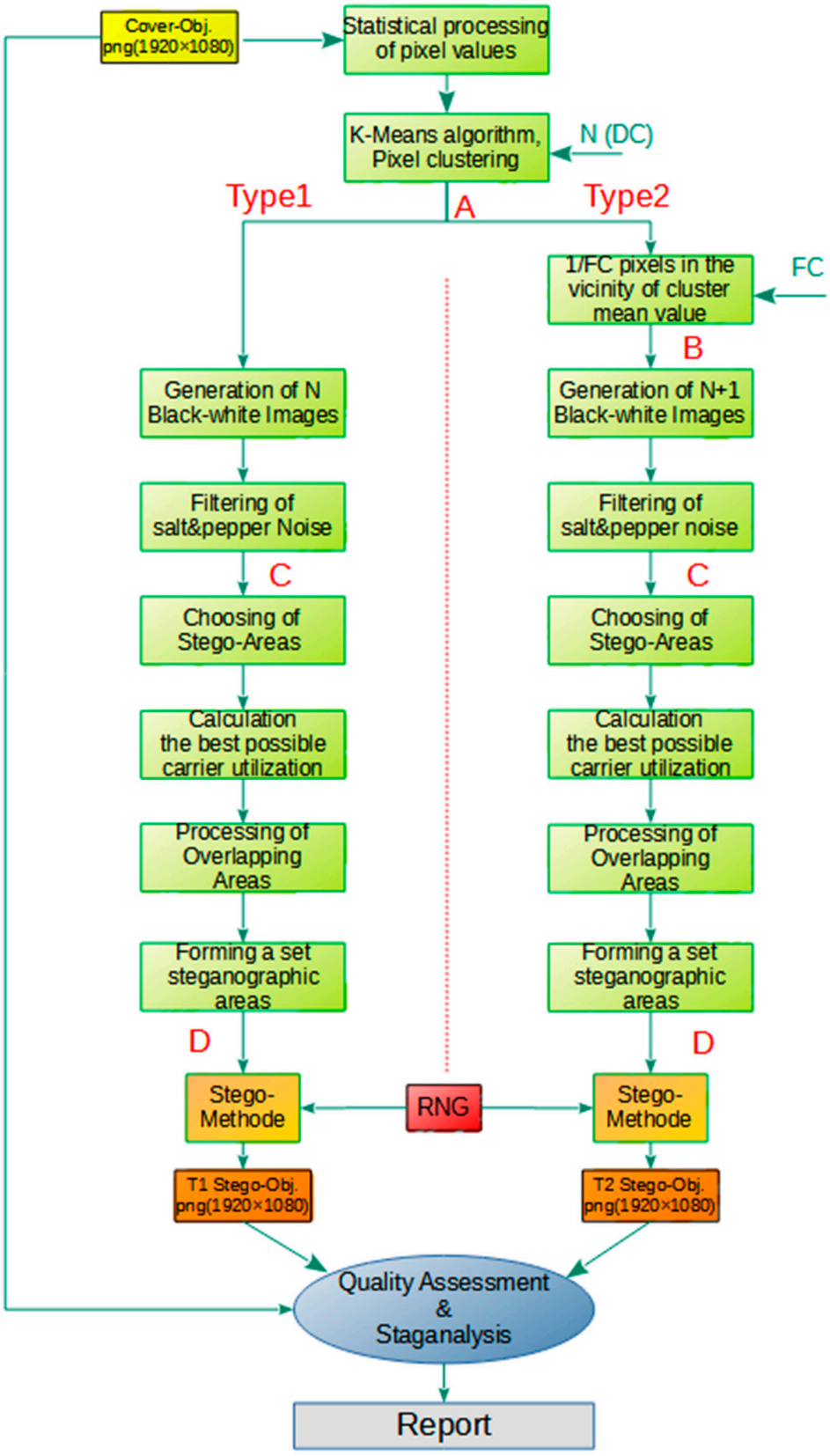

Figure 2. Detailed System Block Diagram.

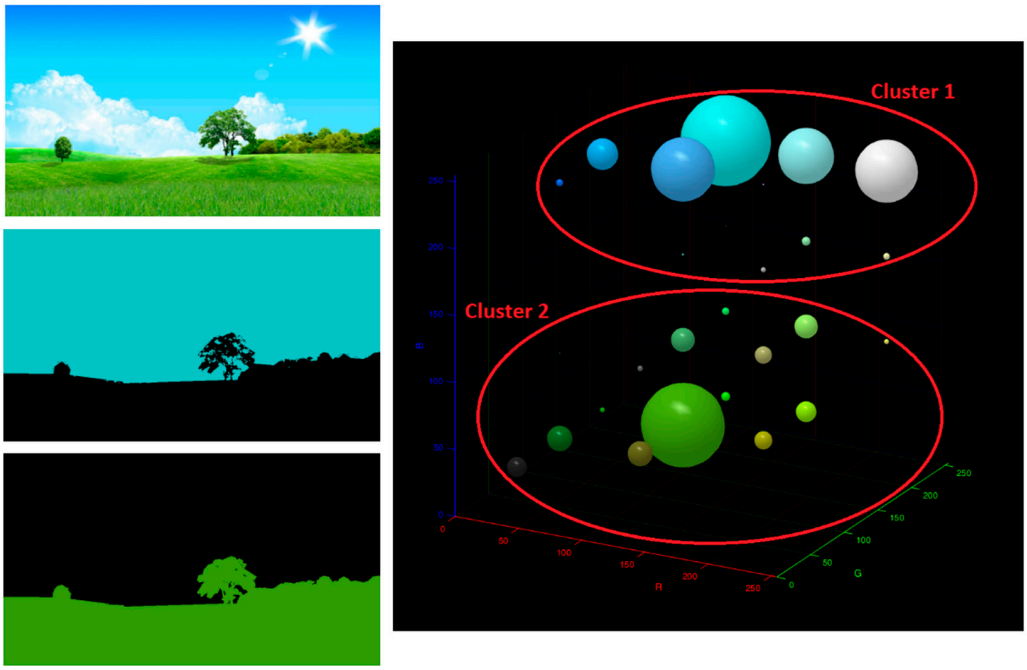

Figure 3. Original image; Distribution of pixels in RGB space, divided into two clusters.

The proposed Type 1 algorithm creates N black and white images where pixels of cluster c = i are shown in white, while pixels belonging to clusters c $\neq$ i are shown in black, where i takes values from 1 to N, where N is the number of required clusters. Figure 4 shows the original image as well as four black-and-white images, the product of the algorithm's interprocessing, for the required N = 4 clusters. Further processing continues on the mentioned black and white images.

Figure 4. Lena.png original and generated black and white images for N = four dominant colors, intermediate processing result in point "C" of the algorithm.

The further flow of the left branch of the algorithm in Figure 2 (Type 1) performs salt and pepper filtering (removing individual solitary pixels to maximize individual zones). At point "C", the next two algorithmic blocks ("Selection of stego area" and "Calculation of the best possible carrier utilization") accept N black and white images, estimate the size of the white areas and try to calculate the rectangles for each black and white image to identify the best possible way to fill the given white area. It is important that the number of calculated rectangles does not exceed the defined limit, and it is also necessary to discard rectangles whose size is smaller than the defined minimum value. The output information from the aforementioned algorithmic block represents a set of rectangles defined for each black and white image, specifically the pixel positions of the upper left and lower right vertices of the rectangle. The next block of algorithms ("Processing overlapping surfaces") accepts information about the calculated rectangles, checks whether there is a possible

overlap of individual rectangles created on different black and white images. If there is an overlap, the algorithm performs an appropriate revision of the rectangle sizes so that, on the one hand, there is no overlap between them, and on the other hand, their size remains as large as possible. Finally, a set of all of the rectangles is formed, selected on N black-and-white images and possibly revised, and the algorithmic block immediately before point "D" ("Formation of a set of steganographic areas") calculates the percentage of stego-areas in a certain carrier, i.e., the amount of confidential information which the carrier can transfer. For visual report purposes, the selected rectangles are drawn in different colors on a grayscale version of the original image so that the viewer can more easily see their position and size. Different geometric shapes can be used in the proposed algorithm. The reason for choosing a rectangle, as a geometric figure that the algorithm will use to form a stego-area, is that multiple rectangles can easily fill an irregular image surface, on the one hand, and on the other hand, information about the position and size of a certain rectangle can be transmitted in minimal amounts of data (upper left pixel position and bottom right pixel position). By increasing the value of the input parameter N, more black-and-white images are obtained, each of which will have a smaller percentage of the white area, which implies the generation of smaller rectangles and thus the reduction in the carrier capacity. As we transmit the information about the generated rectangles (stego-areas) through a special communication channel to the receiving side, it would make sense to define the maximum number of possible stego-areas on one carrier so that the information about them is not too large. In this case, the number of maximum rectangles is limited to less than or equal to 20. Based on the presented idea, it is expected that the capacities of the carriers will differ depending on the type of cover object, so that images with large areas in similar or the same color/shade will have a higher capacity, while images without large zones in similar shades will have a lower capacity.

Now look at the right branch of the algorithm in Figure 2 (Type2), a block behind point "A"-1/FC pixels in the vicinity of the mean color value for a particular cluster is noticed. The idea is different from the previous idea described for the left branch of the algorithm. Actually, the goal is to select 1/FC pixels around the mean color values for individual N clusters (Z_i, i = 1, 2, . . . , N) and create N subsets of pixels composed of them. We declare these subsets as new zones, while all other pixels that deviate sufficiently from the mean values, for each zone Z_i, create a unique, new zone, "Z" (Figure 5). As shown on the right branch of the algorithm in Figure 2, the further flow of processing and calculation of the surface is identical to the left branch of the algorithm, except that now instead of N black and white images, the algorithm searches for stego-regions on N + 1 black and white images. With this approach, we will perform the steganographic process in particular in the zones of dominant colors, and especially in the zone that does not belong to any of the N dominant, so-called "colorful zones". Speaking of LSB steganography, the assumption is that in colorful zones there is a possibility of changing more bits of less weight and at the same time reduce the visual degradation of the quality of the stego-object, while obtaining a greater capacity of the stego-carrier.

Figure 6 is the counterpart of Figure 4 for the right branch of the algorithm (Figure 2). In this case, the number of dominant colors is DC = 2 and the filtration coefficient is FC = 3. The algorithm recognizes the light blue sky color in the image for the input image (a) as well as the green grass area and generates the first two black and white images (b–c). In the third black and white image (d), the white zones clearly show the clustering of all other pixels that do not belong to the 1/FC region for the two dominant colors, just as shown in Figure 5.

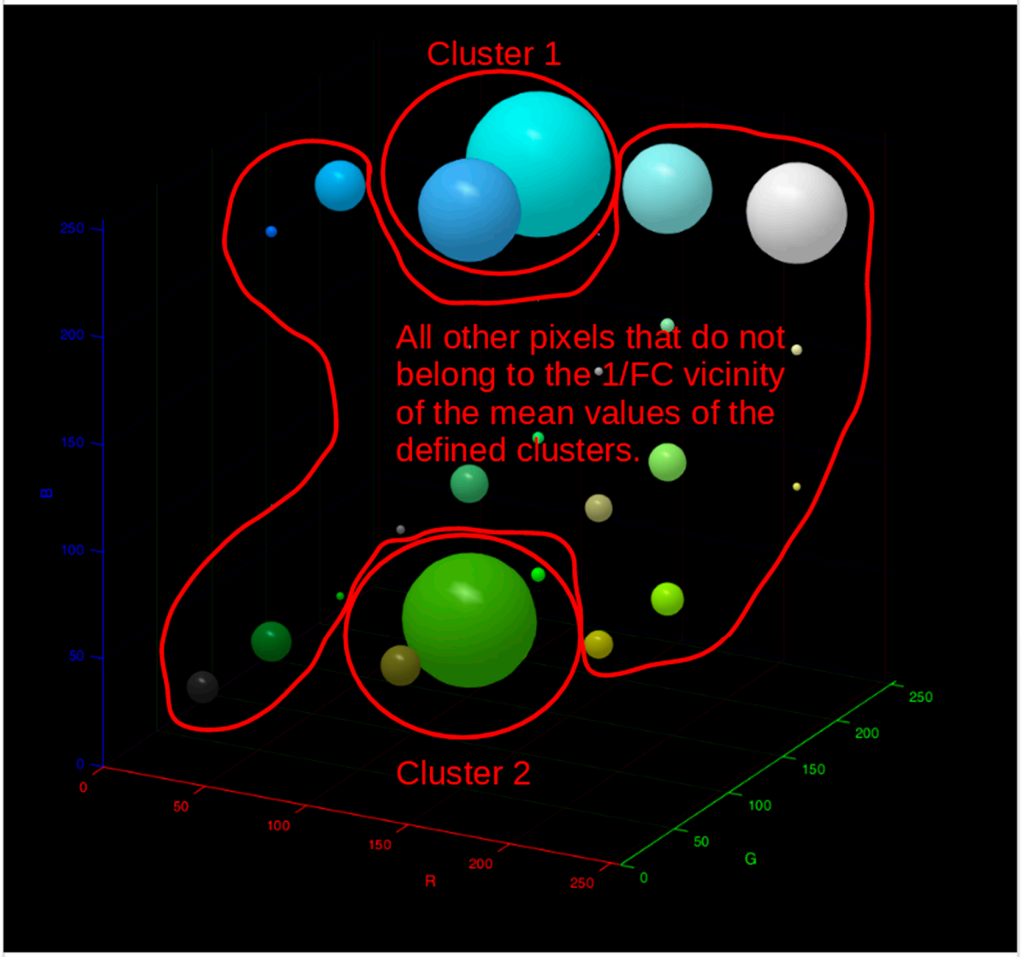

Figure 5. Type 2 pixel clustering method using filtering coefficients.

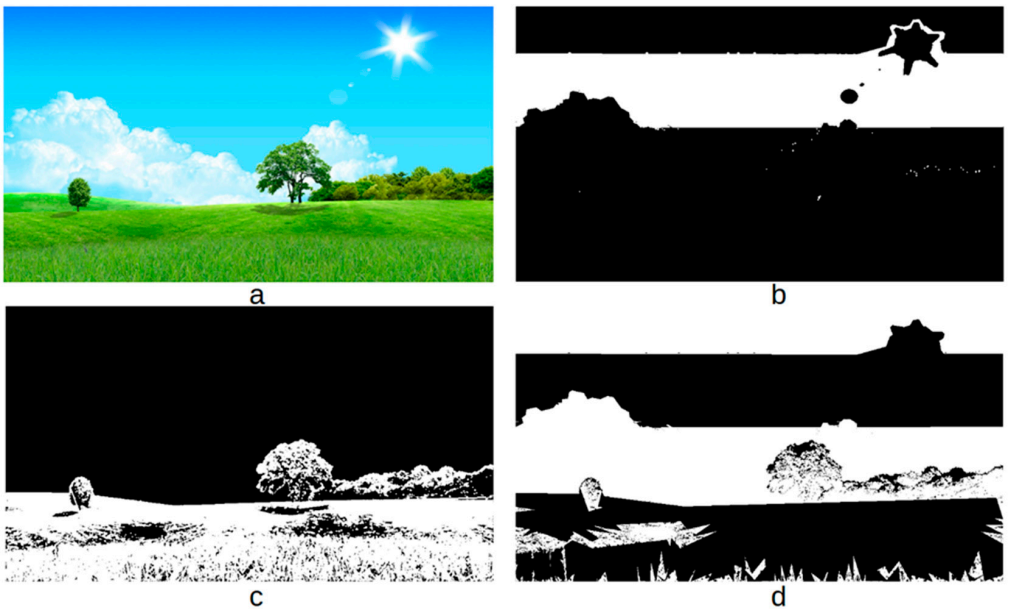

Figure 6. Type 2 pixel clustering method–(**a**) original image, (**b**,**c**) generated black-and-white images where pixels belonging to clusters C1 and C2, respectively, are represented in white color, (**d**) generated black-and-white image where pixels that do not belong to the clusters C1 and C2 are represented in white color.

Finally, Figure 7 shows how the input cover object will be processed, two black-and-white images as a result of interprocessing, and finally the input image presented in grayscale with marked rectangles, i.e., stego-areas. All three images (b-c-d) are part of the stego-region calculation algorithm report.

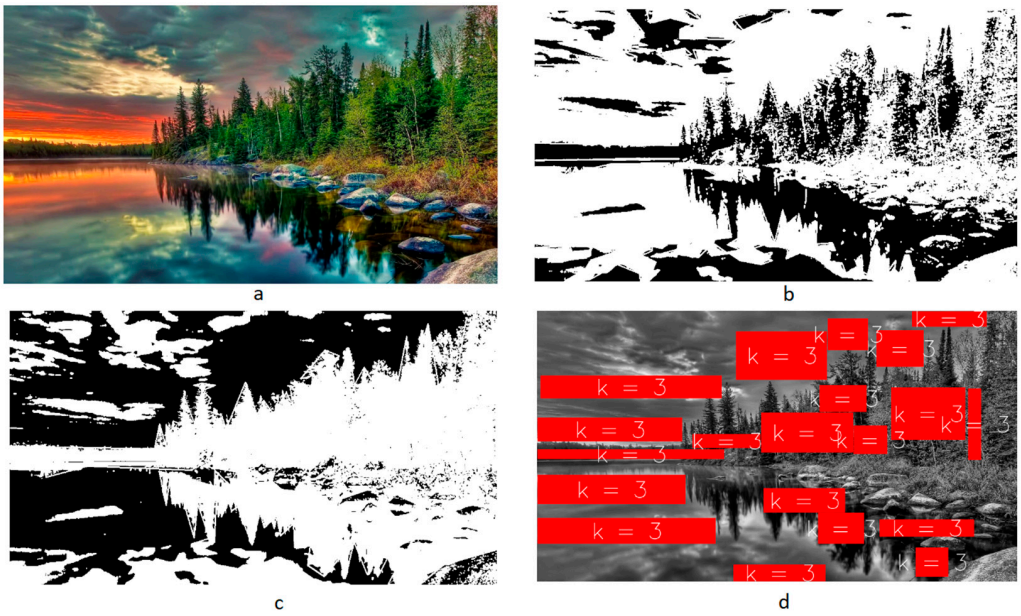

Figure 7. (**a**–**d**) Cover-object Nature2.png; generated black and white images for Type 1, DC = 2; rectangles selected in white zones, presented in additional layer over the grayscale version of original picture.

Based on the explanation of the complete algorithm, it should be noted that complexity is of the order of $O(n^3)$, where n is the number of carrier pixels in one dimension. The processing power and additional time required to run an algorithm of this level of complexity is the price to pay for increasing system security. It should be noted that increasing the resolution of the hiding objects can significantly increase the required processing power and/or processing time.

4.1. Embedding Procedure

Since the areas of the carrier in which the secret content will be imprinted are defined by the algorithm described, serial numbers (indexes) are assigned to the specified rectangles. The process of embedding secret information is completed in pixels, by rows from left to right, and in rectangular areas by indexes, respectively. This approach allows different steganographic methods to be used during the embedding process. The position and the role of the embedding block are shown in Figure 1.

4.2. Extraction Procedure

Since the information about the positions of the rectangles and their serial numbers (indexes) arrives at the receiving side through a special (independent) channel, the algorithm uses this information (Stego-Key), accesses certain areas of the stego-object according to the index, and performs content extraction. As shown in Figure 8, after extracting the content from the defined areas, the inverse process of steganography is performed.

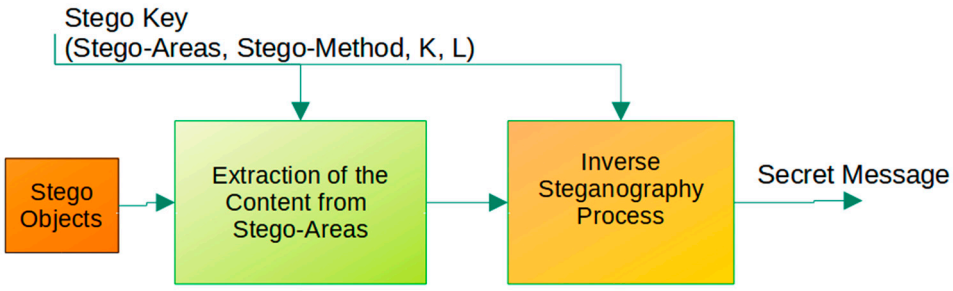

Figure 8. Block diagram of extraction procedure.

5. Implemented Steganographic Methods and Quality Assessment Criteria of Stego Objects

The goal of every steganographic algorithm is to achieve the most performant final product of the system, that is, the stego-object: minimization of visual distortions of the stego-object, greater capacity of the carrier, greater resistance to stego-analytical tools and attacks, greater robustness of the stego-object, better performance expressed in numerical values for carrier quality assessment, less processing time required for imprinting and extraction of secret content. In order to accurately characterize the efficiency of the algorithms, it was necessary to define different evaluation methods and metrics that clearly quantify the quality of the obtained stego-objects as output quantities of the system [14]. There are two types of visual image quality metrics in the literature:

1. Non blind-methods are based on the mathematical calculation of the difference between the input image (image of the carrier-Cover Object) and the output image after the imprinted content (Stego-Object). It is clear that such mathematical tools require two images as input arguments—basic and steganographically modified.

2. Blind methods do not require the original image as a reference for mathematical calculations, but their assessment is based on shape recognition statistics, where the applied algorithm is based on neural networks and machine learning where the processing system is pre-trained.

The subject of this paper is the analysis of the generated stego-objects and the exclusive determination of their quality by means of metrics that show the distortion of the stego-objects in relation to the original concealment objects. Therefore, in further analysis, the focus will be exclusively on Non-Blind metrics.

The methods for image quality assessment (IQA) and calculation of individual (Non blind) metric data applied in this paper are as follows:

MSE—Mean Square Error:

$$MSE = \frac{1}{H \times W} \sum_{i=1}^{H \times W} (C_i - S_i)^2 \quad (1)$$

where C_i is the pixel value of the carrier; S_i is the pixel value of the stego-object and $H \times W$ is the height and width of the carrier image. Lower scores on this metric are considered better.

RMSE—Root Mean Square Error:

$$RMSE = \sqrt{MSE} \quad (2)$$

SNR—Signal to Noise Ratio:

$$SNR = 10 \log_{10} \left(\frac{\sum_{i=1}^{H \times W} C_i^2}{\sum_{i=1}^{H \times W} (C_i - S_i)^2} \right) \quad (3)$$

PSNR—Peak Signal to Noise Ratio:

$$PSNR = 10\log_{10}\left(\frac{Max^2}{MSE}\right) \quad (4)$$

where *Max* is the highest value of pixel intensity (per channel), i.e., 255.

SSIM—Structural Similarity Index:

$$SSIM(x,y) = \frac{(2\mu_x\mu_y + C_1)(2\sigma_{xy} + C_2)}{\left(\mu_x^2 + \mu_y^2 + C_1\right)\left(\sigma_x^2 + \sigma_y^2 + C_2\right)}\sigma_y \quad (5)$$

where μ_x, μ_y, σ_x, σ_y, and σ_{xy} are mean values, standard deviations and cross-variances for images x, y.

Papers [15,16] deal with image quality assessment depending on different metrics. The defined limit values of different quality zones in this paper are a direct consequence of the conclusions and guidelines of the aforementioned studies. Metrics and Numerical Relations:

- RMSE: lower values are considered better.
- SNR: higher values are considered better. Limits: >35 dB—good, >25 dB—acceptable, <25 dB—unacceptable.
- PSNR: higher values are considered better. Limits: >40 dB—good, >35 dB—acceptable, <35 dB—unacceptable.
- SSIM: higher values are considered better. Limit values: >0.99—excellent, >0.95—acceptable, <0.95—unacceptable

Test results for which SNR > 35 dB and PSNR > 40 dB (good quality) with SSIM > 0.99 are classified as excellent quality.

When it comes to the steganalysis of the generated stego-objects, the RS steganalysis described in [12,13] was performed. The obtained results are represented by the parameter p_{rs}, which represents the size of the imprinted content expressed in percentages of RS steganalysis pixels. As the steganography process is performed in certain areas of the carrier, the secret content detectability coefficient p_d is defined and can be calculated as:

$$p_d = \frac{|p_{ib} - p_{rs}|}{cp} \quad (6)$$

where p_{rs} is the length of imprinted content expressed as a percentage of stego-object pixels, p_{ib} is the value of the cover object's initial bias for RS steganalysis, and cp is the percentage of modified stego-object pixels normalized to a range of 0 to 1.

6. Experiment Design

When it comes to steganography in the spatial domain, the LSB and PVD [17] methods are among the most commonly used techniques, so many authors often compare their characteristics and combine them with each other. The MDD method described in [18,19] was used for the basic steganographic method in this work. The MDD method is a derivative of the basic LSB method and, in relation to it, has significant advantages in the quality of stego-objects, which are shown in [18,19]. For the purposes of the experiment, a mutual comparison of the stego-objects obtained by the mentioned methods (MDD/LSB, PVD) was performed, with the expectation that the MDD method will be dominant and thus justify why it was used in this work. In the section dealing with the analysis of the results, a comparison of the quality of stego-objects obtained by the method of adaptive steganography was made, in the context of carrier capacity, quality of stego-objects and resistance to steganalysis.

As described in Sections 3 and 4, the algorithm for calculating the stego-areas passes information about the sizes and positions of the rectangles to the module that performs the steganography process. The sum of the number of pixels of all rectangles represents the

total number of pixels that will be affected during the steganography process, this quantity is called *PixelsToImpact*. This number of pixels can be represented as an absolute value as well as a percentage of the total number of pixels of the cover object. The carrier capacity, *Cap*, for the MDD method is calculated as:

$$Cap = PixelToImpact[\%] \cdot K/8 \quad (7)$$

where K represents the number of LS bits that we change in each channel of the corresponding pixels.

The experiment is performed in two phases, as shown by the left and right branches of the algorithm in Figure 2, on a dataset specially designed for this purposes. We create a dataset consisting of 10 pictures for each of the 10 chosen topics (nature, people, fantasy, food, space, animals, sport, cities, technology, music). The analysis is performed on the full dataset while we illustrate results on the four typical pictures (carriers): Baboon.png, Lena.png, Nature1.png and Nature2.png (Figure 9). In order to better differentiate the obtained results, as the stego-surface calculation algorithm works, the carriers were chosen so that the images Baboon.png and Nature1.png have large areas of similar colors, while this is not the case with the images Lena.png and Nature2.png. In fact, the Nature2.png image was chosen to contain many different colors and without large areas of similar tones. The obtained results and their analysis should show the mentioned differences in the visual experience of the proposed images. It is important to note that all used png image carriers are of full HD format, dimensions 1920 × 1080 pixels, in color, three channels. The size of each of the used media is: 1B × 3Ch(rgb) × 1920 × 1080 = 6075 KB. Before describing the experiments and tests, it should be noted that the complete implementation of the algorithm was developed in the C++ programming language, in the QT development environment and the OpenCV library was used as a tool for image processing.

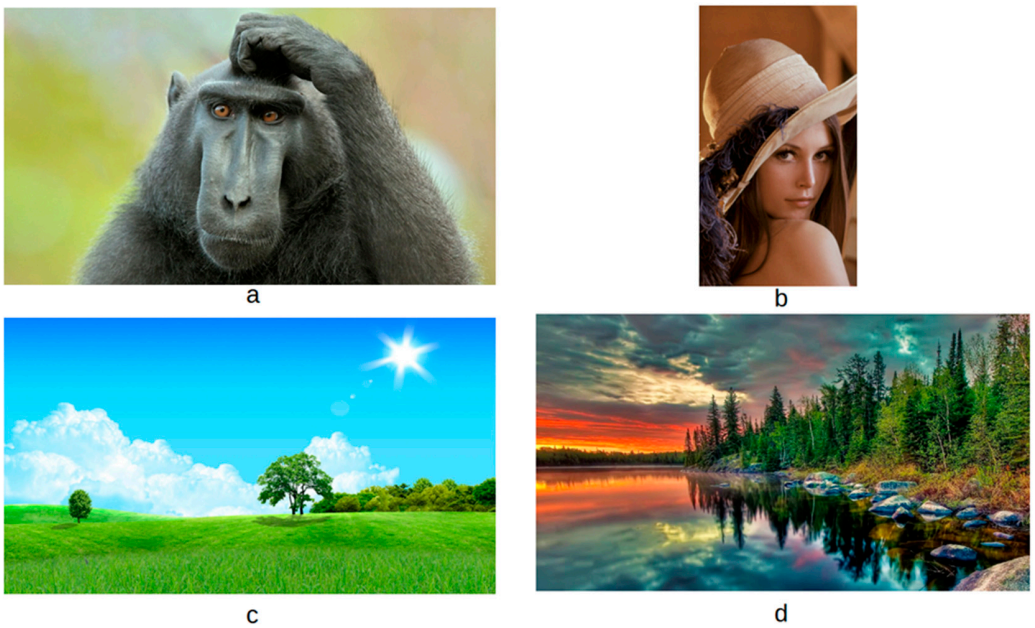

Figure 9. (**a**) Baboon.png; (**b**) Lena.png; (**c**) Nature1.png; (**d**) Nature2.png.

The idea of the Type 1 method is to change the input parameter N (N = 0, 2, 4, 6, 8) and thus zone the corresponding pixels of the input image into N ranges Z_i. The parameter N is varied in steps of two to make the distinction between adjacent measurements more noticeable. For the value of the input parameter N = 0, there is no zoning, that is, the selection of stego-areas which implies the performance of the steganographic process on the entire surface of the stego-carriers.

The software is designed so that it is possible to save the specified black and white derivatives of the processing within the detailed report. After calculating the stego-area of the carrier and marking them on the image in gray scale (Figure 7d), the software also creates a text report that contains data about the rectangles (coordinates of the upper left and lower right pixels), the total number of pixels included in the rectangles, as well as the percentage of specified pixels in relation to the total number of pixels. As stego-methods of the LSB category can be performed with different numbers of K bits that we change, this parameter took the values K = 3, 4 and 5 in the test. As explained earlier, due to the characteristics of the PVD method, it is not possible to choose the number of bits to be modified in the process of steganography, for each channel or for each pixel, so this method will be performed in the usual way, over the entire coverage object or over the stego-areas.

The idea of the Type 2 method is based on the right branch of the algorithm described in Section 3. In this experiment, the number of dominant colors (DC) is fixed at N = 2, while the filtering coefficient is changed as FC = 1, 2, 3, 4. The reason why the parameter N is fixed to the number 2 is that in that case all the pixels are divided into only two large zones and therefore the effects of later filtering around the mean value of the shade for the corresponding cluster according to the FC coefficient are better and clearer. This is where we come to the moment of implementation of the assumption presented in Section 4. Namely, the module for performing the stego-method, for MDD, is implemented with the possibility of influencing K bits in areas belonging to zones Z_i' as well as influencing L bits in zones Z" (so-called "colorful" areas). In this case, the carrier capacity is calculated as:

$$Cap = PixelToImpact[\%](Z') \cdot K/8 + PixelToImpact[\%](Z'') \cdot L/8 \quad (8)$$

where $Z' = \sum_{i=0}^{N} Z_i'$.

In order to better represent the quality behavior of stego-objects for Type 2, the parameter K will have a constant value of K = 3, while the parameter L will have values of 3, 4 and 5.

7. Analysis of Experimental Results Obtained

The results of all tests are presented in the form of a table and can be obtained upon direct request from the authors of this paper. Table 1 as well as Table 2 show the results for the stego-carrier Lena.png obtained based on processing for Type 1 and Type 2 methods, respectively.

Table 1. Results of Type 1 processing on the stego-carrier Lena.png.

Num. of Dominant Colors	Number of Bits to Change	Pix. to Impact [%]	Capacity [%]	bpp	SNR [dB]	PSNR [dB]	SSIM	Rating
0	Complete image K = 3 bits	100	37.50	9.00	32.1586	40.4007	0.9866	Acceptable
	Complete image K = 4 bits	100	50.00	9.00	26.1669	34.409	0.95	Unacceptable
	Complete image K = 5 bits	100	62.50	9.00	20.0243	28.2664	0.8454	Unacceptable
2	Areas K = 3 bits	51.494	19.30	4.63	34.9584	43.2005	0.9922	Acceptable
	Areas K = 4 bits	51.494	25.70	6.18	28.9472	37.1893	0.971	Acceptable
	Areas K = 5 bits	51.494	32.20	7.72	22.7764	31.0185	0.911	Unacceptable
4	Areas K = 3 bits	37.79	14.20	3.40	36.2388	44.4809	0.994	Excellent
	Areas K = 4 bits	37.79	18.90	4.53	30.2328	38.4749	0.9779	Acceptable
	Areas K = 5 bits	37.79	23.60	5.67	24.0319	32.2739	0.933	Unacceptable
6	Areas K = 3 bits	28.89	10.80	2.60	37.7083	45.9504	0.998	Excellent
	Areas K = 4 bits	28.89	14.40	3.47	31.7534	39.9955	0.9922	Acceptable
	Areas K = 5 bits	28.89	18.10	4.33	25.6898	33.9319	0.9737	Unacceptable
8	Areas K = 3 bits	18.425	6.91	1.66	39.5711	47.8132	0.9982	Excellent
	Areas K = 4 bits	18.425	9.21	2.21	33.6024	41.8444	0.9929	Acceptable
	Areas K = 5 bits	18.425	11.50	2.76	27.5033	35.7454	0.9767	Acceptable

Table 2. Results of Type 2 processing on the stego-carrier Lena.png (DC = 2).

Filtering Coef.	Number of Bits to Change	Pix. to Impact [%]	Capacity [%]	bpp	SNR [dB]	PSNR [dB]	SSIM	Rating
1	Areas K = 3 bits, L = 3 bits	51.494	19.30	4.63	34.956	43.1981	0.9922	Acceptable
	Areas K = 3 bits, L = 4 bits	51.494	19.30	4.63	34.956	43.1981	0.9922	Acceptable
	Areas K = 3 bits, L = 5 bits	51.494	19.30	4.63	34.956	43.1981	0.9922	Acceptable
0.5	Areas K = 3 bits, L = 3 bits	43.449	16.30	3.91	35.6914	43.9335	0.9936	Excellent
	Areas K = 3 bits, L = 4 bits	43.449	18.90	4.53	32.1113	40.3534	0.9894	Acceptable
	Areas K = 3 bits, L = 5 bits	43.449	21.60	6.45	26.9894	35.2315	0.9753	Acceptable
0.33	Areas K = 3 bits, L = 3 bits	33.833	12.70	3.05	36.8321	45.0742	0.9958	Excellent
	Areas K = 3 bits, L = 4 bits	33.833	14.10	3.38	33.3766	41.6186	0.9859	Acceptable
	Areas K = 3 bits, L = 5 bits	33.833	20.70	6.89	28.0288	36.2708	0.9584	Acceptable
0.25	Areas K = 3 bits, L = 3 bits	37.301	14.00	3.36	36.6437	44.8858	0.9969	Excellent
	Areas K = 3 bits, L = 4 bits	37.301	17.40	4.17	31.7577	39.9998	0.9912	Acceptable
	Areas K = 3 bits, L = 5 bits	37.301	20.80	6.62	26.0756	34.3177	0.9719	Unacceptable

The results obtained for the Type 1 method (Table 1) show that the carrier capacities decrease with the increase in the number of dominant colors. At the same time, we notice that for the carriers Baboon.png and Nature1.png the capacities decrease more slowly. On the other hand, with Lena.png and Nature2.png carriers, capacities decrease faster due to the characteristics of the images themselves. The change in capacity for different carriers is shown in Figure 10.

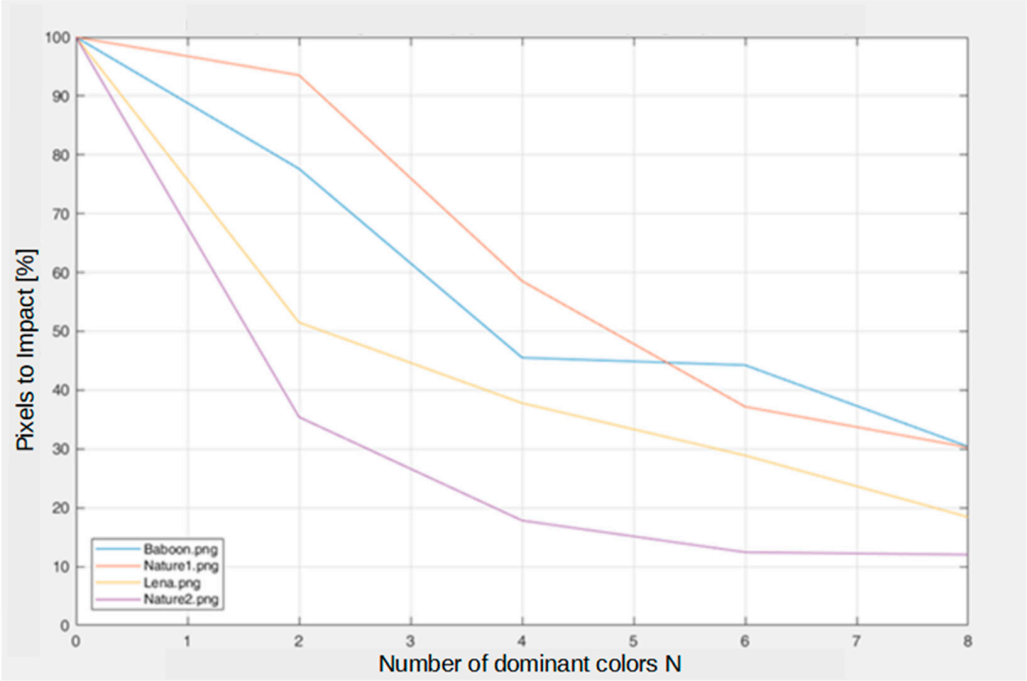

Figure 10. Pixels to Impact for different values of input parameter DC, for Type 1.

The Type 2 method is performed by selecting two dominant colors, changing the filtering coefficient in steps FC ∈ {1, 2, 3, 4}. In this way, the clusters around the two dominant colors are narrowed, and the areas in which the pixel values have larger deviations from the decimal values of the dominant colors are expanded. It is logical that with the filtration coefficient FC = 1 we obtain the same results as in the case of two dominant colors without numerical filtering (Figure 11). It is interesting to note that for three carriers, the minimum capacity is reached at FC = 3, while for Nature2.png the local minimum capacity is reached se for FC = 2. This effect is a consequence of the type of carrier, i.e., the carrier's characteristic is that it does not have large surfaces in the same or similar tones (colors). In order to better represent the average value of the occupancy of stego-carriers of rectangular surfaces after processing with the proposed algorithm, 250 images were randomly selected for processing.

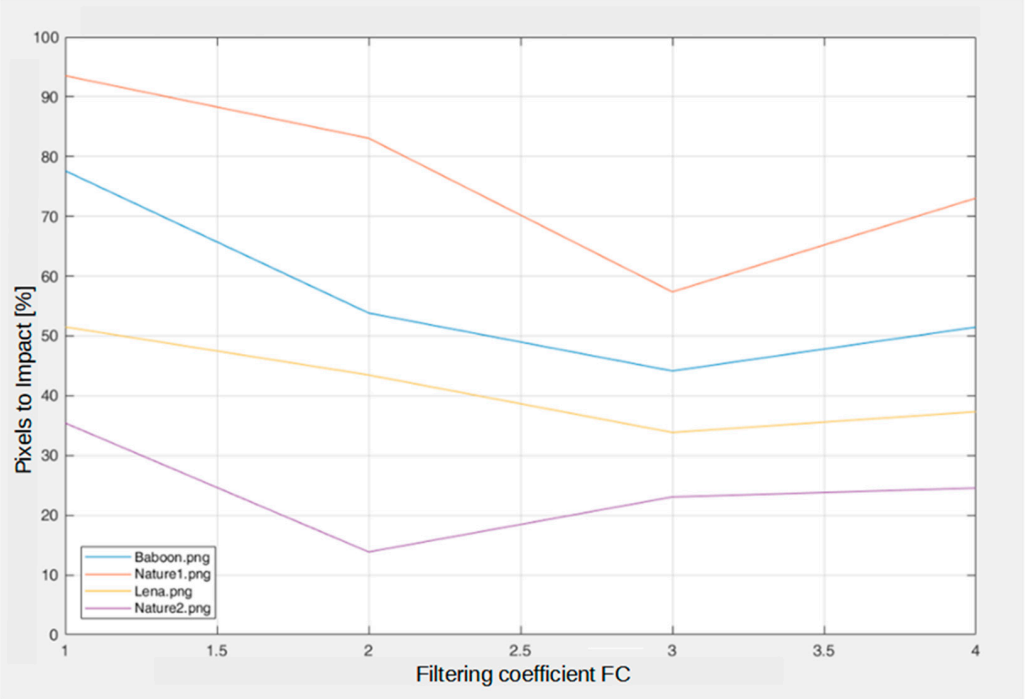

Figure 11. Pixels to Impact for different values of input parameter FC (DC = 2), for Type 2.

Table 3 shows the average value of the percentage of occupancy of stego-carriers depending on the value of the input parameters of the algorithm (the number of dominant colors DC and the filtering coefficient FC).

Table 3. The average values of the pixels to impact obtained on the basis of a sample of 250 different images, for different values of the input parameters of the proposed algorithm.

-	**Type 1 (DC = 2)**	**Type 1 (DC = 4)**	**Type 1 (DC = 6)**	**Type 1 (DC = 8)**	**Type 2, FC = 2 (DC = 2)**	**Type 2, FC = 3 (DC = 2)**	**Type 2, FC = 4 (DC = 2)**
Avg. occupation of stego-carrier areas (%)	58.91	37.94	30.57	26.65	38.71	36.71	36.46

As for Type 1, Figure 12 shows the change in carrier capacity for different methods, for different numbers of selected dominant colors. The graphs are generated based on the numerical data obtained by measurement, the yellow points show the values where the obtained results are considered good, and the green points show the values where the obtained results are considered excellent.

The benefit of steganography in the areas is reflected in the fact that due to the reduction in the capacity of the carriers, the cover object is qualitatively less degraded and thus meets the defined metric limits.

As for Type 2, Figure 13 shows the change in carrier capacity for different methods, for different values of the numerical filtering coefficient (for DC = 2). The graphs are drawn based on the data from the mentioned tables, the yellow points show the values where the obtained results are considered good, and the green points show the values where the obtained results are considered excellent.

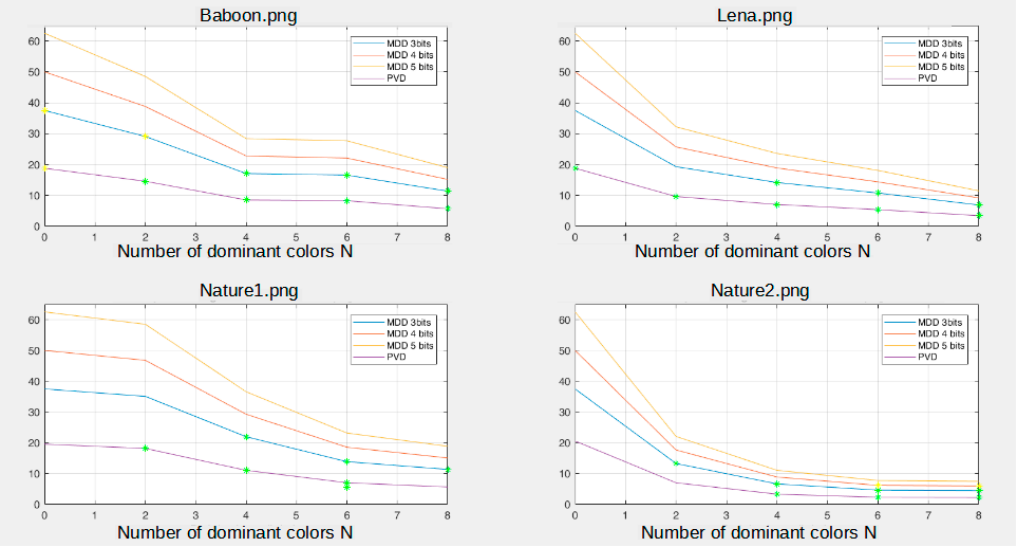

Figure 12. Carrier Capacity for Different Steganographic Methods, Type 1.

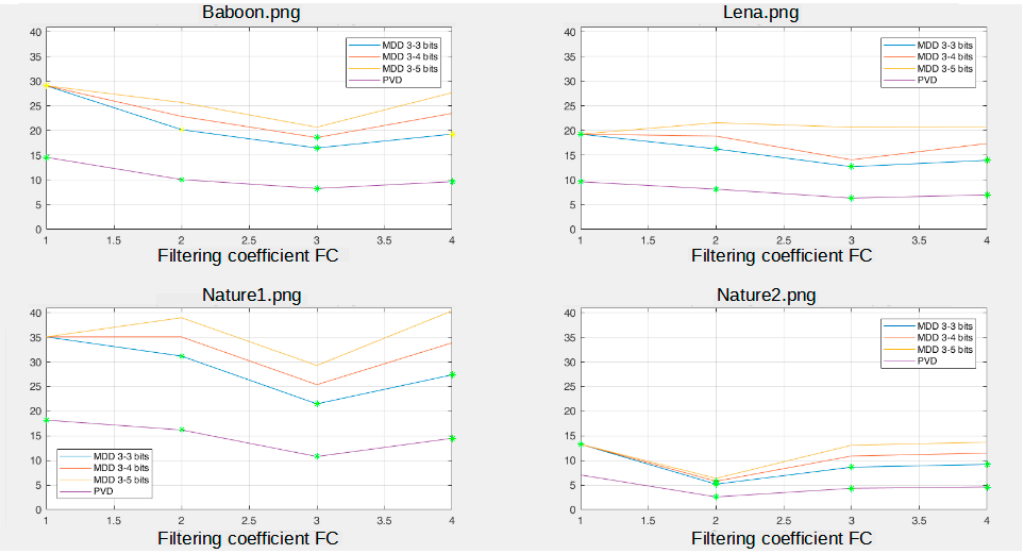

Figure 13. Carrier Capacity for Different Steganographic Methods, Type 2.

Based on the numerical results, it is clear that the SNR and PSNR metrics of the stego-objects decrease with the increase in the number of changed pixels, as well as with the increase in the number of LSB bits that we change. At the same time, by increasing the number of changed LSB bits, the mentioned metric degrades faster.

Several tests and examples have shown better performance of the MDD method compared to PVD, where for the same capacities the MDD stego-carrier gives a better metric or in cases where for similar metric values the MDD has a significantly higher capacity.

The minimum capacity in the graphs shows the best metric performance of the stego-objects, but we can also consider the optimal capacity value and the metric to the left and right of the minimum value, as far as the defined metric limits allow.

A comparative analysis of the results obtained for Type 1 and Type 2 methods leads to clear conclusions about the benefits of performing the MDD steganographic method in selected areas.

Tables 4 and 5 provide a comparative segment of the total set of results for stego-carriers Lena.png and Baboon.png

Table 4. Cover-object Lena.png, Capacity and Metrics.

Type	DC/FC	Method	Bits (K-L)	Pix [%]	Cap [%]	SNR	PSNR	SSIM
1	4/-	MDD	4	37.79	18.9	30.23	38.47	0.9779
2	2/4	MDD	3–4	43.45	18.9	32.11	40.35	0.9894

Table 5. Cover-object Baboon.png, Capacity and Metrics.

Type	DC/FC	Method	Bits (K-L)	Pix [%]	Cap [%]	SNR	PSNR	SSIM
1	4/-	MDD	4	45.51	22.8	32.72	38.14	0.9707
2	2/2	MDD	3–4	53.82	22.9	34.46	39.84	0.9796

The benefit realized by performing steganography with a variable number of LS bits (K = 3, L = 4) for the same carrier capacity is clear.

The generated stego-objects were subjected to RS steganalysis and Table 6 shows the values of the p_{rs} parameter for stego-objects generated by the MDD steganography method. For the purposes of comparing the behavior characteristics of the p_{rs} parameter, the measurement was performed both for the basic LSB method and for the PVD method. The comparative characteristics clearly indicate the dominance of the MDD method in relation to the basic LSB and PVD methods. For a complete set of obtained numerical results, contact the author of this paper.

Table 6. Values of the p_{rs} RS steganalysis parameter for stego-objects obtained by different input parameters of the proposed algorithm over stego-carriers: Baboon, Lena, Nature1 and Nature2.

Cover Object	Initial Bias	Complete Image, K = 3	Type 1, DC = 4, K = 3	Type 1, DC = 8, K = 3	Type 2, DC = 2, FC = 3, K = 3, L = 3	Type 2, DC = 2, FC = 4, K = 3, L = 4
Baboon.png	0.0077	0.0142	0.0075	0.0105	0.0119	0.0016
Lena.png	0.1845	0.324	0.1229	0.1846	0.1557	0.2189
Nature1.png	0.1158	0.3374	0.268	0.1728	0.2703	0.16
Nature2.png	0.1731	0.65	0.2004	0.1876	0.2088	0.2109

As the process of steganography is performed only in certain parts of the stego-carrier, it would be useful to calculate the deviation values of the obtained p_{rs} parameters from the initial bias in relation to the percentage of pixels of the stego-carrier that were affected. Therefore, Table 7 shows the stego-carrier occupancy for different input parameters of the image processing algorithm (expressed in percentages depending on the applied parameters K and L for the MDD method). Table 8 shows the behavior of the detectability factor p_d, described in Section 5, and was obtained based on the data from Tables 6 and 7, which are used to calculate the cp factor from Formula 6.

Table 7. Percentage of changed pixels in stego-objects generated by the MDD method.

Cover Object	Complete Image, K = 3 [%]	Type 1, DC = 4, K = 3 [%]	Type 1, DC = 8, K = 3 [%]	Type 2, DC = 2, FC = 3, K = 3, L = 3 [%]	Type 2, DC = 2, FC = 4, K = 3, L = 4 [%]
Baboon.png	100	45.51	30.38	44.13	51.47
Lena.png	100	37.79	18.42	33.83	37.3
Nature1.png	100	58.54	30.27	57.37	73.05
Nature2.png	100	17.83	12.04	23.05	24.53

Table 8. Values of the detectability factor p_d for stego-objects obtained by the MDD method for different values of the input parameters of the proposed algorithm.

Cover Object	Complete Image, K = 3	Type 1, DC = 4, K = 3	Type 1, DC = 8, K = 3	Type 2, DC = 2, FC = 3, K = 3, L = 3	Type 2, DC = 2, FC = 4, K = 3, L = 4
Baboon.png	0.0065	0.0004	0.0092	0.0095	0.0119
Lena.png	0.1395	0.1630	0.0005	0.0851	0.0922
Nature1.png	0.2216	0.26	0.1883	0.2693	0.0605
Nature2.png	0.4769	0.1531	0.1205	0.1549	0.1541

The way the detectability parameter p_d is defined shows that the detectability of the secret content is higher if the value of the parameter p_d is closer to 1, while for the values of the parameter p_d closer to 0, the detectability of the secret content is lower. Table 8 shows low values of the parameter p_d for stego-carriers Baboon, Lena and Nature2, while somewhat higher values of the parameter p_d were obtained for stego-carrier Nature1. The reason for this is the large areas of the same shades of blue (sky) and green (grass).

The conclusion indicates that this type of stego-carrier should generally be avoided in order to prevent obtaining higher values of the detectability factor p_d. Figure 14 shows RS diagrams for stego-object Lena.png.

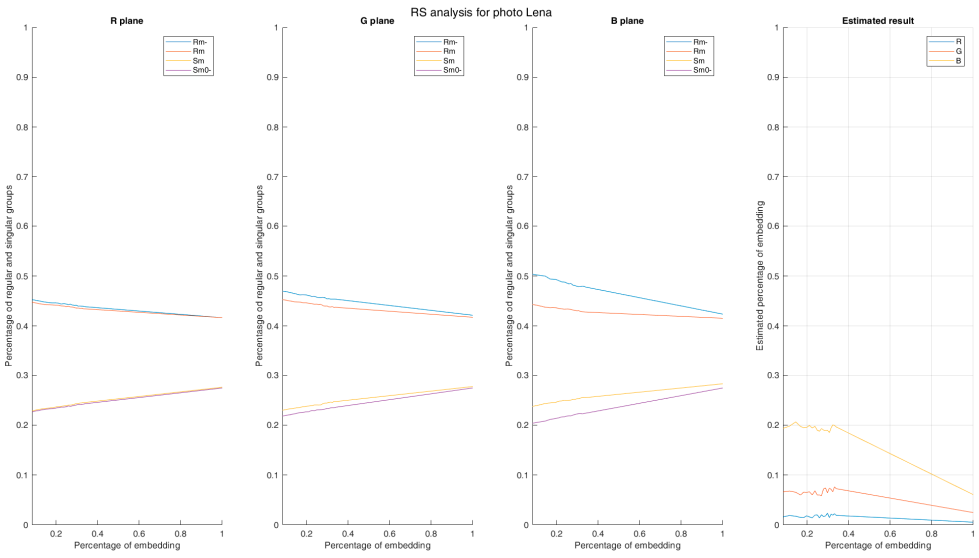

Figure 14. Diagrams of RS steganalysis for MDD stego-objects obtained from stego-carrier Lena.png.

Figure 15 shows histograms for stego-objects obtained by the classical LSB method, the MDD method as well as the PVD method. The histogram for the stego-object obtained by the classic LSB method has noticeable deviations from the histogram of the original stego-carrier, while the histogram of the stego-object obtained by the PVD method is the least distorted with the fact that this stego-object has approximately twice the capacity of the stego-object obtained by the MDD method.

In general, the classical steganographic LSB method leads to the quantization of the histogram in 8-K zones, where K is the number of LS bits that we change. This histogram behavior is very unfavorable in the context of stego-analysis. The MDD method shows better histogram behavior, with less distortion and no quantization effects, as shown in [18].

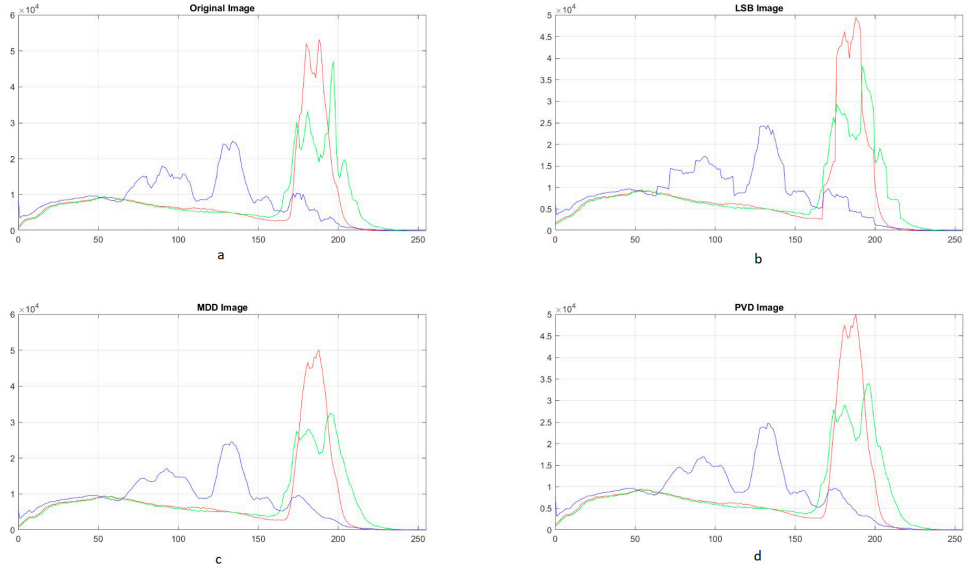

Figure 15. Histograms (RGB channels) for carrier Baboon.png: (**a**) Original Image; (**b**) Stego-Object generated using LSB method; (**c**) Stego-Object generated using MDD method; (**d**) Stego-Object generated using PVD method for Type 1, DC = 8, K = 3.

By performing steganographic procedures on certain areas of the carrier, the distortion of the histogram of stego-objects in relation to the original carrier is additionally reduced, and therefore the price is paid in the reduction in the capacity of the stego-carrier.

Figure 16 shows a significantly smaller distortion of the pixel difference histogram in MDD stego-objects where the steganography procedure is performed in areas compared to the case when the steganography procedure is performed over the entire image (red line).

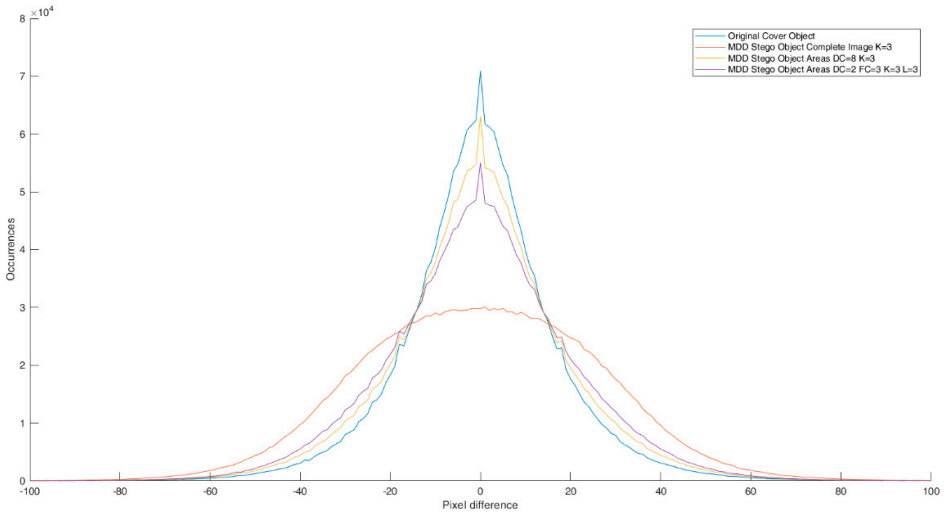

Figure 16. Pixel differencing histograms for carrier Lena.png: Blue Line–Original Cover Picture; Red Line–MDD Stego Object Complete Image K = 3; Yellow Line–MDD Stego Object Areas, T1, DC = 8, K = 3; Violet Line–MDD Stego Object Areas, T2, DC = 2, FC = 3, K = 3, L = 3.

For the purposes of comparison with related works and methods of adaptive steganography by other authors, Table 9 shows the capacity (expressed in percentages and in bpp) and PSNR values for different stego-objects, obtained with different input parameters proposed by the algorithm using different stego-carriers.

Table 9. Values of capacity and PSNR of stego-objects obtained for different input parameters of the algorithm over stego carriers Baboon, Lena, Nature1, Nature2.

Picture	Baboon		Lena		Nature1		Nature2		Average	
	Cap [%/bpp]	PSNR [dB]	Cap [%/bpp]	PSNR [dB]	Cap [%/bpp]	PSNR [dB]	Cap [%/bpp]	PSNR [dB]	Cap [%/bpp]	PSNR [dB]
DC = 2, K = 3	29.1/ 6.98	41.79	19.3/ 4.61	43.2	35.1/ 8.42	39.6	13.3/ 3.19	44.77	24.4/ 5.86	42.34
DC = 4, K = 3	17.1/ 4.1	44.11	14.2/ 3.41	44.48	22.0/ 5.28	41.26	6.69/ 1.61	47.92	14.99/ 3.6	44.44
DC = 6, K = 3	16.6/ 3.98	44.23	10.8/ 2.59	45.95	13.9/ 3.34	43.41	4.67/ 1.12	49.39	11.49/ 2.76	45.745
DC = 8, K = 3	11.4/ 2.74	45.96	6.91/ 1.66	47.81	11.4/ 2.74	44.03	4.51/ 1.08	49.52	8.56/ 2.05	46.83
FC = 2, K = 3, L = 3	20.20/ 4.85	43.38	16.3/ 3.91	43.93	31.2/ 7.49	40.17	5.19/ 1.25	49.16	18.22/ 4.37	44.16
FC = 3, K = 3, L = 3	16.5/ 3.96	44.24	12.7/ 3.05	45.07	21.5/ 5.16	41.33	8.64/ 2.07	46.92	14.83/ 3.56	44.39
FC = 4, K = 3, L = 3	19.3/ 4.61	43.57	14.0/ 3.36	44.88	27.4/ 6.58	40.97	9.2/ 2.21	46.6	17.48/ 4.2	44.0

The results from Table 9, in the first case, will be compared with the results from Table 10. Table 11 represents the sublimated last row (average values) of Table 3 from [7] where the capacities are expressed in percentages by the ratio of the number of embedded bits to the total number of image bits (having given that the authors used images with a size of 512 × 512 pixels) while the PSNR values were kept in the original format. So, for example, for 2,385,386 imprinted bits, the capacity is 2,385,386/(512 × 512 × 3 × 8) = 0.3791—that is, 37.91%.

Table 10. Average values of capacity and PSNR on a sample of 8 images for Khodaei and Faez and for Gandharba Swain method of adaptive steganography.

Khodaei and Faez (Type 1), K = 3		Khodaei and Faez (Type 2), K = 3		Gandharba Swain (Type 1), K = 3		Gandharba Swain (Type 2), K = 3	
Cap [%]	PSNR [dB]	Cap [%]	PSNR [dB]	Cap [%]	PSNR [dB]	Cap [%]	PSNR [dB]
37.9	39.81	39%	38.29	37.6	40.44	39.6	39.29

It is clearly observed that the stego-objects obtained by the Khodaei and Faez method as well as by the G. Swain method have higher capacities and significantly worse PSNR values compared to the values of the proposed method shown in Table 9. Trying to make a comparison between the results shown, we suggest beginning by focusing on the fifth row of Table 9 and the obtained average values of 18.22% for capacity and 44.16 dB for PSNR. This result was chosen because 18.22% represents approximately twice the capacity of Khodaei and Faez and G. Swain in Table 10. From the example, it can be seen that for stego-objects with twice the capacity, the proposed method gives a PSNR value that is more than 4 dB higher than the value obtained by Khodaei and Faez and slightly less than 4 dB higher than the value obtained by the method of Gandharba Swain.

Table 11. Comparison of values of capacity and PSNR between Chen and Ioannidou, Halkidis, Stephanides methods.

Chen et al. method	Cap (%)/bpp	2.71/0.65
	PSNR (dB)	47.1
I.H.S.–Laplacian OR fuzzy RNG step 1,2,3	Cap (%)/bpp	3.89/0.93
	PSNR (dB)	46.88
I.H.S.–Laplacian OR fuzzy RNG step 1,2	Cap (%)/bpp	5.23/1.26
	PSNR (dB)	46.88
I.H.S.–Laplacian OR fuzzy NO RNG	Cap (%)/bpp	7.89/1.89
	PSNR (dB)	45.12
I.H.S.–Sobel OR fuzzy RNG step 1,2,3	Cap (%)/bpp	3.87/0.93
	PSNR (dB)	45.91
I.H.S.–Sobel OR fuzzy RNG step 1,2,	Cap (%)/bpp	5.2/1.25
	PSNR (dB)	46.88
I.H.S.–Sobel OR fuzzy NO RNG	Cap (%)/bpp	7.8/1.88
	PSNR (dB)	44.45

A direct comparison will be performed with the results of the method of A. Ioannidou, S. T. Halkidis and G. Stephanides presented in [9]. Table 11 is a sublimation of Table 1 from [9] in which the authors provide a comparison of their results with the method proposed by Chen in [20]. As in the previous case, in Table 11 the capacities of the carrier are expressed in percentages, bearing in mind that the authors Ioannidou, Halkidis and Stephanides used images with a size of 128 × 128 pixels.

Table 11 shows low stego-carrier capacity values expressed in percentages as well as in bpp, on the one hand, and solidly high PSNR values, on the other hand. By comparing the bpp and PSNR ratio from Table 9, the stego objects obtained by the proposed method in this paper and the values from Table 11, it is clearly seen that the capacity obtained by our proposed method is significantly higher for similar PSNR values. So, for example, if we focus on the penultimate row in Table 9 for the stego-carrier Nature2, we see that with a similar value of PSNR (46.92 dB) we obtain a significantly higher capacity–2.07 bpp, while with the I.H.S. method that value is significantly lower—1.26 bpp.

An interesting algorithm based on hybrid edge detection is presented in the paper [21]. The results presented in this paper show extremely high PSNR values (Table 1) at the cost of some capacity reduction expressed in bpp (Table 2). Table 12 shows a comparison of the results obtained in the experiments, showed in Table 9, with several results from [21] (cover image–Lincoln, hidden image–Barbara, Cameraman).

Table 12. Comparison of the results of average values from Table 9 with the results presented in [21] in Tables 1 and 2.

Average Values (Table 9)		**LSB-PVD-EMD**		**Vernam Algorithm**		**Dhawan and Gupta**	
Cap [bpp]	**PSNR [dB]**	**Cap [bpp]**	**PSNR [dB]**	**Cap [bpp]**	**PSNR [dB]**	**Cap [bpp]**	**PSNR [dB]**
2.76	45.745	2.309	46.597	2.309	45.919	2.309	48.706
2.05	46.83	0.722	48.815	0.722	48.438	0.722	51.548

It is observed that the results obtained by the proposed method are comparable and similar to the results presented in [21] in the terms of the ratio of quality and capacity expressed through PSNR and bpp.

When it comes to the resistance of the proposed method to different types of attacks such as cropping, compression, filtering or noise addition, it should be kept in mind that the complete system is made up of two independent parts: the algorithm for selecting the stego area and the implemented stego method. Different steganographic methods provide different degrees of robustness of stego objects and resistance to image sterilization processes. Some sterilization techniques are presented in [22–24]. As the MDD method belongs to the category of LSB steganography (in spatial domain), it is not resistant to different types of attacks or the sterilization of the stego object. On the other hand, if the stego area selection algorithm were to be combined with another steganographic method more resistant to attacks (such as the steganography methods in frequency domain [3]), it is to be expected that such a system would show improvements in the context of security, which can be the subject of further research. However, considering the application of this system for higher levels of protection, each detection of any kind of attack attempt entails a change in the communication channel.

8. Conclusions

On the basis of the proposed experiment, the tests performed, the results obtained and the analysis carried out, the justification of performing steganography in the selected areas was proven. In addition to increasing the safety of the stego-process itself, it was shown how the desired quality of stego-objects is achieved by degrading the capacity of the carrier. Furthermore, the method of selecting the input parameters of the algorithm, depending on the performance of the carrier, is shown in order to achieve the appropriate capacity/quality ratio. The introduction of additional filtering of pixels within a specific cluster open up a much wider range of possibilities in the way of setting the input parameters in order to achieve the desired effects. Section 7 shows the validity of the assumption presented in the previous sections. In fact, it has been shown that by using a different number of bits for the steganography process in areas of similar colors and hues, steganographic areas containing several different colors can have their advantages for appropriately chosen input parameters of the algorithm. Finally, the dominance of the MDD method over the PVD method is shown. The MDD method in most cases gives better performance as well as the possibility of choosing the LS bits that we influence (K and L). The PVD method showed that there is no difference in performing the stego-process in areas of similar colors or in "colorful" areas. For that reason, the PVD method should be chosen in situations where high quality of the stego-object is important for low capacity values. A high degree of resistance of MDD stego-objects to the process of steganalysis is shown. By comparing the capacity parameters and PSNR values with the values obtained by the authors of similar adaptive steganography methods, the competitiveness of the proposed method was proven.

It is important to note that the basic idea of this approach to the problem has already found its application in several current projects, i.e., systems for secure file exchange, where after the data encryption process, such a hybrid process of steganography is implemented in order to overcome the problem of banning the use of encrypted files on some mail services and clouds (vPCP-FC) [25]. In order to be practically applied in a software solution, the described algorithm must satisfy the following limitations: the maximum number of rectangles on one carrier must be defined, as well as the minimum size of the stego-surface expressed in pixels or as a percentage of the total size of the carrier, in advance.

The disadvantages of this approach can be considered as increased complexity of the system, time required to execute the algorithm for selecting stego-areas, reduced capacity of carriers, the need for an additional method for transmitting information about the number and positions of the stego-area.

Finally, an idea for further work and research could be the implementation of several more steganographic methods of different categories, as well as the creation of a feedback loop in the system (Figure 1 shows the red dotted line). Such feedback would enable the system to select the stego-area, stego-method and stego-process parameters for the

appropriate carrier, desired capacity and quality of stego-objects. In addition, combining the proposed algorithm for area selection with more robust steganographic methods could be the subject of further research in order to create stego objects more resistant to stego attacks as well as the sterilization process. Another branch of the approach to the problem could be reflected in the development of a more advanced algorithm for selecting stego-areas, where the areas of the carrier, in which the secret content would be imprinted, have some other regular geometric shape or even an irregular geometric shape. One of the results of the proposed algorithm for the selection of the stego area, based on the homogenization of the parts of the carrier, can be the detection of typical shapes, objects and contours. As algorithms based on deep learning techniques presented in [26] have the same goal, one of the directions of further research could be to combine these techniques.

Author Contributions: Conceptualization, P.M. and M.M.; methodology, M.M. and P.M.; software, P.M.; validation, P.M., M.M. and Z.B.; formal analysis, P.M.; investigation, P.M.; resources, Z.B.; data curation, P.M.; writing—original draft preparation, P.M.; writing—review and editing, Z.B. and M.M.; visualization, P.M.; supervision, Z.B.; project administration, P.M.; funding acquisition, Z.B. All authors have read and agreed to the published version of the manuscript.

Funding: This paper is an outcome of activities under project Prj_122 vPCWD supported by Vlatacom Institute of High Technologies, Belgrade, Serbia.

Data Availability Statement: Data available on request from the authors.

Conflicts of Interest: The authors declare no potential conflict of interests.

References

1. Ramakrishnan, S. *Cryptographic and Information Security Approaches for Images and Videos*; CRC Press: Boca Raton, FL, USA, 2020.
2. Kaur, R.; Kaur, B. A Study and Review of Techniques of Spatial Steganography. *Int. J. Sci. Res. (IJSR)* **2015**, *4*, 3198–3203.
3. Cheddad, A.; Condell, J.; Curran, K.; Mc Kevitt, P. Digital image steganography: Survey and analysis of current methods. *Signal Process.* **2010**, *90*, 727–752. [CrossRef]
4. Hussain, M.; Wahab, A.W.A.; Bin Idris, Y.I.; Ho, A.T.; Jung, K.-H. Image steganography in spatial domain: A survey. *Signal Process. Image Commun.* **2018**, *65*, 46–66. [CrossRef]
5. Khodaei, M.; Faez, K. New adaptive steganographic method using least-significant-bit substitution and pixel-value differ-encing. *IET Image Process.* **2012**, *6*, 677–686. [CrossRef]
6. Khodaei, M.; Bigham, B.S.; Faez, K. Adaptive Data Hiding, Using Pixel-Value-Differencing and LSB Substitution. *Cybern. Syst.* **2016**, *47*, 617–628. [CrossRef]
7. Swain, G. A Steganographic Method Combining LSB Substitution and PVD in a Block. *Procedia Comput. Sci.* **2016**, *85*, 39–44. [CrossRef]
8. Hussain, M.; Wahab, A.W.A.; Javed, N.; Jung, K.-H. Hybrid Data Hiding Scheme Using Right-Most Digit Replacement and Adaptive Least Significant Bit for Digital Images. *Symmetry* **2016**, *8*, 41. [CrossRef]
9. Ioannidou, A.; Halkidis, S.T.; Stephanides, G. A novel technique for image steganography based on a high payload method and edge detection. *Expert Syst. Appl.* **2012**, *39*, 11517–11524. [CrossRef]
10. Hamid, N.; Yahya, A.; Ahmad, R.B.; Al-Qershi, O.M. A comparsion between using SIFT and SURF for characteristic region based image steganography. *Int. Juurnal Comput. Sci. Issues (IJCSI)* **2012**, *9*, 110–116.
11. Manikandan, G.; Krishnan, R.B.; Kumar, N.R.; Narasimhan, D.; Srinivasan, A.; Raajan, N.R. Steganographic approach to enhancing secure data communication using contours and clustering. *Multimedia Tools Appl.* **2018**, *77*, 32257–32273. [CrossRef]
12. Practical Steganalysis of Digital Images-State of the Art-Researchgate (No Date). Available online: https://www.researchgate.net/publication/2534088_Practical_Steganalysis_of_Digital_Images_-_State_of_the_Art (accessed on 26 October 2022).
13. Fridrich, J.; Goljan, M.; Du, R. Detecting LSB steganography in color, and gray-scale images. *IEEE Multimed.* **2001**, *8*, 22–28. [CrossRef]
14. Sara, U. Comparative Study of Different Quality Assessment Techniques on Color Images. *Iconic Res. Eng.* **2019**, *2*, 127–133.
15. Divya, A.; Thenmozhi, S. Steganography: Various Techniques In Spatial and Transform Domain. *Int. J. Adv. Sci. Res. Manag.* **2016**, *1*, 81–89.
16. Sara, U.; Akter, M.; Uddin, M.S. Image Quality Assessment through FSIM, SSIM, MSE and PSNR—A Comparative Study. *J. Comput. Commun.* **2019**, *7*, 8–18. [CrossRef]
17. Wu, D.-C.; Tsai, W.-H. A steganographic method for images by pixel-value differencing. *Pattern Recognit. Lett.* **2003**, *24*, 1613–1626. [CrossRef]

18. Milosav, P.; Banjac, Z.; Unkašević, T.; Milosavljević, M. Minimal Decimal Difference Method Applied in Spatial Image Steganography. In Proceedings of the 2020 19th International Symposium INFOTEH-JAHORINA (INFOTEH), East Sarajevo, Bosnia and Herzegovina, 18–20 March 2020.
19. Milosav, P.; Milosavljević, M.; Banjac, Z. Stego-Objects Metrics Improvement Using the Method of Minimal Decimal Difference in Spatial Image Seganography. *J. Mechatron. Autom. Identif. Technol.* **2020**, *5*, 19–25.
20. Chen, W.-J.; Chang, C.-C.; Le, T.H.N. High payload steganography mechanism using hybrid edge detector. *Expert Syst. Appl.* **2010**, *37*, 3292–3301. [CrossRef]
21. Dhawan, S.; Gupta, R. High-quality steganography scheme using hybrid edge detector and Vernam algorithm based on hybrid fuzzy neural network. *Concurr. Comput. Pract. Exp.* **2021**, *33*, e6448. [CrossRef]
22. Geetha, S.; Subburam, S.; Selvakumar, S.; Kadry, S.; Damasevicius, R. Steganogram removal using multidirectional diffusion in fourier domain while preserving perceptual image quality. *Pattern Recognit. Lett.* **2021**, *147*, 197–205. [CrossRef]
23. Ganguly, S.; Mukherjee, I. Image Sterilization through Adaptive Noise Blending in Integer Wavelet Transformation. In Proceedings of the 2022 IEEE 19th India Council International Conference (INDICON), Kochi, India, 24–26 November 2022. [CrossRef]
24. Mukherjee, I.; Paul, G.; Jawahar, J.A. Defeating Steganography with Multibit Sterilization Using Pixel Eccentricity. *IPSI BgD Internet Res. Soc.* **2015**, *11*, 25–34.
25. Available online: https://www.vlatacominstitute.com/encryption-authentication (accessed on 13 April 2023).
26. Kumar, V.; Sharma, S.; Kumar, C.; Sahu, A.K. Latest Trends in Deep Learning Techniques for Image Steganography. *Int. J. Digit. Crime Forensics* **2023**, *15*, 1–14. [CrossRef]