Minimal Decimal Difference Method Applied in Spatial Image Steganography

Predrag Milosav, Zoran Banjac, Tomislav Unkašević
Vlatacom Institute
Belgrade, Serbia
predrag.milosav@vlatacom.com,
zoran.banjac@vlatacom.com,
tomislav.unkasevic@vlatacom.com

Milan Milosavljević
Singidunum University
Belgrade, Serbia
mmilosavljevic@singidunum.ac.rs

Abstract—**This paper deals with the improved method of spatial image steganography - Minimal Decimal Difference Method. The basic LSB method, as a starting point, was improved, an implementation algorithm was proposed and developed, and then measurements were made and results were processed. The benefits achieved by the advanced method in comparison with the classical LSB (Least Significant Bit) method are presented graphically and numerically and further research and development is proposed in order to achieve even better results.**

Keywords-Spatial Image Steganography, LSB, Histogram, Image Processing, MSE, PSNR, SSIM.

I. INTRODUCTION

The word Steganography is derived from the Greek origin and means "concealed writing" from the Greek words *steganos* meaning "covered or protected", and *graphein* meaning "to write." The first recorded use the term is 1499 Johannes Trithemius in his Steganographia. Different types of steganography and the method of hiding a secret message have been used throughout history, sometimes combined with cryptography methods, and in the last few years steganography has again come into the focus of research. In line with the advancement of computer and communication technologies, the increasing processing power of computers, the development of neural networks and deep learning, every day more and more powerful smart systems for traffic analysis are being developed. Such systems installed at large telecommunication hubs handle an enormous amount of traffic daily. With the increase of the power of such systems, the need for the development of new steganographic techniques, the improvement of the existing ones, the improvement of their robustness and resilience to the tools for stego-analysis as well as to the stego-attacks. In Section II, a basic classification of steganographic algorithms will be presented, while in Section III some of the tools and metrics for image quality assessment will be discussed taking into account that proposed method is based on steganography in this media type. Section IV will propose an enhancement of the basic steganography algorithm in the spatial domain, and Section V will describe the measurement performed, the results presented and commented on. Section VI is slated to conclusion.

II. CLASSIFICATION OF STEGANOGRAPHIC TECHNIQUES

For a technique considered steganographic, there are 4 required elements [1]:

- **Cover Object**: Original objects which are used as a carrier for conceal the information, usually called Carrier.
- **Message**: Secret information we want to hide.
- **Stego Object:** After embedding message or secret information into cover object is known as stego-object.
- **Stego Key:** A key (algorithm) is used for embedding or extracting the messages to Cover Object and from Stego Object.

As the subject of this paper is image steganography, it is clear that Cover Object as well as Stego-object will be image in pngor some other image format.Since steganography can be considered to be a process that is applied after the process of encryption of a secret message, we will assume that the content being imprinted into the carrier has the properties of a random binary array.Stego-Key, actually the algorithm is what will actually be the focus of this paper. The goal of each steganographic algorithm is to achieve better process performance: less perceptibility, greater capacity, greater resistance to stego-analytic tools and attacks, greater robustness of the stego-object, better performance expressed in numerical values to evaluate carrier quality, less processing time required for embedding and extracting secret content.

Steganographic algorithms can be classified in different ways and the common one domain-based.

Classification based on algorithm type

There are two basic approaches in developing and implementing image steganography algorithms: Frequency Domain Techniques and Spatial Domain Techniques, [2].

A. Frequency Domain Techniques

These techniques are based on message coding in frequency domain of the carrier. The frequency domain data embedding

method is widely used for robust watermarks, [2]. A similar technique can be used to imprint content for steganographic purposes.In order to transform a carrier from a spatial domain into a frequency one of 3 suitable transformations is used: Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT) and Discrete Fourier Transform (DFT), [2]. By embedding in frequency domain, the hidden data are in more robust conditions, spread throughout the entire image and providing better resistance to signal processing. Embedding of secret information is based on a change in the corresponding coefficients in the frequency domain. Because of the robustness properties of frequency domain embedding, these techniques are generally more applicable to the "Watermarking" aspect of data hiding, [1].

B. Spatial Domain Techniques

Steganography in the spatial domain involves the manipulation of raw bits in a digital record of a carrier. In the case of image steganography, manipulation of raw bits involves changing individual bits of pixels, whether it is a grayscale image or a colour image. The study in [3] gave an excellent theoretical overview of different techniques in the spatial domain, the peculiarities of each of them as well as comparative characteristics, advantages and disadvantages.Steganography techniques in the spatial domain can be divided into several basic categories:

1. LSB Steganography
2. RGB Based Steganography
3. Pixel Value Differencing Steganography
4. Mapping Based Steganography
5. Pallete Based Steganography
6. Collage Steganography
7. Spread Spectrum Steganography
8. Code Based Steganography

Each of these categories contains several specific algorithms explained and detailed in [3]

III. STEGANOGRAPHY METHODES EVALUATIONS

The increasing need to use steganography has led to the development of different algorithms. In order to accurately characterize the efficiency of the algorithms, it was also necessary to define different evaluation methods and metrics that clearly quantify their quality. The visual quality metrics described in [4] attempt to numerically represent Stego-object distortions that may be visible to the human eye. It is very difficult to define whether standard measurement techniques can assess the level of visual modification to decide whether the steganographic method is perceptually transparent or not, [5].The literature distinguishes between two types of visual image quality metrics, [4]:

1. *Non-Blind* methods are based on the mathematical calculation of the difference between input image (Carrier Image) and output image after imprinted content (Stego-Object). It is clear that such mathematical tools require both images - basic and steganographically modified - as input arguments.
2. *Blind methods* do not require the original image as a reference for mathematical calculations, but their estimation is based on shape recognition statistics, where the applied algorithm is based on neural network and deep learning and is pre-trained.

The methods for assessing the quality (image quality assessment - IAQ) and computing the individual metrics applied in this paper are as follows:

- **MSE** - Mean Square Error (Non-Blind IAQ)

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

where C_i is carrier pixel value, S_i is stego pixel value and $H \times W$ represent the height and width of the carrier image. Lower values considered better.

- **RMSE** – Root Mean Square Error (Non-Blind IAQ)

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

- **SNR** – Signal to Noise Ratio (Non-Blind IAQ)

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

- **PSNR** – Peak Signal to Noise Ratio (Non-Blind IAQ)

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

Where *Max* is maximum pixel intensity value that is 255.

- **SSIM** – Structural Similarity Index (Non-Blind IAQ). An image quality metric that assesses the visual impact of three characteristics of an image: luminance, contrast and structure.

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

Where $\mu_x, \mu_y, \sigma_x, \sigma_y$ and σ_{xy} are the local means, standard deviations and cross-covariance for images x,y.

- **BRISQUE** - Blind/Referenceless Image Spatial Quality Evaluator. Calculates the no-reference image quality score for image.BRISQUE compare input image to a default model computed from images of natural scenes with similar distortions. A smaller score indicates better perceptual quality.
- **NIQE** – Naturalness Image Quality Evaluator - Blind/Referenceless. NIQE measures the distance between the NSS-based features calculated from input image to the features obtained from an image database used to train the model. The features are modelled as

multidimensional Gaussian distributions.

The aim of this paper is to demonstrate enhancement of proposed steganography method in spatial domain through the metrics and numerical parameters of image quality assessment, in addition to the subjective visual experience of the modified carrier enhancement.In this paper, we did not address the methods of stego-analysis over the obtained stego-objects. The stego-analysis of the proposed method, its numerical results and comparison with the results of other steganographic methods may be the subject of some future work. The MatLab software package and corresponding functions were used to calculate all the metrics listed.

IV. Proposed Algorithm of Minimal Decimal Difference

The standard LSB method of spatial image steganography involves changing the *k* bit of the less significant value of individual image pixel p_i. Suppose we have a secret message *M* composed of *n* bits that we want to send in a steganographic carrier by modifying the *k* bits of each pixel. The LSB method requires sequentially extracted *k* bits from *M* that will be embedded into the corresponding pixel of the carrier p_i. Let us denote this combination of bits with m_k. By embedding m_k (*k* bits) into each pixel, the *8-k* MSB bits of each pixel will retain their original value. Such an operation requires

$$i_{max} = \begin{cases} n \div k, n \bmod k = 0 \\ n \div k + 1, n \bmod k > 0 \end{cases} \quad (6)$$

pixels, where ÷ represents an integer division operation and *mod* represents rest of an integer division operation. We can perform a similar process using an RGB image and in that case we would change *k* bits in each of the 3 channels. Then

$$i_{max} = \begin{cases} n \div (k * 3), n \bmod k = 0 \\ n \div (k * 3) + 1, n \bmod k > 0 \end{cases} \quad (7)$$

pixels are required to transmit the desired *n* bit length information. For such an algorithm, *k* LSB bits for each of the modified pixel (or channels) p_i'on the receiving side need to be read in sequence according to the pattern of pixels used on the transmitting side. If the steganography process is not carried out over the entire surface of the image (using all pixels), it is necessary to transmit, via an alternative channel or in the form of some header, information which pixels were used as carriers of the classified information. In addition to its good properties, this method has several disadvantages and one of them is a significant increase in distortion with increasing *k* value. So the biggest decimal difference in the pixel values before and after changing the *k* LSB bit is $d_{max} = 2^k - 1$ .The method of minimum decimal difference (MDD) is based on the idea of reducing the d_{max}coefficient as much as possible. Unlike the classic LSB method, which did not take into account the decimal value of the original pixel, the MDD method takes this value into account and changes the original pixel value by adding an appropriate coefficient d_i (positive or negative) with the aim that binary representation of the new obtained decimal value for the last *k* The LSB bit has the $m_k$value that we want to transmit. With this approach, we can calculate the minimum and maximum values of the coefficients depending on the number *k*:

$$-2^{k-1} + 1 \leq d_i \leq 2^{k-1} \quad (8)$$

For example: if the value of *k = 3*, for the classical LSB method, the decimal difference of the original and modified pixels can range: $0 \leq d_i \leq 7$, while it is: $-3 \leq d_i \leq 4$ for MDD. Therefore, the expected benefit of MDD is a smaller distortion of the stego-object that will be reflected in the numerical values of the *MSE* and *PSNR* parameters as well as in the visual experience of the image. Such an idea can have many different software implementations and one of them is the introduction of an additional function that will calculate the coefficient d_i for the corresponding *k* bit combinations we want to transmit, m_k, and the original decimal pixel values. The pixel value to be sent is the result of the sum of the original decimal pixel value and the calculated coefficient: $p_i' = p_i + d_i$. In the case of transmission of *k* = 2 bits in each pixel p_i, the functionality of such a software component may also be displayed in a Table I where by columns are combinations of 2 bits of the secret message m_k, and by rows of combination the last 2 bits of the binary representation of original pixel values p_i.

TABLE I.Coefficients $\boldsymbol{d_i}$ for 2 bits combinations of message to transmit $\boldsymbol{m_k}$ by columns and last 2 bits of current pixel values $\boldsymbol{p_i}$ by rows

	00	**01**	**10**	**11**
00	0	+1	+2	-1
01	-1	0	+1	+2
10	+2	-1	0	+1
11	+1	+2	-1	0

Similar tables like Table I, (sizes $2^k \times 2^k$), can be created for other values of the k bits we want to transmit.

Pixel Decimal Values in Boundary Regions

Bearing in mind that the value of each pixel p_i can be in the range 0-255, and the value of the coefficients added, d_i, can be both positive and negative, it is necessary to solve the problem of boundary regions. The solution to this problem is to scale all the values of p_i from the edge of the interval to the first, closest, acceptable value p_{im}depending on the possible values of d_i, that depends on number k:

$$p_{im} = \begin{cases} 2^{k-1} - 1, p_i < 2^{k-1} - 1 \\ p_i, 2^{k-1} - 1 \leq p_i \leq 255 - 2^{k-1} \\ 255 - 2^{k-1}, p_i > 255 - 2^{k-1} \end{cases} \quad (9)$$

Equation (9) clearly shows that the boundary regions will increase with the increase of the coefficient k and the performance of the MDD algorithm will, in the worst case, be equal to the performance of the classical LSB method.

The extraction of the bits on the receiving side is performed in the same way as in the basic method - by sequential reading of k LSB bits from the i_{max} modified pixels of a Stego-object.

It should be noted that Goljan-Holotyak [6], which adds positive and negative values to the existing decimal pixel value, as well as Van Dijk - Willems [7] dealing with pre-coding of secret bits had similar ideas for how to modify k LSB bits, which for some codes can have a similar effect as well as the MDD method.

V. Description of The Measurement Process and Sorting of The Results Obtained

Testing was performed on 50 different images from which four colour images were selected for analysis: Baboon.png, Colors.png, Lena.png and Sunset.png, Fig1.

Figure 1. Baboon.png, Sunset.png, Lena.png, Colors.png.

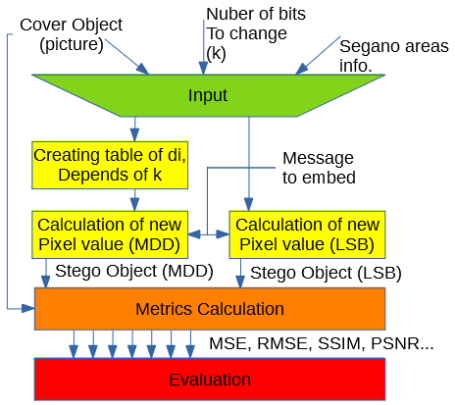

Figure 2. Block diagram of proposed algorithm

The concept of described algorithm is shown as block diagram in the Figure 2.

The parameters of each image (size, resolution, BRISQUE and NIQE values) are shown in the TableII. - Table V. with complete measurement results. For each of these images, six tests were performed using both methods, LSB and MDD. These six tests include the following:

1. Performing Steganography over entire image changing 3 bits for every channel, for every pixel (Table II. to Table V. Method - M1).
2. Performing Steganography over entire image changing 4 bits for every channel, for every pixel(Table II. to Table V. Method - M2).
3. Performing Steganography over entire image changing 5 bits for every channel, for every pixel(Table II. to Table V. Method - M3).
4. Performing Steganography in chosen areas of the image changing 3 bits for every channel, for every pixel (Table II. to Table V. Method - M4).
5. Performing Steganography in chosen areas of the image changing 3 bits and 4 bits for every channel, for every pixel (Table II. to Table V. Method - M5).
6. Performing Steganography in chosen areas of the image changing 3 bits and 5 bits for every channel, for every pixel (Table II. to Table V. Method - M6).

Mentioned areas in each image are selected in the form of a rectangles, such that k=3 bits are changed in areas containing one dominant shade of the corresponding colour, and more bits (k=4, k=5) are changed in areas containing more than one colour.

Figure 3. Areas for embedding content; Red k=3 bits, Green k=5 bits

This principle was adopted in order to increase the security, reduce the readability of the changes made on the carrier and at the cost of the reduced capacity of the carrier, Fig 3. For the purposes of analysing and implementing both algorithms, special software is written in the C++ programming language, which generates random content and then embed it into the carrier, whether it is the entire surface of the image or only selected areas. The developed software automatically calculates the capacity of each carrier for the appropriate scenario of steganography application, which in this test ranges from 7.92% to 62.50%.

By calculating the above metrics from Section III, it can be seen that the SNR and PSNR parameters decrease by 6dB each with the increase in the number of bits we transmit, k. It is also

shown in all the tests performed that the gain of the MDD method comparing to the LSB method is approximately 3dB. Typical values for the PSNR in lossy image compression/transmission are between 30 and 50 dB, provided the bit depth is 8 bits, where higher is better. Acceptable quality is considered for any Stego-Object where the PSNR parameter has a value greater than 40dB. The tabulated results show that the MDD method for multiple scenarios (M1-M6) satisfies this condition, in more cases then LSB method.

If we compare the values of MSE and RMSE calculated for both methods, we see that$RMSE_{LSB} \approx 1.34 RMSE_{MDD}$, which even numerically proves less distortion of Stego-Object using MDD method compared to LSB.

Comparing the values of SSIM, one can conclude that the MDD method has up to 10% better results by applying steganography to the entire surface of the image and up to 2% better results by applying steganography to particular areas of the carrier. For applying steganography by MDD method in certain areas of the image, SSIM > 0.95 which is an excellent score and shows the quality of the chosen concept. The analysis of the presented results clearly shows that in the LSB method SSIM < 0.95 in 33% of cases, while in the MDD method this SSIM < 0.95 in 25% of cases.

By analysing BRISQUE and NIQE parameters it follows that better scores (lower values) were obtained for tests where we perform steganography only in certain areas of the image. It is also interesting that better values are obtained for the LSB method, where we perform greater image distortion in areas with similar shades of colour.

For the purposes of computing histograms and metrics from Section III, the Matlab software package was used, and the results are shown in Table II. - Table V. as well as Figure 4.to Figure 6. Furthermore, the histograms for the original Baboon.png image (Figure 4.) and the histograms of the full-image steganography (Figure 5.) are compared using basic LSB method (3 bits, 4 bits, 5 bits) and the Figure 6. is histograms using MDD method (3 bits, 4 bits, 5 bits).

TABLE II.MEASUREMENT RESULTS OBTAINED USING BABOON.PNG (2048X2048 RGB, ORIGINAL FILESIZE: 12MB, BRISQUE = 39.8224, NIQE = 3.3237)

Steganography Method	Method	Capacity[%]	Non Blind Methods					Blind Methods	
			MSE	RMSE	SNR[dB]	PSNR[dB]	SSIM	BRISQUE	NIQE
LSB Method	M1	37.50	10.50	3.24	28.93	37.92	0.97	31.03	5.25
	M2	50.00	42.35	6.51	22.88	31.86	0.88	25.98	7.54
	M3	62.50	169.28	13.01	16.86	25.84	0.70	40.07	10.18
	M4	7.92	2.23	1.49	35.66	44.64	0.99	37.08	3.17
	M5	8.96	4.91	2.22	32.23	41.22	0.98	34.45	3.11
	M6	10.00	15.56	3.94	27.23	36.21	0.97	29.38	3.10
MDD Method	M1	37.50	5.50	2.34	31.74	40.73	0.98	35.26	4.71
	M2	50.00	21.50	4.64	25.82	34.81	0.93	19.05	6.95
	M3	62.50	85.53	9.25	19.82	28.81	0.80	37.44	10.30
	M4	7.92	1.16	1.08	38.49	47.48	0.99	38.70	3.32
	M5	8.96	2.49	1.58	35.18	44.16	0.99	37.06	3.26
	M6	10.00	7.82	2.80	30.21	39.20	0.98	31.14	3.21

TABLE III.MEASUREMENT RESULTS OBTAINED USING SUNSET.PNG (2500X1875 RGB, ORIGINAL FILESIZE: 13.4MB, BRISQUE = 22.9667, NIQE = 3.0316)

Steganography Method	Method	Capacity[%]	Non Blind Methods					Blind Methods	
			MSE	RMSE	SNR[dB]	PSNR[dB]	SSIM	BRISQUE	NIQE
LSB Method	M1	37.50	10.50	3.24	31.87	37.92	0.96	27.49	6.47
	M2	50.00	43.11	6.57	25.73	31.79	0.86	42.68	9.00
	M3	62.50	169.36	13.01	19.79	25.84	0.67	43.78	11.59
	M4	17.60	4.91	2.22	35.16	41.22	0.98	9.39	3.36
	M5	18.90	8.23	2.87	32.92	38.98	0.96	8.36	3.36
	M6	20.20	20.21	4.50	29.02	35.08	0.94	9.55	3.37
MDD Method	M1	37.50	5.55	2.36	34.64	40.69	0.98	34.55	5.58
	M2	50.00	21.91	4.68	28.67	34.72	0.92	43.30	8.56
	M3	62.50	89.11	9.44	22.58	28.63	0.76	43.56	11.96
	M4	17.60	2.59	1.61	37.94	44.00	0.99	13.86	3.37
	M5	18.90	4.30	2.07	35.74	41.79	0.98	10.30	3.36
	M6	20.20	11.91	3.45	31.32	37.37	0.95	7.62	3.33

TABLE IV.MEASUREMENT RESULTS OBTAINED USING LENA.PNG (1960X1960 RGB, ORIGINAL FILE SIZE: 11MB, BRISQUE = 11.2498, NIQE=2.2135)

Steganography Method	Method	Capacity[%]	Non Blind Methods					Blind Methods	
			MSE	RMSE	SNR[dB]	PSNR[dB]	SSIM	BRISQUE	NIQE
LSB Method	M1	37.50	10.68	3.27	29.57	37.84	0.97	12.79	4.79
	M2	50.00	44.05	6.64	23.41	31.69	0.92	35.49	7.14
	M3	62.50	176.10	13.27	17.39	25.67	0.80	43.41	10.08
	M4	11.00	3.10	1.76	34.94	43.22	1.00	13.23	2.24
	M5	11.50	4.40	2.10	33.42	41.70	1.00	14.66	2.23
	M6	12.00	9.97	3.16	29.86	38.14	0.99	18.47	2.21
MDD Method	M1	37.50	6.03	2.46	32.05	40.33	0.98	16.03	4.18
	M2	50.00	24.76	4.98	25.92	34.19	0.94	33.42	6.79
	M3	62.50	103.95	10.20	19.68	27.96	0.85	43.45	10.35
	M4	11.00	1.62	1.27	37.76	46.04	1.00	8.48	2.30
	M5	11.50	2.30	1.52	36.23	44.51	1.00	10.22	2.28
	M6	12.00	5.14	2.27	32.74	41.02	0.99	14.70	2.25

TABLE V. MEASUREMENT RESULTS OBTAINED USING COLORS.PNG (2880X1800 RGB, ORIGINAL FILE SIZE: 14.8MB, BRISQUE = 36.3163, NIQE = 3.7577)

Steganography Method	Method	Capacity[%]	Non Blind Methods					Blind Methods	
			MSE	RMSE	SNR[dB]	PSNR[dB]	SSIM	BRISQUE	NIQE
LSB Method	M1	37.50	10.70	3.27	32.48	37.84	0.99	25.61	4.42
	M2	50.00	43.62	6.60	26.37	31.73	0.98	28.29	6.44
	M3	62.50	177.84	13.34	20.27	25.63	0.94	39.42	8.99
	M4	9.69	2.78	1.67	38.33	43.69	1.00	34.29	3.56
	M5	11.20	6.83	2.61	34.42	39.79	1.00	33.04	3.58
	M6	12.80	23.26	4.82	29.10	34.47	0.99	31.66	3.58
MDD Method	M1	37.50	6.14	2.48	34.89	40.25	1.00	28.10	4.02
	M2	50.00	25.49	5.05	28.71	34.07	0.99	26.06	5.65
	M3	62.50	109.85	10.48	22.36	27.72	0.96	35.43	8.52
	M4	9.69	1.64	1.28	40.61	45.97	1.00	34.42	3.53
	M5	11.20	4.00	2.00	36.75	42.11	1.00	33.94	3.57
	M6	12.80	14.24	3.77	31.23	36.60	0.99	32.24	3.58

The obtained results show that the LSB method quantifies histograms in the 2^{8-k}regions, while using the MDD method, histogram distortions exist but are not so noticeable especially in cases where the attacker does not have the original carrier image. By a similar comparative histogram test in cases of applied steganography in certain areas of the carrier, we can conclude that the distortions are even smaller and there is no quantization effect.

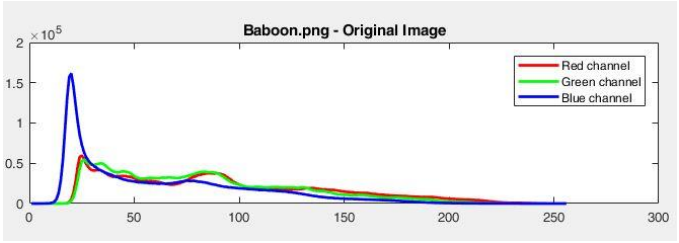

Figure 4. Histogram of original Baboon.png cover image

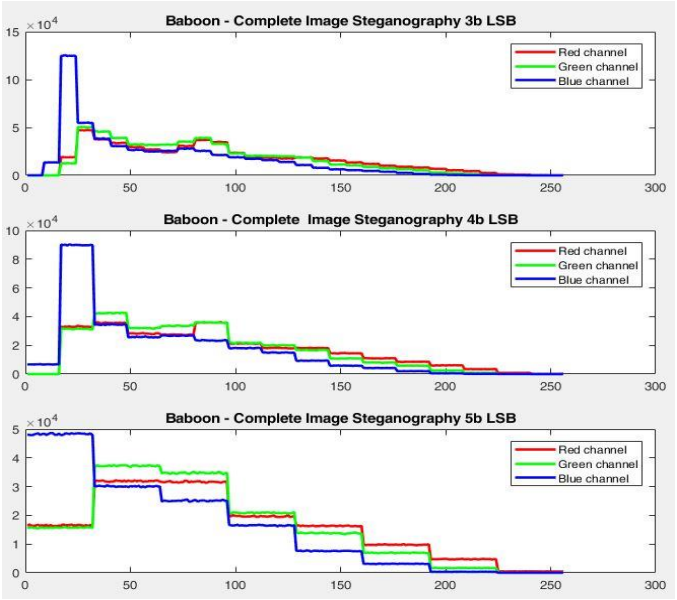

Figure 5. Histograms of stego-objects derived from Baboon.png using basic LSB method changing 3 LSB, 4 LSB and 5 LSB.

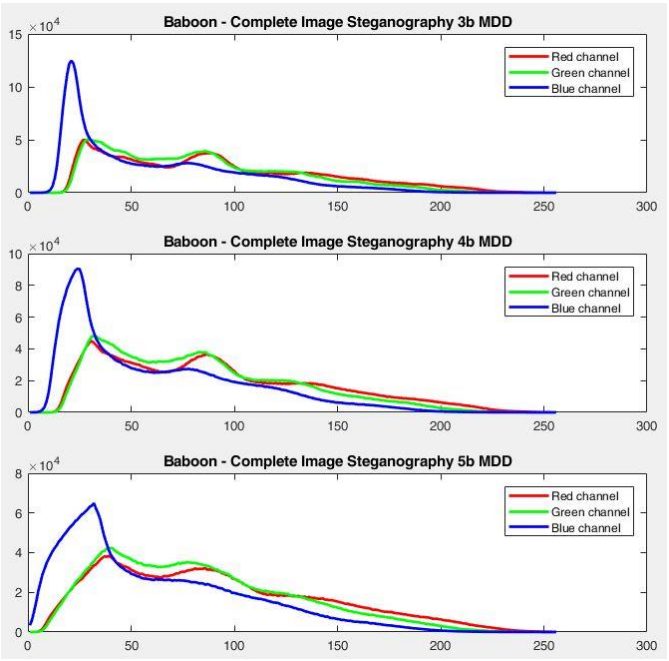

Figure 6. Histograms of stego-objects derived from Baboon.png using basic MDD method changing 3 LSB, 4 LSB and 5 LSB

In this case, the results obtained using the MDD method are even better and the histogram distortions are smaller. In papers [8] and [9], comparative characteristics of different steganographic methods in the spatial domain are described. If we refer to the MDD method where the content of all carrier pixels changes, we can consider that the results match the corresponding results of the methods described in [6] and [7]. Making changes in only certain parts of the carrier, as described above, may further contribute to the quality of the results obtained. All numerically obtained results as well as the generated full size images for each of the above methods can be obtained directly from the author of the paper upon request.

VI. CONCLUSION

In this paper, a hybrid method of spatial domain steganography is proposed and described. Comparative measurements and tests were conducted to prove the advantage of the proposed MDD (Minimal Decimal Difference Method) method over the basic LSB (Least Significant Bit) replacement method. For both methods, results were obtained and processed in the event that steganography is performed over the entire surface of the image (steganographic carrier) as well as when steganography is performed in certain, predefined, areas of steganographic carrier. Numerical comparative results as well as histograms were obtained using tools from the Matlab software package. The advantage of the MDD algorithm over LSB is unambiguously shown, as by the numerical values of the quality parameters, the subjective experiences of the visual quality of the altered carriers, and the level of histogram distortion. Particular contribution is made by the concept of steganography in particular areas of the carrier. With this methodology, in addition to enhancing security in the transmission of classified information, we also gain in every aspect of carrier image quality assessment, visual, numeric and histogram. In addition to some disadvantages of the steganography method over dedicated parts of the stegano-carrier (decreasing capacity of the carrier and a more complex algorithm for imprinting and extracting secret content), this paper also shows good features that this concept implies. Such results provide a good basis for continued research in the context of better selection of different carrier areas for steganography implementation, with the aim of increasing capacity while minimizing Stego-object distortion.

REFERENCES

[1] R. Kaur, B. Kaur, "A Study and Review of Techniques of Spatial Steganography",*International Journal of Science and Research (IJSR)*, vol. 4, no. 4, pp. 3198–3203, April 2015.

[2] G.S. Sravanthi, B.Sunitha Devi, S.M.Riyazoddin, M.Janga Reddy, "A Spatial Domain Image Steganography Technique Based on Plane Bit Substitution Method",*Global Journal of Computer Science and Technology*, vol. 12, no. 15, pp. 1-9, Nov 2012.

[3] G. Swain, S.R. Lenka, "Classification of Image Steganography Techniques in Spatial Domain: A Study", *International Journal of Computer Science & Engineering Technology (IJCSET)*, vol.5, no. 3, pp. 219-232, Mar 2014.

[4] M. Hussain, A. W. A. Wahab, Y. I. B. Idris, A. T. Ho, and K.-H. Jung, "Image steganography in spatial domain: A survey," *Signal Processing: Image Communication*, vol. 65, pp. 46–66, 2018.

[5] A. Yahya, "Steganography Techniques," *Steganography Techniques for Digital Images*, pp. 33–42, 2018.

[6] M. Goljan, J. Fridrich, and T. Holotyak, "New blind steganalysis and its implications," *Security, Steganography, and Watermarking of Multimedia Contents VIII*, vol. 6072, pp. 1-13, Feb. 2006.

[7] Van Dijk, M. and Willems, F.: Embedding information in grayscale images. *Proc. 22nd Symposium on Information and Communication Theory in the Benelux*, pp. 147-154, Enschede, The Netherlands, May 15-16, 2001.

[8] C.p, S. T, and U. G, "A Study of Various Steganographic Techniques Used for Information Hiding," *International Journal of Computer Science & Engineering Survey*, vol. 4, no. 6, pp. 9–25, 2013.

[9] A. Yahya, "Steganography Techniques for Digital Images," 2019.