International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-9 Issue-4, February 2020

Image Steganography by Modified Simple Linear Iterative Clustering

Ismail Kich, El Bachir Ameur, Youssef Taouil

Abstract: ***Steganography is an information security technique that consists of concealing secret data into digital medias including videos, texts, network protocols and images. In this paper, a steganography method to dissimulate the secret information in gray-scale images is proposed; the dissimulation is adapted to the cover image's texture, data is hidden in the edge areas. The edge pixels are selected by over-segmentation using Modified Simple Linear Iterative Clustering (M-SLIC). This algorithm allows to decompose the cover image into K regions which we call superpixels. The image's texture and the amount of the secret data are the factors that help to determine the value of the parameter K. Choosing the pixels of complex regions to conceal secret information is due to the fact that the human visual system is designed to notice changes in the pixels of smooth areas. Therefore, edge areas tolerate larger changes than smooth areas without causing detectable distortions. Experiment on a large set of images were carried out; results illustrate the good performance of the proposed work in terms of capacity, security and imperceptibility in comparison to recent works.***

Keywords: ***Steganography, Data hiding, Steganalysis, Superpixels, Edge detection, SLIC.***

I. INTRODUCTION

A. General context

Nowadays, the internet revolution and the digitization of information provides the easiness of the interchange of data; meanwhile, privacy and security of information for any organization and users has become a challenge over the public networks. Various techniques have been proposed; data encryption remains one of the most used solutions which uses certain algorithms to cipher secret data. However, even though the encryption protects the content of secret information, it still attracts attention of a third-party eavesdropper. That's why we use steganography that makes the communication invisible. It is a sub-discipline of Data Hiding; whose main purpose is to hide even the fact that secret information is exchanged [1], [2].

Revised Manuscript Received on February 28, 2020.
***** Correspondence Author
Ismail Kich*, Research Team MSISI – LaRIT, University Ibn Tofail, Morocco. kichsma@gmail.com
El Bachir Ameur, Research Team MSISI – LaRIT, University Ibn Tofail, Morocco. ameurelbachir@yahoo.fr
Youssef Taouil, Research Team MSISI – LaRIT, University Ibn Tofail, Morocco. taouilysf@gmail.com

Imperceptibility, capacity and resistance to various attacks are the main pillars that support the development of a steganographic model. Imperceptibility allows to estimate the quality of the stego image; it is measured generally by the PSNR. Capacity refers to the quantity of secret data that can be inserted in the cover image, whereas security express the undetectability by third-party steganalysis attacks [3]. These parameters are narrowly related. It is therefore essential to look for a compromise between the values of these parameters, and especially that which allows obtaining a good capacity while keeping acceptable values of other parameters.

Spatial domain and transform domain are the main approaches in steganography. Least Significant Bit technique (LSB) is the most famous technique in the spatial domain approach [4], [5]. It directly integrates secret data by substituting the LSBs of the cover image's pixels with secret information bits. Nevertheless, it has shown vulnerability to statistical attacks due to the uniformity created in the histogram. In the second approach, the host image is converted to frequency domain before embedding the secret data in the transform coefficients like the Discrete Cosine Transform and the Discrete Wavelet Transform [6], [7]. Transform domain techniques are more robust against attacks and manipulation by third-party. Several methods have been developed in both domains to improve the Stego image quality against different attacks. The proposed scheme is a type of spatial domain technique.

B. Related work

The key objective of any steganographic systems is their undetectability against visual attacks, and their security against structural attacks. after the concealment, the statistical distribution of the stego image shall be as identical as possible to the cover image's, because a significant modification in the visual and statistical characteristics of the host image can lead to easily being detected by steganalysis attacks. Therefore, the selection of regions that will host the secret data is an important factor in the undetectability of any steganography model. Pixels in complex zones are not easy to model since they are considered as noise pixels; their intensity differ remarkably to their neighbor. because of this property, they are a better choice to conceal secret information in comparison to smooth regions. Hence, edge adaptive hiding schemes are one of the eminent techniques in the spatial domain-based steganography.

Edges adaptive schemes are based on classical edge detectors in which operators as Laplacian, Prewitt, Sobel, Robert, Fuzzy, and Canny are applied to find edge pixels in the Cover image.

There are so several edge detection methods developed but some of them still pose the problem of obtaining the same results for the edge areas before and after the embedding process.

In [8], authors use hybrid edge detection, fuzzy and canny detectors to select pixels where data is meant to be hidden; the insertion is performed by the LSB substitution. They could increase hiding payload with better Stego image quality. Moreover, it is secure versus statistical detection attacks.

The authors in [9], proposed a steganography method by applying canny edge identification on only one channel of color images; the embedding process is performed by applying LSB matching in the other two channels using the first one as an edge map. Experimental results showed that the technique improved security against visual attacks compared to existing steganography techniques. However, the structural image quality is poor against Blind image attacks. In [10], the authors proposed to operate only the edge pixels of the host image to dissimulate the secret information. The canny filter helps to detect the edge pixels based on the capacity of the message. They enhanced the resistance to steganalysis attacks outperforming other edge-based steganographic systems such as Hiding Behind Corners (HBC) [11] and Edge Adaptive Image Steganography (EALMR) [12].

In [13], a novel image data hiding algorithm to conceal secret information either in the transform or in the spatial domain of the cover image is proposed; the technique fuses the advantages of edge detection and XOR coding to get better imperceptibility results than other steganography methods. In [14], an adaptive steganography scheme based on fuzzy edge detection that embeds secret data in the edge areas of the gray image is proposed. Experiment results showed that this technique increases the quality of the output image better than other techniques for the same payload.

In this paper, M-SLIC based image steganographic model is proposed. The host image is segmented by the M-SLIC algorithm and thus fragmented into K regions (superpixels). The segmentation is very helpful to objects identification and contours detection between the said objects. The idea behind the segmentation by M-SLIC algorithm is to qualify the borders separating the objects as edge areas. On the contrary of edge regions, Human visual system is conceived to notice modifications within smooth areas pixels. Therefore, edge areas tolerate stronger modifications than smooth areas without causing detectable distortions [15]. The dissimulation of the secret message in the 2-LSB violates the basic assumption of statistical attacks, thus it is advantageous than simple LSB-substitution [16]. Finally, the algorithm of 2^r correction is performed to reach better stego image quality. Experimental results reveal that the model proposed in this paper is visually and statistically undetectable in comparison to existing steganographic systems. The performance is analyzed by testing it on two images databases, BOSSbase[1] ver. 1.01 and BOWS2[2] databases, each one has 10,000 gray images.

The rest of the paper is structured as follows: The Modified SLIC algorithm and the simple LSB with 2^r correction techniques are respectively presented in section 2 and 3. The proposed steganographic model is conceived in section 4. In section 5, Results of the proposed model tests and the comparison to prior works are presented and discussed. Finally, section 6 concludes the paper with a recapitulation and perspectives.

II. M-SLIC ALGORITHM

A. Simple Linear Iterative Clustering

The algorithm of SLIC is one of the best and most modern superpixels approaches [17]. It generates superpixels by expanding the k-means clustering algorithm, which allows to obtain a larger number of superpixels. It has a linear complexity in numbers of pixels and related to the color and distance simulation to implement the superpixels segmentation.

The SLIC algorithm was originally developed for color image represented in the CIELAB color space to form the superpixels. There are two input parameters for this algorithm: K is the number of the desired superpixels, and m is the weight coefficient. The superpixels size is approximately equal, and m controls the dependence between spatial proximity and color similarity.

Let C be the cover image that has to be segmented into K superpixels by the SLIC algorithm, and let N be the pixels number and S be the grid interval where $S=\sqrt{\frac{N}{K}}$.

The SLIC chooses randomly K cluster centers; then, in each $2S\times 2S$ region, we compute the distance between pixels and centers. Depending on the distance, each pixel is tagged to the nearest center. The mathematical expression of the distance D_{ij} between the pixel i and the j^{th} cluster center is given as follows [17]:

$$D_{ij}=\sqrt{d_{lab}^2+\left(\frac{m}{S}\right)^2 d_{xy}^2},\quad i,\ j\in\{1,...,N\} \tag{1}$$

where

$$d_{lab}=\sqrt{\left(l_i-l_j\right)^2+\left(a_i-a_j\right)^2+\left(b_i-b_j\right)^2} \tag{2}$$

$$d_{xy}=\sqrt{\left(x_i-x_j\right)^2+\left(y_i-y_j\right)^2} \tag{3}$$

$m\in[10,20]$ and (l_i,a_i,b_i) the CIELAB space color coordinates of the pixel i in location $\{x_i,y_i\}$. Hence, the initial color image is segmented to K compact clusters; which are visually separated by either drawing borders or coloring superpixels differently as can be seen in section 4.

B. Modified SLIC

The extension of the SLIC algorithm to the gray images is based on modifying the distance D_{ij} as follows [18]:

$$D'ij=\sqrt{\left(I_i-I_j\right)^2+\left(\frac{m}{S}\right)^2 d_{xy}^2},\quad i,j\in\{1,...N\} \tag{4}$$

[1] BOSSbase database ver.1.01 in http://dde.binghamton.edu
[2] BOWS2 database in http://bows2.ec-lille.fr

where I_i and I_j are the values of the pixel i and the j^{th} cluster center respectively. In the proposed method, the role of the modified SLIC algorithm is to construct the edge pixels' map that will locate the host pixels.

III. SIMPLE LSB WITH 2^R CORRECTION METHODS

A. Simple LSB Substitution

The approach of LSB Substitution is simple and easy to implement. It takes advantage of the fact that the human vision is less perceptible at the higher level of precision in different formats of image. thus, small changes in the colors will not be noticed by the human eye. Therefore, the LSB's idea consists on replacing the least significant bit of each pixel with a bit of the of secret message. the output image is seemed unaltered compared to the original one [19].

For example, if we want to dissimulate the character *"S"* represented in ASCII code by the following binary string "01010011" in a gray image. we will need 8 pixels to dissimulate *"S"*. suppose that these 8 bits are as follows:

1101010**0** 1100110**1** 1100100**0** 1101001**0**
1100111**0** 1100101**1** 1101100**1** 1101110**1**

After having concealed the binary chain of *"S"* we obtain the following result:

1101010**0** 1100110**1** 1100100**0** 1101001**1**
1100111**0** 1100101**0** 1101100**1** 1101110**1**

In the example above, only two out of eight bits were really changed (shown in bold). the statistics have shown that by applying the LSB substitution, about half of the pixels' LSB will be changed which gives strength to this method in terms of imperceptibility.

B. 2r Correction method

The embedding of the secret information in the pixels of the cover image leads to differences between the values of the Cover-pixels and Stego-pixel; these differences can cause remarkable decrease in the quality of the output image. To overcome these differences, the 2^r correction allows to obtain a better imperceptibility.

The algorithm of 2^r correction is detailed as in [20]:

After hiding r bits into the cover pixel pi, let $EV=|p_i-p'_i|$ be the issued error value between p_i and its corresponding Stego-pixel p'_i. Let p''_i be the obtained value of Stego-pixel after the 2^r correction.

if $\left(p'_i - p_i > 2^{r-1}\right) \& \left(p'_i - 2^r \geq 0\right)$

$$p''_i = p'_i - 2^r$$

Else if $\left(p'_i - p_i < -2^{r-1}\right) \& \left(p'_i + 2^r \leq 255\right)$

$$p''_i = p'_i + 2^r$$

Else

$$p''_i = p'_i$$

For example:

Secret binary data: $\underline{00}1001010..._{(2)}$, $r=3$

Cover pixel value $p_i = 198 = 11000110_{(2)}$

Stego pixel value $p'_i = 193 = 11000001_{(2)}$

Error value $EV = |198-193| = 5 > (2^{3-1} = 4)$

in this case, p''_i has two possible values:

$p''_i = p'_i - 2^3 = 193-8 = 185$ or $p''_i = p'_i + 2^3 = 193+8 = 201$

The 2^r consists of choosing between these two values the closest one to the pixel p_i. Thus $p''_i = 201\,(11001\underline{001})$

This way, the 2^r correction makes the new Stego pixel p''_i closer to the original Cover pixel p'_i without affecting the secret data.

IV. PROPOSED METHOD

The main problem encountered by most steganographic techniques built from edge detection is to retrieve the same edge areas before and after the integration process [13]. So, true message extraction is impossible in some cases. The proposed technique remedies to this problem and ensures the same edge locations are retrieved in the extraction phase of the steganographic system. The proposed M-SLIC algorithm is used to segment the cover image into *K* superpixels; the borders between those superpixels are considered edge pixels that embed the secret data. The number of superpixels *K* depends on the image texture and the payload of data to be embedded. The shorter messages, the smaller is the needed value of *K* to accomplish the concealment. When the message's size increases, the value of *K* is adapted accordingly. As result, an edges map is established from the obtained superpixels. Figure 1 shows the edge maps for different values of *K* compared to the one obtained using conventional canny detection.

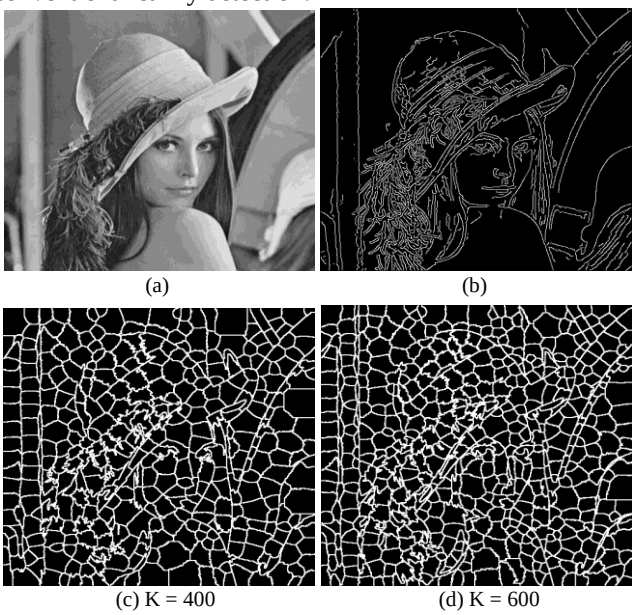

Fig. 1. (a) Cover, (b) Canny detection and proposed M-SLIC detection (c) with K = 400 (d) with K = 600

To guarantee obtaining the same edge map in both the embedding and the extraction phases, the M-SLIC algorithm is not applied directly on the host image; but the *2*-LSBs of each pixel are masked, then the edge detection is performed on the remaining six most significant bits (MSB) to generate the edge map of the host image. Table 1 reveals numbers of edge pixels detected by the proposed technique, before and after masking the 2-LSBs of the host image for 100 images randomly selected in BOSSbase ver. 1.01. Results are compared to those obtained by applying Canny edge identification. It should be noted for the Canny method, there is no generic method for determining a kernel width and thresholds producing satisfactory results on all types of images. The modification of these parameters does not have a great influence on numbers of edge pixels obtained. These thresholds will be chosen automatically by the algorithm itself. Results in Table I reveal that the number of edge pixels of the cover image is nearly the same as of the masked image; also the proposed method gives the opportunity to augment amounts of edge pixels while increasing numbers of superpixels which makes it possible to augment the payload of the secret data.

Table I. Average of number of edge pixels' difference

Edge Detection Method		Edge pixels	Edge Pixels (masked)	Difference
Canny		30184	30230	46
Superpixel M-SLIC	**K = 100**	28752	28842	90
	K = 200	39237	39440	203
	K = 300	47416	47728	312
	K = 400	54467	54814	347
	K = 600	64762	65120	358

Secret information dissimulated in the pixels' *2*-LSBs, then the 2^r correction technique is utilized to reach better imperceptibility.

To reinforce the security grade, the edges map is randomly permuted using a random key (*KEY*). This way, the secure information can be taken out from the Stego image only by intended users.

Finally, the secret message's length, the number of superpixels *K* and the key (*KEY*) are concatenated to help the recipient to successfully extract hidden information. These parameters are inserted in predefined pixels.

Embedding Algorithm

1) The *2*-LSBs of each pixel are masked to create a modified image, the edge identification is done only based on the remaining six MSB.
2) The modified image thus created is segmented into *K* superpixels where *K* is chosen by the user.
3) From the superpixels obtained, an edge map is built from the pixels that form the contours between these superpixels.
4) If numbers of edge pixels are good enough to hide the secret message, go to step 5, if not increase *K* by 10 and go to step 2.
5) The edge Map obtained is rearranged by a permutation (*KEY*) to increase the security level. The resulting edge map is utilized to embed the secret data.
6) The *2*-LSB replacement corrected by 2^r correction method is applied to insert two secret data bits into the 2-LSBs of the edge pixels selected by the (*KEY*).
7) Numbers of superpixels *K* and the key (*KEY*) required in the extraction phase to recover the message secret are integrated into predefined non-edge pixels in the Stego image before transporting it to the consignee.

Figure 2 show the diagram block of the embedding algorithm of the proposed method.

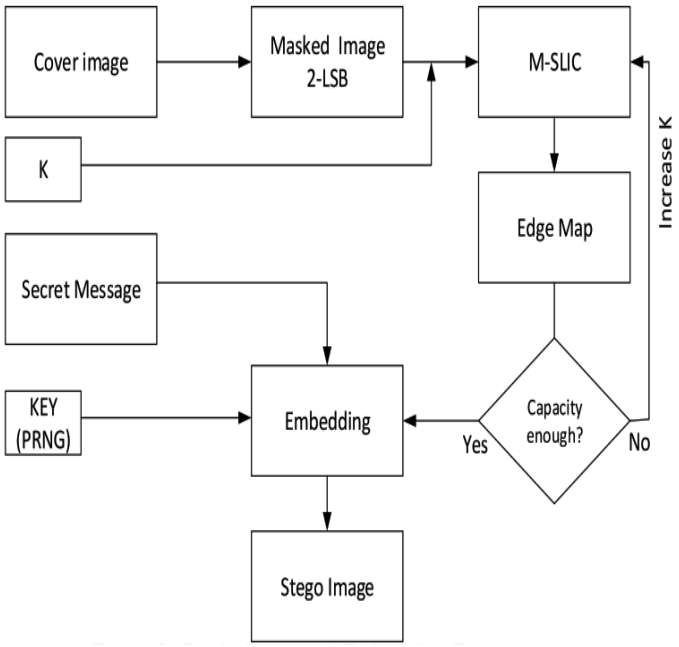

Fig. 2. Block diagram of Embedding Process

To extract the hidden information, we follow the same steps as in the dissimulation phase. The Stego image is preprocessed to retrieve the message's length, the number of superpixels *K* and the *KEY*.

Extraction Algorithm

1) The Stego image is pretreated to extract the values of *K* and *KEY*, these two parameters will be used during the rest of the extraction phase.
2) Each pixel's *2*-LSBs of the stego image are masked to create a modified image.
3) The modified image thus created is segmented into *K* superpixels.
4) From the superpixels obtained, an edge map is built from the pixels that form the contours between these superpixels.
5) Edge Map obtained is randomly arranged using *KEY*. The resulting edge Map locates from where to extract the secret data.

Figure 3 shows the diagram block of the extraction algorithm.

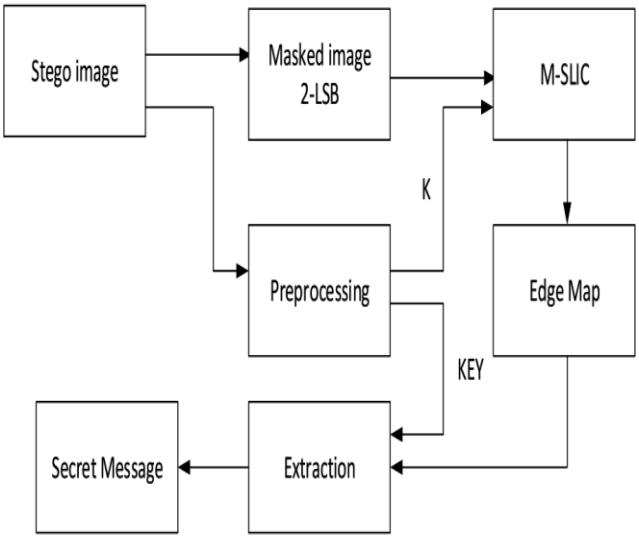

Fig. 3. Block diagram of Extraction Process

V. RESULTS AND DISCUSSION

In this section, the experiment results of the tests and the comparison are presented and discussed. The proposed model has been tested on two large images datasets: BOSSbase and BOWS2, each one has 10000 8-bit gray-scale images with size of 512x512.

The secret message is randomly generated by a pseudo random number generator (PRNG). The evaluation of the proposed steganographic system is based on the output image quality and the resistance to visual and structural attacks like weighted Stego (*WS*) [21] and sample pair analysis (*SP*) [22]. The tests are accomplished using different payload rates.

Image quality metrics like (*PSNR*), Normal Absolute Error (*NAE*), Image Fidelity (*IF*) and Average Difference (*AD*) are often utilized to evaluate the imperceptibility. These metrics are calculated by the following expressions:

$$PSNR = 10\log_{10}\left(\frac{255^2}{MSE}\right) \tag{5}$$

$$MSE = \frac{1}{CL}\sum_{i=1}^{C}\sum_{j=1}^{L}\left(p_{i,j} - p'_{i,j}\right)^2 \tag{6}$$

$$NAE = \frac{\sum_{i=1}^{C}\sum_{j=1}^{L}\left|p'_{i,j} - p_{i,j}\right|}{\sum_{i=1}^{C}\sum_{j=1}^{L} p_{i,j}} \tag{7}$$

$$IF = \frac{\sum_{i=1}^{C}\sum_{j=1}^{L}\left(p'_{i,j} - p_{i,j}\right)^2}{\sum_{i=1}^{C}\sum_{j=1}^{L} p^2_{i,j}} \tag{8}$$

$$AD = \frac{1}{CL}\sum_{i=1}^{C}\sum_{j=1}^{L}\left(p_{i,j} - p'_{i,j}\right) \tag{9}$$

Where $p_{i,j}$ and $p'_{i,j}$ are the pixels intensity of the cover and stego image respectively, *C* and *L* are the width and height of the cover image. The more the cover and stego images are close, the higher is the value of *PSNR* is greater than 35.

The *NAE* is the ratio of the absolute error to the cover image intensity, the optimal value of *NAE* is 0.

The IF shall be very close to 1, it measures the relative variation of the image's energy. *AD* is simply the average of the difference between the reference image and the test image [23], its optimal value is 0.

The Structural Similarity Index measurement (*SSIM*) [24] is used to estimate the similarity of the Stego and cover images. It is calculated from three terms, the luminance, the contrast, and the structural one. The index is computed by the expression above:

$$SSIM(x,y) = l(x,y)c(x,y)s(x,y) \tag{10}$$

where

$$l(x,y)=\frac{2\mu_x\mu_y+C_1}{\mu_x^2+\mu_y^2+C_1},\ c(x,y)=\frac{2\sigma_x\sigma_y+C_2}{\sigma_x^2+\sigma_y^2+C_2},\ s(x,y)=\frac{\sigma_{xy}+C_3}{\sigma_x\sigma_y+C3}$$

μ_x is the average of *x*; μ_y is the average of *y*; σ_x^2 is the variance of x; σ_y^2 is the variance of y; $\sigma_{x,y}$ is the covariance of *x*, *y*; C_1 and C_2 are the variables to stabilize the division weak denominator.

Figure 4 shows three randomly selected cover images from the BOSSbase database and their corresponding Stego images. The payloads embedded are successively 0.4 and 0.7 *bpp*. From these visual results, the similarity between the cover images and their output images is evident.

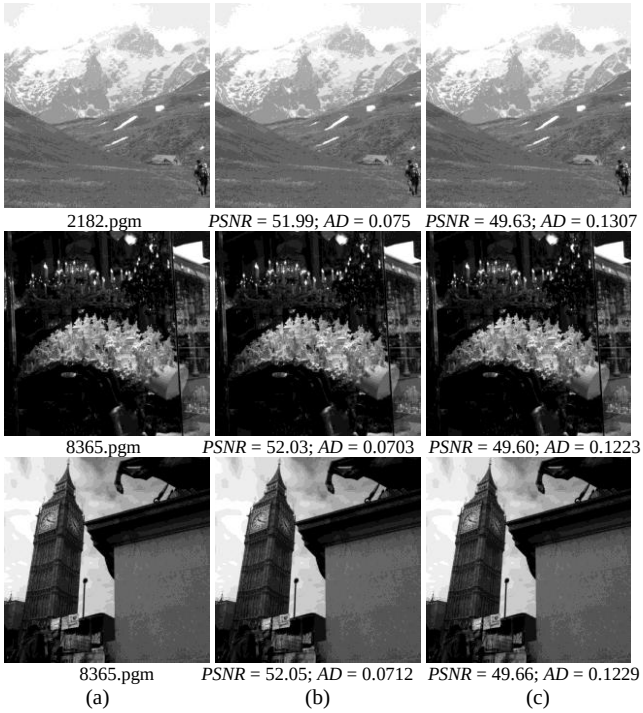

Fig. 4. (a) Cover image; (b-c) Stego images with payload of 0.4 bpp and 0.7 bpp

To check that, the proposed method is applied to 100 randomly selected images in the BOSSbase database. Quality metrics as *PSNR*, *IF*, *NAE* and *SSIM* are measured to verify the imperceptibility and similarity of the cover image and the Stego image. The payloads used are 0.1 *bpp*, 0.3 *bpp*, 0.5 *bpp*, and 0.7 *bpp*. Table 2 gives the imperceptibility and the similarity tests results.

Table II. Perceptual quality assessment of proposed system using 100 randomly selected images

Payload (*bpp*)		*PSNR*	*IF*	*NAE*	*SSIM*
0.1	***min***	56.058	0.999580	$3.32\,e-4$	0.997663
	max	58.838	0.999998	$5.92\,e-3$	0999897
	mean	58.093	0.999991	$5.16\,e-4$	0.999138
0.3	***min***	51.413	0.998766	$6.92\,e-4$	0.992030
	max	53.982	0.999995	$1.75\,e-2$	0.999685
	mean	53.310	0.999975	$1.55\,e-3$	0.997544
0.5	***min***	49.324	0.997973	$1.16\,e-3$	0.987479
	max	51.7798	0.999992	$2.91\,e-2$	0.999483
	mean	51.078	0.999959	$2.58\,e-3$	0.996030
0.7	***min***	48.034	0.997171	$1.61\,e-3$	0.982997
	max	50.068	0.999988	$4.09\,e-2$	0.999294
	mean	49.629	0.999944	$3.57\,e-3$	0.994642

Results show that the proposed method keeps a good level of imperceptibility Even with the concealment of a large payload of data. The payload exceeds 0.7 bpp with a slight decrease in image quality. The lowest value of *PSNR* is 49.62 *dB*. *NAE* is very close to 0, and *IF* values are very close to 1. From Table II we can also see there is a strong similarity between the Cover and their Stego images. The values of the *SSIM* are very close to 1. Even with the significant increase in secret data concealed, the *SSIM* value decreases very slightly. The advantage of the proposed technique is that the dissimulation in the edge pixels allows preserving the quality of the stego images which provides a strong resistance to visual attacks.

Table III shows the average value of the image quality evaluation of the BOWS2 database with different data capacities of the proposed method compared with Edge Adaptive LSB [12], EDGE-XOR [13], Canny Edge detection [10] and the one that use the novel Fuzzy detection method presented in [14].

Note the average results values of *PSNR* and *AD* for the 0.25 *bpp* payload for the Canny detection method are calculated only from a portion of the images in the BOWS2 database.

Most images do not exceed 10% payload. Compared to other techniques, the results illustrate the proposed technique provides a high image quality indicated by the *PSNR* for different hidden payloads as well as lower values for the Average Differences between Cover image and its resulting Stego image. The *PSNR* values of the proposed method lie between 58.10 *dB* and 49.63 *dB* with different amount of data, although the values for Edge detection method [14] are between 56.76 *dB* and 48.59 *dB*.

Similarly, the Average Difference lies between 0.0179 and 0:1240 in the proposed method, whereas the values for Fuzzy Edge detection method are between 0.0321 and 0.1831. The graphical comparison plot between the proposed technique with other methods using *PSNR* and *AD* metrics is shown in Figure 5. The proposed technique with the M-SLIC algorithm to define the edge pixels compared to other techniques in domains spatial attain higher quality values for the Stego images.

Table III. Perceptual quality assessment comparison of proposed method

Payload (*bpp*)		Edge Adaptive LSB	Edge XOR	Fuzzy Edge detection	Canny Edge detection	Proposed Method
0.1	***PSNR***	53.26	53.53	56.76	57.31	**58.10**
	AD	0.0842	0.0849	0.0321	**0.0081**	0.0179
0.25	***PSNR***	48.82	49.72	52.98	53.31	**54.09**
	AD	0.2216	0.2085	0.0703	**0.0202**	0.0448
0.4	***PSNR***	46.88	47.83	50.98	####	**52.02**
	AD	0.3446	0.3282	0.1076	####	**0.0719**
0.5	***PSNR***	45.89	46.94	50.03	####	**51.08**
	AD	0.4292	0.4049	0.1321	####	**0.0893**
0.6	***PSNR***	45.09	46.17	49.25	####	**50.28**
	AD	0.5173	0.4842	0.1577	####	**0.1072**
0.7	***PSNR***	44.42	45.50	48.59	####	**49.63**
	AD	0.6027	0.5651	0.1831	####	**0.1240**

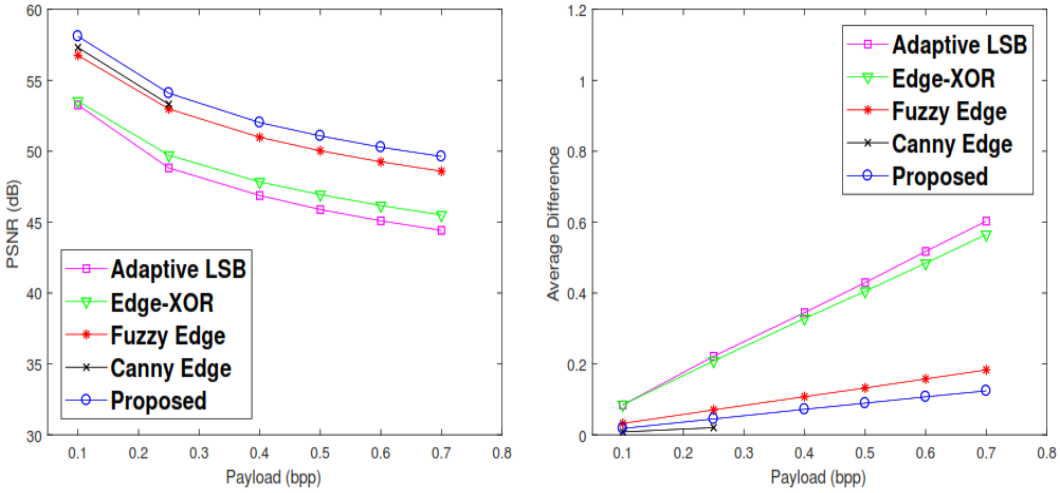

Fig. 5. Comparison of (a) *PSNR* values and (b) Average Difference values with the proposed technique.

The structural attacks are built on the observation of the first and the second order statistical changes in image structure. The *WS* [21] and *SP* [22] are two well-known attacks that aim to detect the existence of a hidden data and calculate its length by estimating numbers of pixels susceptible to hide data in the Stego image. These two attacks are applied to the original images of both databases to estimate the average value relative of payload.

Table IV compares the results of the *WS* and *SP* for the Canny edge method [10] and the proposed method; the payload used are 0.1 *bpp* and 0.25 *bpp*. The results for the 0.25 *bpp* are calculated for just the images that have the ability to hide this payload. It can be noted the estimated payloads of the message hidden in the Stego images are close to the estimated average values for the Cover images for both methods. We can also notice that the average value of the *PSNR* increased for the proposed technique. Hence, we can conclude the proposed model does not raise any doubt and is robust against visual and structural attacks.

Table IV. *WSP* and *SP* relative message length for Canny edge and proposed techniques (estimation results)

Database	Payload (*bpp*)	Attacks	Cover image	Canny Edge	Proposed method
BOSSbase ver.101	0.1	*SP*	0.0091	0.0371	0.0241
		WS	0.0008	0.0173	0.0103
		PSNR	#####	57.31	58.10
	0.25	*SP*	0.0091	0.1000	0.0526
		WS	0.0008	0.0441	0.0256
		PSNR	#####	53.31	54.10
BOWS2	0.1	*SP*	0.0006	0.0276	0.0115
		WS	0.0001	0.0167	0.0090
		PSNR	#####	57.32	58.13
	0.25	*SP*	0.0006	0.0787	0.0409
		WS	0.0001	0.0411	0.0259
		PSNR	#####	53.33	54.09

In both image databases, numbers of edge pixels obtained using the Canny technique does not exceed 10% in most images; consequently, the capacity of this method does not exceed 0.1 *bpp*. In contrast, the proposed model can double or even triple the capacity of the proposed method by increasing numbers of superpixels and, simultaneously, we maintain its security against visual and structural attacks, as shown in Table V.

Table V. SP and WS relative message length for proposed technique for different values of *K* (estimation results)

Database	Attacks	Proposed method			
		K = 100	K = 200	K = 400	K = 600
		0.1 *bpp*	0.2 *bpp*	0.3 *bpp*	0.4 *bpp*
BOSSbase ver.101	SP	0.0241	0.0414	0.0619	0.0781
	WS	0.0103	0.0198	0.0305	0.0400
	PSNR	58.10	55.08	53.31	52.01
BOWS2	SP	0.0115	0.0293	0.0488	0.0684
	WS	0.0090	0.0186	0.0287	0.0406
	PSNR	58.13	55.09	53.32	52.02

VI. CONCLUSION

Hiding the secret data in the complex regions is one of the methods that allows minimizing distortion in the cover image; which increases the level of undetectability of the stego image against visual attacks and their security against structural attacks. In this paper, an adaptive steganography model in gray scale image is proposed; the method uses Modified-SLIC edge detection technique to insert secret data without having a perceptible anomaly in the Cover image. The edges are (regarding the data length) detected using the over-segmentation by Modified SLIC. The proposed technique permits to find the same edge locations in the dissimulation and extraction processes; which enables the recipient to accurately retrieve the secret information dispatched by the sender. The obtained results show that the capacity exceeds 0.7 *bpp* while keeping a good quality of Stego image, even with the significant increase in secret data concealed, the *PSNR* and *SSIM* value decreases slightly. As for the security, it can be noted that the modifications in edge areas do not significantly affect the original distribution of the image, the estimated payloads of the hidden message in the Stego images by the *SP* and *WS* attacks are close to the estimated average values for the Cover images and too less than the actual length of hidden message for different capacity tested.

Experiment results reveal the proposed technique is resistant to visual and structural attacks. In addition, it outperforms other models developed in the spatial domain for the same embedding capacity rates. In future work, this method can be extended to color images.

REFERENCES

1. N. Provos and P. Honeyman, "Hide and seek: An introduction to steganography", IEEE security & privacy, vol. 99, 2003, n° 3, p. 32-44.
2. Y. Taouil, E. L. Ameur et M. T. Belghiti, "New image steganography method based on haar discrete wavelet transform", Europe and *MENA* Cooperation Advances in Information and Communication Technologies, 2017 p. 287-297.
3. N. F. Johnson, Z. Duric and S. Jajodia, "Information Hiding: Steganography and Watermarking-Attacks and Countermeasures: Steganography and Watermarking: Attacks and Countermeasures", vol. 1, 2001.
4. X. Liao, Q. Wen, and J. Zhang, "A steganographic method for digital images with four-pixel differencing and modified LSB substitution", Journal of Visual Communication and Image Representation, vol. 22, 2001, p. 1-8.
5. A. Benhfid, E. B. Ameur and Y. Taouil, "High capacity data hiding methods based on spline interpolation", 2016 5th International Conference on Multimedia Computing and Systems (ICMCS), 2016, p. 157-162.
6. J. Fridirich, M. Goljan and R. Du, "Detecting LSB steganography in color, and gray-scale images", IEEE multimedia, vol. 8, 2001, n° 4, p. 22-28.
7. Y. Taouil, E. B. Ameur, A. Benhfid, R. Harba and R. Jennane, "A Data Hiding Scheme Based on the Haar Discrete Wavelet Transform and the K-LSB", International Journal of Imaging and Robotics, vol. 17, n° 3, 2017.
8. W. Chen, C. Chang and N. T hoang, "High payload steganography mechanism using hybrid edge detector", Expert Systems with applications, vol. 37, 2010, n° 4, p. 3292-3301.
9. M. Modi, S. Islam and P. Gupta, "Edge based steganography on colored images", International Conference on Intelligent Computing, 2013, p. 593-600.
10. S. Islam, M. Modi and P. Gupta, "Edge-based image steganography", EURASIP Journal on Information Security, Vol. 2014, n° 1, p. 8.
11. Hempstalk, Kathryn, "Hiding behind corners: Using edges in images for better steganography", Proc. Computing Women's Congress, Hamilton, New Zealand, vol. 14, 2006.
12. W. Luo, F. Hung and J. Hung, "Edge adaptive image steganography based on LSB matching revisited", IEEE Transactions on information forensics and security, Vol. 5, 2010, p. 201-214.
13. H. Al-Dmour and A. Al-Ani, "A steganography embedding method based on edge identification and XOR coding", Expert systems with Applications, vol. 46, 2016, p. 293-306.
14. S. "Kumar, A. Singh and M. Kumar, "Information hiding with adaptive steganography based on novel fuzzy edge identification", Defence Technology, 2018.
15. Y. Taouil and E. L. Ameur, "Steganographic Scheme Based on Message-Cover matching", International Journal of Electrical and Computer Engineering (IJECE), vol. 8, 2018, n° 5, p. 3594-3603.
16. Ker, Andrew D, "Steganalysis of embedding in two least-significant bits", IEEE Transactions on Information Forensics and Security, vol. 2, 2007, n° 1, p. 46-54.
17. R. Achanta, A. Shaji, K. Smith and A. Lucchi, "SLIC superpixels compared to state-of-the-art superpixel methods", IEEE transactions on pattern analysis and machine intelligence, vol. 34, 2012, n° 11, p. 2274-2282.
18. X. Bai, Z. Cao, Y. Wang, M. Ye and L. Zhu, "Image segmentation using modified SLIC and Nyström based spectral clustering", Optik-International Journal for Light and Electron Optics, vol. 125, 2014, n° 16, p. 4302-4307.
19. C. Chan and L. Cheng, "Hiding data in images by simple LSB substitution", Pattern recognition, vol. 37, 2004, n° 3, p. 496-474.
20. Sun, Shuliang, "A novel edge based image steganography with 2k correction and Huffman encoding", Information Processing Letters, vol. 116, 2016, n° 2, p. 93-99.
21. A. Ker and B. Rainer, "Revisiting weighted stego-image steganalysis", Security, Forensics, Steganography, and Watermarking of Multimedia Contents X, vol. 6819, 2008, p. 681905.
22. S. Dumitrescu, X. Wu and N. Memon, "On steganalysis of random LSB embedding in continuous-tone images", Proceedings. International Conference on Image Processing, vol. 3, 2002, p. 641-644.
23. A. Eskicioglu and P. S. Fisher, "Image quality measures and their performance", IEEE Transactions on communications, vol. 43, 1995, n° 12, p. 2959-2965.
24. Z. Wang, A. Bovik, H. Sheikh and E. Simoncelli, "Image quality assessment: from error visibility to structural similarity", IEEE transactions on image processing, vol. 13, 2004, n° 4, p. 600-612.

AUTHORS PROFILE

Ismail Kich, PhD Student, department of computer science, Research Team MSISI – LaRIT, University IbnTofail, Morocco. His researches are focused on image and signal processing, machine learning, deep learning, steganography and data hiding.

El Bachir Ameur, Researcher Professor of Computer Sciences at the University of Ibn Tofail, Faculty of Science, Kenitra, Morocco. In 2002, he received his PhD in Numerical Analysis and Computer Sciences from the University of Mohamed I Oujda, Morocco. His PhD concerned approximation and reconstruction of 2D/3D data by spline and wavelet functions. His research interests include approximation and reconstruction of 2D/3D surfaces by spline and wavelets, signal and image processing and data hiding.

Youssef Taouil obtained his PhD degree from the Faculty of Sciences, Ibn Tofail University in 2018. He obtained in 2014 his Engineering degree in Electronics and Embedded Systems from the National School of Applied Sciences at the same University. His researches are focused on image and signal processing, multi-resolution analysis and wavelets, steganography and data hiding.